The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a new or updated Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002. This will also assess whether a new or updated System of Records Notice (SORN) is required under the Privacy Act of 1974.

Please complete this form and send it to the ICE Privacy & Records Office at (b)(7)(E)

Upon receipt, the ICE Privacy & Records Office will review this form. The DHS Privacy Office is the final adjudicator of the form. If a PIA is required, you will receive guidance on how to begin the PIA process.

Questions? Contact the ICE Privacy & Records Office at 202-732-3300 and ask to speak to a member of the Privacy Branch staff.

PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

SUMMARY INFORMATION

Project or Program Name:	Student and Exchange Visitor Information System (SEVIS)		
Component:	Immigration and Customs Enforcement (ICE)	**Office or Program:**	Student and Exchange Visitor Program (SEVP)
TAFISMA Name:	SEVIS SEVIS Modernization	**TAFISMA Number:**	(b)(7)(E)
Type of Project or Program:	IT System	**Project or program status:**	Modification

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	Student and Exchange Visitor Program (SEVP)	**Title:**	Unit Chief, Systems Management Unit
Phone:	(202) 904-(b)(6);(	**Email:**	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6);(b)(7)(C)		
Phone:	(202) 868-(b)(6);	**Email:**	(b)(6);(b)(7)(C)

ROUTING INFORMATION

Date submitted to Component Privacy Office:	September 19, 2017
Date submitted to DHS Privacy Office:	December 8, 2017
Date approved by DHS Privacy Office:	Click here to enter a date.

SPECIFIC PTA UPDATE QUESTIONS

1. Describe the changes and/or upgrades planned for this system that are triggering this PTA Update:

Please provide a general description of the changes or upgrades using non-technical language and highlighting any changes involving or affecting Personally Identifiable Information (PII).

(b)(5)

2. Project or Program status			
Date first developed:	**TBD**	**Date last updated:**	**TBD**
Scheduled deployment of changes/upgrades:	**October 30, 2017**	**Degree of confidence in schedule:**	☒ High ☐ Medium ☐ Low ☐ Deploy date is unknown at this time
Name of system change/upgrade (e.g., EARM v 3.0):		N/A	

3. Is this project a technology/system that relates solely to infrastructure? For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?	☐ Yes (Stop here. Submit PTA Update.) ☒ No (Continue with next question.)

4. Does the system currently contain PII about individuals, including ICE and DHS personnel, contractors, aliens, criminal suspects, or members of the public? (TAFISMA identifies which systems in the ICE inventory contain PII.)	☒ Yes ☐ No
5. Are the system changes/upgrades limited to "bug fixes" only?	☐ Yes (Stop here. Submit PTA Update.) ☒ No (Continue with next question.)

6. Do the changes/upgrades affect (either add or subtract) the types of individuals about whom the system collects, processes, or retains PII? *Please check all that apply.*

☒ No.

☐ Yes. Information about additional types of individuals will be added.

<Please describe the new types of individuals and the source of this information.>

☐ Yes. Information will no longer be collected from one or more types of individuals.

<Please describe.>

7. Do the changes/ upgrades pertain to Social Security Numbers (SSNs)?	☐ No. The project will continue to collect/use SSNs as before.
	☒ No. SSNs are not now and will not be collected or used (full or partial).
	☐ Yes. Check the applicable box below: ☐ The SSN will no longer be collected or used. ☐ Full SSNs will no longer be collected or used; instead only partial SSNs (last 4) will be used. ☐ SSNs will now be collected or used. Check which: ☐ Full ☐ Partial

8. <u>Other than the SSN</u>, do the changes/upgrades affect (either add or subtract) the PII that is collected, created, processed, or retained in the system? *Please check all that apply.*

☒ No.

☐ Yes. New types of data about individuals will be created or added.

<Please describe the data and its source.>

☐ Yes. Data previously collected about individuals will no longer be collected.

<Please describe the data.>

9. Do the changes/upgrades alter the way the PII is used, or change the reason we are maintaining it or operating the system generally?	☒ No ☐ Yes <Please describe.>

10. Do the changes/upgrades impact connections with other IT systems, either within or outside of ICE? For example, are system connections being added or terminated? Is the system being migrated from a stand-alone environment to the ICE network?	☐ No ☒ Yes (b)(5)

11. Do the changes/upgrades affect how or why data about individuals will be shared within ICE, within DHS, or outside of DHS? This would include an increase or decrease in the amount of data shared, or sharing with new partners, or adding categories of new system users.
Please check all that apply.

☒ No.

☐ Yes. Changes how or why data will be shared within ICE.

<Please describe the changes.>

☐ Yes. Changes how or why data will be shared within DHS.

<Please describe the data.>

☐ Yes. Changes how or why data will be shared outside of DHS.

<Please describe the changes.>

12. Do the changes/upgrades result in the system obtaining information from any new source?	☒ No ☐ Yes

13. Will the changes/upgrades add to the system new analytical capabilities or other tools that will analyze or use PII?	☒ No ☐ Yes
14. What is the date of the most recent ATO for the system?	7/19/2016
15. Will the system changes/upgrades require an update to the C&A?	☒ No ☐ Yes

16. What is the FIPS 199 determination for the as-is environment:	Confidentiality:	☐ Low ☒ Moderate ☐ High
	Integrity:	☐ Low ☒ Moderate ☐ High
	Availability:	☐ Low ☒ Moderate ☐ High
Will the FIPS 199 categorizations need to be updated due to the system changes/upgrades?	☒ No ☐ Yes	
If yes, identify the new (or expected) FIPS 199 categorization for the future state:	Confidentiality:	☐ Low ☐ Moderate ☐ High
	Integrity:	☐ Low ☐ Moderate ☐ High
	Availability:	☐ Low ☐ Moderate ☐ High

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Michelle Escobar
Date submitted to DHS Privacy Office:	December 8, 2017
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
(b)(5);(b)(7)(E)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6);(b)(7)(C)
Date approved by DHS Privacy Office:	December 14, 2017
PCTS Workflow Number:	(b)(6);(b)(7)

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA Update adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA Update sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required.
PIA:	PIA update is required. If covered by existing PIA, please list: forthcoming SEVP PIA
SORN:	System covered by existing SORN

	If covered by existing SORN, please list: DHS/ICE 001 Student and Exchange Visitor Information System, January 5, 2010, 75 FR 412

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

(b)(5)

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.

Page 819

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 820

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 821

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 822

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 823

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 824

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 825

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 826

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 827

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 828

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 829

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 830

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 831

Withheld pursuant to exemption

Non Responsive Record

of the Freedom of Information and Privacy Act

Page 832

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 833

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 834

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 835

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 836

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 837

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 838

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 839

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 840

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 841

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 842

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 843

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 844

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 845

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 846

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 847

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 848

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 849

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 850

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 851

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 852

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 853

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 854

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 855

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 856

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 857

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 858

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 859

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 860

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 861

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 862

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 863

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 864

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 865

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 866

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 867

Withheld pursuant to exemption

Non Responsive Record

of the Freedom of Information and Privacy Act

Page 868

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 869

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 870

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 871

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 872

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 873

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 874

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 875

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 876

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 877

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 878

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 879

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 880

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 881

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 882

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 883

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 884

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 885

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 886

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 887

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 888

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 889

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 690

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 691

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 692

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 693

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 694

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 695

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 696

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 697

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 698

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 699

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 900

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 901

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 902

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 903

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 904

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 905

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 906

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 907

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 908

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 909

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 910

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 911

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**ICE Cloud GSS**		
Component:	Immigration and Customs Enforcement (ICE)	**Office or Program:**	OCIO
Xacta FISMA Name (if applicable):	**ICE Cloud GSS**	**Xacta FISMA Number (if applicable):**	I(b)(7)(E)
Type of Project or Program:	**IT System**	**Project or program status:**	**Development**
Date first developed:	**October 1, 2016**	**Pilot launch date:**	**May 1, 2017**
Date of last PTA update	**N/A**	**Pilot end date:**	**N/A**
ATO Status (if applicable)	**In progress**	**ATO expiration date (if applicable):**	**N/A**

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	**OCIO/OPS/ASB**	**Title:**	ICE Cloud Broker
Phone:	**202-732**(b)(6);(b	**Email:**	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6);(b)(7)(C)		
Phone:	**202-732-1**(b)(6	**Email:**	(b)(6);(b)(7)(C)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
The ICE Cloud is a cloud based General Support System (GSS) that provides Infrastructure as a Service (b)(5);(b)(7)(E)

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☒ This program does not collect any personally identifiable information[2] ☐ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is 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. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4. What specific information about individuals is collected, generated or retained?	
(b)(5)	
4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
6. Does this project, program, or system connect, receive, or share PII with any	☒ No.

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

external (non-DHS) partners or systems?	☐ Yes. If yes, please list: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	N/A
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: N/A, does not collect PII ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☒ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6);(b)(7)(C)
Date submitted to Component Privacy Office:	**April 14, 2017**
Date submitted to DHS Privacy Office:	April 25, 2017
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
(b)(5)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6);(b)(7)(C)
PCTS Workflow Number:	
Date approved by DHS Privacy Office:	April 28, 2017
PTA Expiration Date	April 28, 2020

DESIGNATION

Privacy Sensitive System:	No If "no" PTA adjudication is complete.
Category of System:	Other If "other" is selected, please describe: Click here to enter text.
Determination:	☒ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

	☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

(b)(5);(b)(7)(E)

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a new or updated Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002. This will also assess whether a new or updated System of Records Notice (SORN) is required under the Privacy Act of 1974.

Please complete this form and send it to the ICE Privacy & Records Office at ICEPrivacy@ice.dhs.gov.

Upon receipt, the ICE Privacy & Records Office will review this form. The DHS Privacy Office is the final adjudicator of the form. If a PIA is required, you will receive guidance on how to begin the PIA process.

Questions? Contact the ICE Privacy & Records Office at 202-732-3300 and ask to speak to a member of the Privacy Branch staff.

PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

SUMMARY INFORMATION

Project or Program Name:	**ICE Cloud General Support System (ICE Cloud GSS)**		
Component:	Immigration and Customs Enforcement (ICE)	**Office or Program:**	OCIO
TAFISMA Name:	**ICE Cloud GSS**	**TAFISMA Number:**	(b)(7)(E)
Type of Project or Program:	IT System	**Project or program status:**	Operational

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	**OCIO/OPS/ASB**	**Title:**	ICE Cloud Broker
Phone:	**202-732-**(b)(6);(b	**Email:**	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6);(b)(7)(C)		
Phone:	**202-732-**(b)(6);	**Email:**	(b)(6);(b)(7)(C)

ROUTING INFORMATION

Date submitted to Component Privacy Office:	January 17, 2018
Date submitted to DHS Privacy Office:	Click here to enter a date.
Date approved by DHS Privacy Office:	Click here to enter a date.

SPECIFIC PTA UPDATE QUESTIONS

1. Describe the changes and/or upgrades planned for this system that are triggering this PTA Update: *Please provide a general description of the changes or upgrades using non-technical language and highlighting any changes involving or affecting Personally Identifiable Information (PII).*
P e A (b)(5);(b)(7)(E)

2. Project or Program status			
Date first developed:	**October 1, 2016**	**Date last updated:**	**N/A – hardware/software changes occur continuously**
Scheduled deployment of changes/upgrades:	**N/A**	**Degree of confidence in schedule:**	☐ High ☐ Medium ☐ Low ☒ Deploy date is unknown at this time
Name of system change/upgrade (e.g., EARM v 3.0):		The ICE Cloud GSS system boundary has extended to the Microsoft Azure Government Cloud	

3. Is this project a technology/system that relates solely to infrastructure? For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?	☐ Yes (Stop here. Submit PTA Update.) ☒ No (Continue with next question.)

4. Does the system currently contain PII about individuals, including ICE and DHS personnel, contractors, aliens, criminal suspects, or members of the public? (TAFISMA identifies which systems in the ICE inventory contain PII.)	☐ Yes ☒ No

5. Are the system changes/upgrades limited to "bug fixes" only?	☐ Yes (Stop here. Submit PTA Update.) ☒ No (Continue with next question.)

6. Do the changes/upgrades affect (either add or subtract) the types of individuals about whom the system collects, processes, or retains PII? *Please check all that apply.*

☒ No.

☐ Yes. Information about additional types of individuals will be added.

<Please describe the new types of individuals and the source of this information.>

☐ Yes. Information will no longer be collected from one or more types of individuals.

<Please describe.>

7. Do the changes/ upgrades pertain to Social Security Numbers (SSNs)?	☐ No. The project will continue to collect/use SSNs as before. ☒ No. SSNs are not now and will not be collected or used (full or partial). ☐ Yes. Check the applicable box below: ☐ The SSN will no longer be collected or used. ☐ Full SSNs will no longer be collected or used; instead only partial SSNs (last 4) will be used. ☐ SSNs will now be collected or used. Check which: ☐ Full ☐ Partial

8. <u>Other than the SSN</u>, do the changes/upgrades affect (either add or subtract) the PII that is collected, created, processed, or retained in the system? *Please check all that apply.*

☒ No.

☐ Yes. New types of data about individuals will be created or added.

<Please describe the data and its source.>
☐ Yes. Data previously collected about individuals will no longer be collected. <Please describe the data.>

9. Do the changes/upgrades alter the way the PII is used, or change the reason we are maintaining it or operating the system generally?	☒ No ☐ Yes <Please describe.>

10. Do the changes/upgrades impact connections with other IT systems, either within or outside of ICE? For example, are system connections being added or terminated? Is the system being migrated from a stand-alone environment to the ICE network?	☒ No ☐ Yes <Please describe the IT connections affected and how they are affected.>

11. Do the changes/upgrades affect how or why data about individuals will be shared within ICE, within DHS, or outside of DHS? This would include an increase or decrease in the amount of data shared, or sharing with new partners, or adding categories of new system users. *Please check all that apply.*
☒ No.
☐ Yes. Changes how or why data will be shared within ICE. <Please describe the changes.>
☐ Yes. Changes how or why data will be shared within DHS. <Please describe the data.>
☐ Yes. Changes how or why data will be shared outside of DHS.

<Please describe the changes.>

12. Do the changes/upgrades result in the system obtaining information from any new source?	☒ No ☐ Yes <Please describe.>
13. Will the changes/upgrades add to the system new analytical capabilities or other tools that will analyze or use PII?	☒ No ☐ Yes <Please describe.>
14. What is the date of the most recent ATO for the system?	January 8, 2018
15. Will the system changes/upgrades require an update to the C&A?	☒ No ☐ Yes

16. What is the FIPS 199 determination for the as-is environment:	Confidentiality:	☐ Low ☐ Moderate ☒ High
	Integrity:	☐ Low ☐ Moderate ☒ High
	Availability:	☐ Low ☐ Moderate ☒ High
Will the FIPS 199 categorizations need to be updated due to the system changes/upgrades?	☒ No ☐ Yes	
If yes, identify the new (or expected) FIPS 199 categorization for the future	Confidentiality:	☐ Low ☐ Moderate ☐ High

state:	Integrity:	☐ Low ☐ Moderate ☐ High
	Availability:	☐ Low ☐ Moderate ☐ High

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Click here to enter text.
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
Click here to enter text.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Click here to enter text.
Date approved by DHS Privacy Office:	Click here to enter a date.
PCTS Workflow Number:	Click here to enter text.

DESIGNATION

Privacy Sensitive System:	Choose an item. If "no" PTA Update adjudication is complete.
Category of System:	Choose an item. If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA Update sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	
Click here to enter text.	

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018
ORIGINATING OFFICE: FO:TO
SUPERSEDES: Directive 3340-049
REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 PURPOSE. To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 POLICY

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., an importation of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the functional equivalent of the border (FEB), or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

3 DEFINITIONS

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

4 AUTHORITY/REFERENCES. 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1225, 1357, and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country. *See, e.g.*, *United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior"). Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign. *See Boumelhem*, 339 F.3d at 423.

In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, such as electronic devices. *See, e.g.*, 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of

the United States from places outside thereof are liable to inspection and search by a Customs officer."). These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. This includes, among other things, the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting the United States"; "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP's broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

5 PROCEDURES

5.1 Border Searches

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

5.1.3 Basic Search. Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.4 Advanced Search. An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents. In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.

5.1.5 Searches of electronic devices will be documented in appropriate CBP systems, and advanced searches should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire advanced search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.6 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel office or the CBP Privacy Officer, as appropriate.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive.

5.3 Review and Handling of Passcode-Protected or Encrypted Information

5.3.1 Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

5.4 Detention and Review in Continuation of Border Search of Information

5.4.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

5.4.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned. Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without

impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.

5.4.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.4.2 Assistance

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

5.4.2.1 Technical Assistance. Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern. Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

5.4.2.3 Approvals for Seeking Assistance. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.4.2.4 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

5.4.2.5 When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, or his or her presence on a watch list.

When notification is made to the individual, the Officer will annotate the notification in CBP systems and on the Form 6051D.

5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

5.5 Retention and Sharing of Information Found in Border Searches

5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice. For example, information

collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.5.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is authorized by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. § 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

5.5.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.6 Reporting Requirements

5.6.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.6.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.6.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.7 Management Requirements

5.7.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.7.2 The appropriate CBP second-line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.7.3 The appropriate CBP second-line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another agency or entity.

5.7.4 The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of

information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

6 **MEASUREMENT.** CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 **AUDIT.** CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 **NO PRIVATE RIGHT CREATED.** This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 **REVIEW.** This Directive shall be reviewed and updated, as necessary, at least every three years.

10 **DISCLOSURE.** This Directive may be shared with the public.

11 **SUPERSEDES.** Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

Acting Commissioner