Report from the Policy Subcommittee to the Data Privacy and Integrity Advisory Committee (DPIAC)

Privacy Recommendations on the Use of Live Data in Research, Testing, or Training

Tasking

Certain DHS components use or plan to use personally identifiable information (PII) collected for operational use (live data) for training purposes, for testing new or updated systems, or for research. These uses are subject to component-specific policies and privacy protections, including Privacy Impact Assessments (PIA) and System of Records Notices (SORN). In order to develop a DHS-wide privacy policy for these uses of live data and thereby to assure uniform standards are in place for determining appropriate non-operational use of live data, the Chief Privacy Officer (CPO) in March 2012 requested that the DPIAC undertake fact finding and provide recommendations on privacy best practices on this issue.

The Policy Subcommittee was tasked with undertaking fact-finding and preparing a public report on its recommendations for the DPIAC to consider. Final DPIAC recommendations should inform the CPO in creating a Department-wide policy. The specific considerations to be addressed were the following:

1. What privacy considerations should DHS include in determining if a research, testing, or training initiative is an appropriate use of live data?
2. What specific privacy protections should DHS consider when using live data for research, testing, or training purposes?

For the purposes of this tasking we define live data as information containing PII[1] that comes from a production system, vendor, or public records, or any other dataset that otherwise contains operational data. PII that has been extracted from production systems for testing, research, or training is commonly referred to as real data; however within this tasking we consider this to be a subset of live data (*e.g.* copies of alien files, interview videos, or extracted live data that is no longer used on a production system).

I. Introduction/Findings

In order to get an overview of current practices regarding the use of live data for the relevant purposes, the Subcommittee met with the Privacy Officers of three DHS components who provided examples of their use. These interviews resulted in our classification of the types of uses into three broad categories: use in research, use in testing, and use in training.

[1] DHS defines PII as “any information that permits the identity of an individual to be directly or indirectly inferred, including any information that 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.”

A. Different Use Types

Use in Research: The Privacy Officer of the Science and Technology Directorate (S&T) reported on their use of live biometric data (iris images and fingerprints) collected at borders to conduct operational pilots and other evaluations of biometric recognition technology. S&T used live data in developing and testing forensic tools for extracting user information from used gaming consoles. In other research on security devices and related measures for securing the transport of cargo across our borders, cargo owners, trucking and freight company owners and operators voluntarily allow their GPS location data to be transmitted and collected, with no PII associated with it. S&T used live Suspicious Activity Report (SAR) data that could contain PII to test and evaluate analytic tools for a SAR Analytical Toolkit.

Use in Testing: The Privacy Officer of Immigrations and Customs Enforcement (ICE) reported on their process for granting permission to use real data to test an IT system or project. Requests are submitted in the format of a Proposal to Use Real Data for Testing, which gathers information about the intended use and the plans for managing the real data. Proposals are reviewed by the ICE Privacy Office and Office of the Chief Information Officer Information Assurance Division (OCIO IAD) to determine whether to authorize the use and under what conditions.

Use in Training: The Privacy Officer for U.S. Citizenship and Immigration Services (USCIS) reported on their policies and practices regarding the use of live data in training. USCIS uses live data in training courses for officers in their Fraud Detection and National Security Directorate and the Controlled Application Review and Resolution Program. The training is done in closed, simulated environments and may use live data in production or real data that is a copy of live data extracted from the system, as well as dummy data without PII. USCIS's policies are enunciated in a memorandum of 10/6/11 on "Using Live Data/Personally Identifiable Information (PII) for Training Purposes."

B. Potential Benefits

When considering the use of live data for the above purposes, we recommend an examination of the potential benefits. At a high level, we considered some of these benefits as follows:

- ***Realism:*** Providing training that is based on live data may provide more realistic training opportunities and the achievement of minimum competencies for certain key functions of DHS components. This allows for the more seamless transition of DHS employees into their final assignment and use in the field.
- ***Better operational effectiveness:*** Use of live data and systems may reduce margins of error when moving from the test environment to operational use.
- ***Improved research:*** Testing on live data may allow for better integrity and reliability in uses associated with research.
- ***Fitness for purpose:*** The ability to test new approaches or technology on live data may assist with determining the operational value and effectiveness of a specific program.

- ***Failure detection:*** The ability to determine when a new proof of concept product and service fails to deliver on its goals in a more expedient manner.
- ***Heightened sensitivity:*** For some users, live data may provide greater sensitivity to the PII that will be collected by the new product or service when it goes live.

C. Privacy Risks/Concerns

In trying to determine whether or not live data should be used, we recommend considering whether new privacy risks are created by the use, the same privacy risk exists as on the production system, or this privacy risk is merely heightened. In many instances, new privacy risks are not created, but rather existing privacy risks are heightened depending on the specific implementation of the testing, training, or research program. Privacy risks that may be created or heightened by these uses of live data include the following:

- ***Data breach:*** Heightened risk of release of live data containing PII to unauthorized persons as the result of its use for training, research, or testing.
- ***Data corruption:*** Use of live data in production for training, research, or testing results in inappropriate modification or destruction of the data is a risk that may be heightened if proper education and awareness regarding the use of live data is not explained.
- ***Secondary Use:*** Use of live data in testing, training, or research may heighten the risk of secondary use other than routine uses as identified in related SORNs. This is of special concern if this data is relied upon and is incorrect, stale, or mixed with dummy data.
- ***Invasions of Privacy:*** Unauthorized access to records in testing, training, or research is also a concern for matters involving the invasion of privacy on a system that may lack certain controls or have less robust controls in place.

II. Privacy Considerations on Use of Live Data for Training, Research, or Testing

A. Presumptions Regarding the Use of Live Data

While we recommend DHS components take a risk-based approach regarding the use of live data, this analysis should begin with a rebuttable presumption that the use of live data is not approved. The process used to make this analysis must include a written intake request, a risk analysis across standardized and delineated data points, ownership of the live data request and subsequent activity, an escalation and approval process, and auditing.

B. Process for Authorizing Use

In order to authorize the use of live data, the Subcommittee makes the following draft recommendations:

- ***Education and Awareness*****:** Include within the privacy training and awareness program instruction on how to spot live data being used or required for testing, training, or research and how to request a review by the component privacy office.

- ***Intake Questionnaire:*** Creation of a rigorous written intake questionnaire that covers the live data being requested, testing plan, risk identification and mitigation, and security controls that will be implemented in order to allow the component Privacy Officer to make a final determination. This may be accomplished by amending the current Privacy Impact Assessment (PIA), Privacy Threshold Assessment (PTA), or System of Record Notice (SORN). This process must be well defined and auditable. The Subcommittee points to the ICE ICIO "Proposal to Use Real Data for Testing" document as an example. (*See* Appendix A)
- ***Component Review:*** All proposals involving the use of live data must be reviewed and approved by the component Privacy Officer. If the component does not have a Privacy Officer, the DHS Privacy Office will review and approve all such proposals.
- ***Conditions:*** The approving privacy office may make the use of live data contingent upon meeting specified conditions.
- ***Component Reporting:*** The component Privacy Officer will timely report all approvals to the DHS Privacy Office.
- ***Approvals:*** While component Privacy Officers will review and make determinations on the use of live data, the DHS Privacy Office may make a final, over-ruling determination.

C. Issues to Address in Intake Questionnaire

Key to the analysis of the request to use live data is an understanding of the intended use, nature of the data, and controls in place to mitigate risk. Only after these areas are examined can a proper decision be rendered.

- **Intended Use of the Data**
  - Justify the need for live data for the specific use including any negative consequences that might result. Explain why data other than live data will not suffice for the intended purpose.
  - How long will the data be needed for the intended use? What are the data retention protocols and the process by which the data will be destroyed?
  - How will future expanded uses of the live data be handled, if any?

- **Nature of the Data**
  - Identify the sources of the data, data owners, and any restrictions on the onward use of the live data.
  - Identify whether the live data will be electronic information, physical documents, or audio/visual material.
  - List the data fields that contain PII, identifying those that will be removed or obscured and the specific methods used to obscure.
  - Describe the nature and number of data subjects and the criteria used to select those subjects. Address unintentional misuse of live data that is re-used or inappropriately re-introduced into a production environment.

    - Acknowledge that some PII is more sensitive than other types of information and thus requires heightened awareness of subsequent responsibilities (*e.g.* HIPAA-related information).

- **Controls and Risk Mitigation During the Use of Live Data**
    - Identify the privacy risks posed by the intended use of live data in addition to the use, transmission, and access to the live data.
    - Describe the degree of data obfuscation that can be employed (removing, masking, filtering, or otherwise obscuring PII data fields).
    - Detail the role-based access controls for controlling access/authorization to the live data.
        - Who will authorize access to the live data during the intended use?
        - How will access to the live data be limited to authorized users only?
        - How will access to the live data be documented and/or audited?
    - How will the environment where the live data will be used be protected?
        - Administrative, technical, and physical controls.
        - Confidentiality, integrity, and availability of the live data.
    - How will data be destroyed at the end of use? (Including all copies made during use.)

III. Recommended Privacy Protections for Use of Live Data for Training, Research, or Testing

The Subcommittee recommends that DHS and its components evaluate and implement mitigating controls to reduce the inherent privacy risk of using live data in training, testing, or research within appropriate residual risk levels. The implementation of these controls depends on a number of factors including the type of live data being used, the length of requested use, the current control environment, and the technical feasibility of using the live data after controls have been implemented.

Recommended controls are listed below:

- ***Data Obfuscation:*** Use obfuscation methods to remove/protect PII to the maximum extent possible consistent with meeting project objectives.
- ***Data Minimization:*** Minimize the size of datasets and the number of PII fields used.
- ***Physical/Environmental Protection:*** Restrict and secure the environment where the data is used and stored. Limit the ability to remove live data in either physical or electronic format from the environment.
- ***Access Controls:*** Limit access to the data to authorized users with business need and who have received appropriate data protection training.
- ***Technical Controls:*** Use other security safeguards, such as encryption, to protect the data where appropriate.
- ***Retention Limits:*** Limit the time period for use of the data to the extent consistent with meeting project objectives. Securely dispose of live data at end of use period.

- ***Use Limits:*** Limit through controls and education the likelihood that live data, whose integrity is not reliable, is re-introduced into production systems or transferred to others beyond its intended purpose.
- ***Destruction:*** Destroy physical and electronic live data used for training, testing, or research on a regular basis or at the conclusion of the project.
- ***Watermarking:*** Include warning information on live data where possible to ensure users do not assume it is dummy data.
- ***Legal Controls:*** Implement Confidentiality and Non-Disclosure Agreements where practicable for employees as well as third parties and consultants.
- ***Accountability:*** Ensure that identified personnel (by role) are assigned responsibility for compliance with any conditions of the approval for the use of live data.
- ***Training & Awareness:*** Provide safety and training sessions for all persons having access to live data.

IV. Conclusion

The Subcommittee believes that there are occasions when the use of live data containing PII in research, testing, and training can be justified. We recommend the use of a rigorous privacy risk analysis process that will allow privacy officers to determine the necessity and the privacy risks implicated by such a proposed use. With such a process, DHS can make wise decisions, including the implementation of appropriate controls on approved uses, which will enable it to achieve its mission-critical operational objectives without imperiling individual privacy.

Appendix A

Proposal to Use Real Data for Testing Questionnaire
DHS Immigration & Customs Enforcement

PROPOSAL TO USE REAL DATA FOR TESTING

Complete this Testing Questionnaire when there is a need to request permission to use real data, whether in original or altered form, to test an IT system/project at ICE.

"Real data" means data from a production system, vendor, or public records, or any other dataset which otherwise contains operational data. For example, a dataset that is a ten-year old backup of an existing system and contains data about real individuals, matters, or cases, would be real data. A set of public records that was purchased from a vendor for use in testing would also be real data.

The ICE Privacy Office and OCIO Information Assurance Division (IAD) will use this form to determine whether to authorize the use of real data for testing and under what conditions. The goal is to ensure that risks to privacy and security are minimized while allowing needed tests to proceed. If you are unsure if the test dataset is real data, please contact the ICE Privacy Office.

Instructions: Return this completed form to the ICE Privacy Office and the ICE OCIO IAD email addresses below. Please include a copy of the Independent Test Plan. The ICE Privacy Office will coordinate with IAD and the final determination will be reflected on the last page of this form. The form will be returned to you in PDF when final and uploaded into Trusted Agent FISMA.

Contact Points:

ICE Privacy Office
202-732-3300
ICEPrivacy@dhs.gov

ICE OCIO IAD
IAD-Se@ice.dhs.gov

Recommendations: To limit review time, please be sure to follow these tips:

- Use diagrams to illustrate the proposal. Submit a diagram that visually depicts the flow of data from the source(s) into the testing environment and, if the test data will be disseminated further, to other environments as well. Be sure it clearly depicts what C&A boundaries the data originates from, is sent through, and is stored in.

- Avoid overly technical language. Remember that overly technical language will make the questionnaire more difficult for the Privacy Office to understand and approve. Please explain technical concepts in plain language whenever possible. Attach diagrams or flow charts if that makes it simpler to explain.

- Use consistent terminology. Decide at the beginning what terms you will use to describe the relevant systems, databases, environments, and datasets, and use those terms throughout once defined.

SECTION 1: Basic Information

DATE submitted to ICE Privacy Office:

IT System/Project From Which the Test Data Originates:

Name/version:

What PIA(s) describes this system/project and the data being used for testing?

What SORN(s) covers the data in this system/project and the data being used for testing?

System Owner (ICE Office): <Select Office>
Sub-Office, if applicable (e.g., Office of International Affairs):

Primary OCIO POC
Name:
Title:
DHS Email address:
Phone number:

Alternate OCIO POC
Name:
Title:
DHS Email address:
Phone number:

System Owner POC (Please ensure this POC is aware of this proposal)**
Name:
Title:
DHS Email address:
Phone number:

System ISSO

Name:
Title:
DHS Email address:
Phone number:

Does the proposed testing involve classified systems or classified data?

□ No. [Proceed to Section 2.] □ Yes. [STOP. Contact IAD.]

SECTION 2: Testing Plan

1. **Which of the following best describes the proposal?**

   □ Use real data as-is (no plans to remove, mask, filter, or otherwise obscure any data fields)

   □ Remove, mask, filter or otherwise obscure **some** of the data fields

   □ Remove, mask, filter or otherwise obscure **all** of the data fields

   □ Use synthetic data to replace **some** of the data fields (some real data will be used)

   □ Use synthetic data in **all** data fields (real data will not be used) **If selected, please complete questions 2-4 only and return to the ICE Privacy Office.*

2. **Is there a Data Management Plan (DMP) and a Test and Evaluation Master Plan (TEMP) in existence?** □ YES □ NO **If yes, provide e-copies to the ICE Privacy Office.**

   Note: If the plan is to mask, filter, replace or otherwise obscure data, please ensure that the TEMP adequately describes (1) all data fields in the proposed test dataset, (2) which of those fields will be removed or altered, and (3) how that will occur. If more space is needed for the response, please provide this information in a separate attachment.

<Describe here.>

3. **Select the option that best describes the intended use of this test dataset:**

   □ One-time use only; the data will be deleted when this test is complete (proceed to next question)

   □ Create one dataset for use in this test and future tests, with a defined end point; the test data will not be refreshed. Test data will be deleted when this batch of testing is complete (*answer Question 3.a.)

   a) **Describe the type of testing that will be conducted and an estimated completion date for the testing.**

   □ Create a test dataset for use in this test and refresh or replace that test dataset with new data for use in future tests, with a defined end point; the data will be deleted when this batch of testing is complete (*answer Question 3.b.)

   b) **Describe the type of testing that will be conducted. Explain whether the refresh will be a complete replacement of the original test data or add/mod/delete update to the original test data. Explain why the test data needs to be refreshed at all and how often it is estimated the refresh process will occur. Include an estimated completion date at which the testing will be over and the test dataset deleted.**

4. **Select the type(s) of testing for which the data will be used. Select all that apply and enter estimated start/end dates for each.**

□ System Acceptance Testing Start: End:

□ Performance Testing Start: End:

□ Security Testing Start: End:

□ Disaster Recovery Testing Start: End:

□ Interoperability Testing Start: End:

□ User Acceptance Testing Start: End:

□ Sect. 508 Interoperability Testing Start: End:

□ Other (describe below) Start: End:

5. **Identify any and all IT environment(s) that test data would reside in or be sent/exposed to, and whether those environments are part of a production or separate test environment. If testing will include transmission of test data to other environments, list those environments and whether they will be sending or receiving the test data, or both. Also identify the ATO date for the environment.**

Environment Name	FISMA ID #	Owner (e.g., ICE, DHS, Vendor)	Production or Test Environment?	Send / Receive Test Data? (S/R/Both)	ATO Date

SECTION 3: Test Dataset

6. **Identify all sources of the production data or any other real data (including data from a vendor or public records) that are proposed for use during testing. For ICE systems, identify the system or subsystem name. For sources outside of ICE, also identify the agency, vendor, or entity that owns and/or is providing the data.**

Data Source Name (e.g., ENFORCE, NCIC)	FISMA ID #	Owner (e.g., ICE, DHS, Vendor)	ATO Date

7. **For each data source identified in Question 6, how many records from the production dataset (and any other source(s) of real data) are proposed to be used in testing? (If the number of records vary for different types or stages of testing, please indicate that and specify the numbers for each testing type.)**

Answer:

a) **How was the number of records determined? Describe the factors that were considered and how the number is reasonably related to the goals of the testing.**

Answer:

b) **If fewer records were authorized to be used for testing, could the testing goals still be achieved?**

□ Yes. Indicate the minimum number of records required:

□ No. Describe what specific test goals would be hampered and why:

8. **Whose personally identifiable information (PII)[1] would be included in the intended test dataset? Check all that apply. (Please answer even if some/all of this data will be removed or obscured prior to testing.)**

□ DHS employees and/or contractors

□ Other federal personnel or contractors

□ Aliens, subjects of criminal investigations

□ Members of the public *(Briefly describe below the types of individuals, e.g., people who file FOIA requests)*

□ The dataset is real data but it does not contain any information about individuals. *(Briefly describe below what general categories of data are in the dataset. Then* ***stop here*** *and send to the ICE Privacy Office for review.)*

[1] Personally identifiable information (PII) is 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 the individual's citizenship or immigration status. Information about an individual may be considered PII even after the individual's name has been removed or masked.

□ The dataset will consist of synthetic (artificial) data only. No real or operational data will be used. *(If selected, **stop here** and send to the ICE Privacy Office for review.)*

9. **What types of data about individuals are contained in the test dataset? Check all that apply. (Answer even if some/all of this data is proposed to be removed/obscured before testing.)**

□ Name

□ Social Security Number: □ Partial *or* □ Full

□ Date of Birth: □ Partial *or* □ Full

□ Biometric data (e.g., fingerprints, retina scans)

□ Other identifying data (e.g., photographs, addresses, phone numbers, identification document numbers)

□ Employment-related data (e.g., training, benefits, hiring, background, performance, etc.)

□ Financial data (e.g., accounts, salary, transactions, income tax, etc.)

□ Income tax data

□ Investigatory data (criminal or administrative)

□ Criminal history data

□ Immigration enforcement/detention/removal/benefits/case data

□ Alien Number (A-Number)

□ Confidential information (e.g., visa application, asylum, VAWA, grand jury, SSI, etc.)

□ Medical data

□ Other. Describe the data here:

SECTION 4: General Risk Identification and Mitigation

10. **a. Who has the authority to authorize persons for access to the test data (hereafter, “testers”)? Identify name(s) and title(s).**

Answer:

b. What is the proposed minimum level of suitability for test personnel?

Answer:

c. Will the testers be government personnel, contractors or both? If contractors, please describe whether and how they will be supervised by government personnel during the testing process.

Answer:

11. **Will the identities of testers be documented?**

□ Yes. Please describe how and where:

□ No.

12. **Will tester activities be recorded, monitored and/or reviewed to detect wrongdoing or for use in an investigation if wrongdoing is suspected?**

□ Yes. Please describe how:

□ No. Describe below what other controls are in place to safeguard the data against improper use or theft by testers.

13. **How will access to the test data be properly controlled and/or appropriately limited to only authorized testers?**

Answer:

14. **If any of the test environments listed in Question 5 have a valid C&A, review any outstanding POA&Ms for those environments. Do any of these POAMs indicate there are potential risks to the test data that should be considered or addressed before testing can begin?**

□ No.

□ Yes. Please explain below.

15. **If any of the test environments do not have a valid C&A, please explain why not.**

Answer:

16. **Describe how the test data will be placed into the test environment(s), and how the data will be secured during any transfer to minimize its risk of loss, theft, or compromise.**

Answer:

17. **Does the testing require making copies of the test data (other than the primary test dataset) on portable media, for example, or its transmission across systems?**

□ No.

□ Yes. Please describe below how the various copies of test datasets or records are tracked, and how you will ensure they are destroyed at the appropriate time.

18. **How long would the test dataset(s) (including any copies identified in Question 17) be retained and why?**

Answer:

19. **Describe the proposed plan for destruction for the test data. If refreshes of the dataset will occur, please be sure to describe how the data that is no longer needed will be destroyed as part of the refresh process.**

Answer:

20. **Identify the federal employee who will be responsible for overseeing and certifying that destruction is complete.**

Name:	**Phone:**
Title:	**Office:**

SECTION 5: Risk Identification for Use of Real, Unaltered Data

**** Complete Section 5 if the proposed test dataset consists of only real, unaltered data. If the dataset also consists of masked or otherwise obscured data, please complete Section 6 instead. ****

21. **Why is the use of real unaltered data necessary and justified for the purpose of this testing?**

Answer:

22. **If the proposal to use real, unaltered data is not approved, what would be the adverse outcomes? E.g., what testing objectives could not be achieved? What test results may not be considered reliable?**

Answer:

23. **Is it possible to mask, scramble, or remove only the most sensitive data fields containing PII, without the adverse consequences described above? (E.g., remove or mask the SSN and DOB only; remove or scramble names)**

<Describe here.>

Answer:

24. **Could the test be broken up into smaller testing segments to limit the use of real, unaltered data to just those segments that require it to ensure test integrity?**

<Describe here.>

Answer:

25. **If this request proposes to create a test dataset for ongoing testing of a system, has the development/testing team considered also creating one or more test datasets of lower sensitivity (e.g., masked or artificial dataset) that can be used when the testing does not require real, unaltered data?**

Answer:

SECTION 6: Risk Identification for Use of Altered/Obscured Data

**** Complete Section 6 only if the proposed test dataset consists -- in whole or in part -- of masked, filtered, scrambled, or otherwise obscured data ****

26. **For the test dataset, list the data fields that contain PII (see note[2]) and identify which fields will remain intact, and which will be altered, removed, or otherwise obscured in some way. If**

[2] Please be sure to include all fields that contain any information that identifies or relates to an individual. This is very broad and would include fields that contain identifying data such as name, address, DOB, SSN, as well as other fields containing criminal, medical, employment, or financial data, for example. Fields containing record identifiers for databases such as NCIC, IDENT, etc. should also be listed, as should general comment fields which often contain information about individuals. If you are unsure about which fields to include, you may provide all fields or contact the ICE Privacy Office for guidance.

additional space is needed, send this in a separate document, or provide the ITP if it includes this detail.

Answer:

27. **For obscured fields, please describe below the specific method(s) that will be used to obscure data. If there are specific COTS tools, please identify those. If multiple methods will be used, be sure that the list provided indicates which method will be used on which fields.**

Answer:

28. **If the test dataset will contain any PII in real, unaltered form, please explain below why those fields are not being obscured or removed.**

Answer:

SECTION 7: Other Information

29. **Provide any other information about the proposed testing not already requested above that could be useful to the Privacy Office and IAD in assessing this proposal (e.g., additional safeguards).**

Answer:

DETERMINATION
(To be completed by the ICE Privacy Office and OCIO IAD)

Privacy Office Reviewer: Determination Date:

IAD Reviewer:

- □ **Use of real or obscured/masked data is not authorized. Testing may proceed using artificial data only.**
- □ **Use of obscured/masked data is authorized, subject to any conditions below.**
- □ **A combination of real, unaltered data and/or obscured/masked data is authorized, subject to any conditions below.**
- □ **Use of real, unaltered data is authorized, subject to any conditions below.**
- □ **Creation of a test dataset for long-term use is authorized, subject to any conditions below.**

CONDITIONS

- □ **Authorization is limited to the dataset as described in this questionnaire and accompanying documentation. Any proposed expansion of the dataset, in terms of the PII or the number or sources of records for the test data, must be approved by the ICE Privacy Office & IAD.**
- □ **All environments used for testing must have a valid Security Authorization (SA).**
- □ **Before testing begins, SA must be completed for these environments:**
- □ **Testing is authorized in a vendor environment that has a valid SA.**
- □ **Testing is not authorized in a vendor environment.**
- □ **Additional data fields must be obscured or removed as specified below:**
- □ **Upon completion of testing, test data must be destroyed and a certificate of destruction completed and returned to the ICE Privacy Office by <insert date> or □ no date specified.**
- □ **Authorization to use the test data described in the section above expires on <insert date>. Authorization must be renewed for testing to continue.**
- □ **The minimum level of suitability for test personnel is <insert suitability level>.**
- □ **Additional controls must be implemented, as follows:**
- □ **Other conditions:**

ICE OCIO IAD AND PRIVACY OFFICE COMMENTS