

## **Privacy Policy 2017-01 Questions & Answers**

### **U.S. Citizen Definitions**

#### **Who is a U.S. citizen?**

A person may become a U.S. citizen at birth, if:

- i. He or she was born in the United States or certain territories or outlying possessions of the United States, and subject to the jurisdiction of the United States; or
- ii. She or he had a parent or parents who were citizens at the time of your birth (if you were born abroad) and meet other requirements.

A person may become a U.S. citizen after birth, if:

- i. She or he applies for “derived” or “acquired” citizenship through parents, or
- ii. He or she applies for naturalization.

#### **Who is a lawful permanent resident?**

A person is a lawful permanent resident if he or she enjoys the status accorded to an individual who has been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with immigration laws, and that status has not changed.

#### **Who is an immigrant?**

A person who is an alien in the United States, except one legally admitted under specific non-immigrant categories as discussed below in response to question 14. Additionally, a person who has entered without inspection, an illegal alien, is also considered an immigrant.

#### **Who is a non-immigrant?**

A person who is an alien seeking temporary entry to the United States for a specific purpose. The alien must have a permanent residence abroad (for most classes of admission) and qualify for the nonimmigrant classification sought. The nonimmigrant classifications include: foreign government officials, visitors for business and for pleasure, aliens in transit through the United States, treaty traders and investors, students, international representatives, temporary workers and trainees, representatives of foreign information media, exchange visitors, fiancé(e)s of U.S. citizens, intracompany transferees, NATO officials, religious

workers, and some others. Most nonimmigrants can be accompanied or joined by spouses and unmarried minor (or dependent) children.

**1. Why is the Policy changing?**

- a. The Department of Homeland Security (DHS) is changing its policy regarding the extension of Privacy Act protections to all persons as directed by section 14 of Executive Order 13768, which states, that “[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.” Previously, DHS had provided the administrative protections of the Privacy Act to all persons, as permitted by regulatory guidance from the Office of Management and Budget. The policy of the current Administration is to grant Privacy Act protections only to those explicitly covered by the Privacy Act.

**2. What changes result from the new Policy?**

- a. Generally, the new policy clarifies that immigrants and non-immigrants may only obtain access to their records through the Freedom of Information Act and may not be granted amendment of their records upon request. The Executive Order limits the rights and protections of the Privacy Act, subject to applicable law, to U.S. citizens and lawful permanent residents. The new policy requires that decisions regarding the collection, maintenance, use, disclosure, retention, and disposal of information being held by DHS conform to an analysis consistent with the Fair Information Practice Principles, see questions 7 and 8.

**3. What changes to the analysis of records and information disclosure under the Freedom of Information Act result from the new Policy?**

- a. The new Policy does not change the analysis of records and information disclosure under the Freedom of Information Act (FOIA), an applicable law. Decisions to withhold information requested by third parties about immigrants and non-immigrants will be analyzed in accordance the FOIA exemptions at 5 U.S.C. § 552(b)(6) or (b)(7)(C), which balance the public’s right to know about government operations against the personal privacy interests of the subject. With respect to FOIA requests about oneself, an immigrant or non-immigrant will receive those records that are not exempt under the FOIA, just like any other person.

**4. What is the impact of the new Policy on the Judicial Redress Act?**

- a. The new Policy has no effect upon the Judicial Redress Act, an applicable law. The Judicial Redress Act provides that “covered persons,” who are citizens of covered foreign states, will have both administrative and judicial Privacy Act rights with respect to their information contained in “covered records,” which are law enforcement in nature. This means that certain foreign nationals, currently citizens of the majority of European Union states, may seek access or amendment of their covered records held and covered by a DHS System of Records Notice (SORN), or pursue judicial redress for access, amendment, or wrongful disclosure of such records. For more information see, <https://www.justice.gov/opcl/judicial-redress-act-2015>.

**5. What changes to the sharing or disclosure of information with the Congress result from the new Policy?**

- a. The new Policy does not change the requirements for sharing information in full in response to a request from the Chairperson of Congressional Committee asking upon behalf of the Committee regarding a matter within the jurisdiction of the Committee. Such a response is normally confidential for use in support of the Committee’s business and not a public disclosure. Similarly, the new Policy does not change how we respond to Congressional requests on behalf of constituents, who are U.S. citizens or lawful permanent residents, in that it is treated as a first-party Privacy Act request by consent of the constituent; nor does it change how we respond to Congressional requests on behalf of immigrants, non-immigrants, or other third parties (such as, state and local government, or the Congressperson asking in a personal capacity), in that it is treated as a Freedom of Information Act request.

**6. What changes to the sharing or disclosure of information with federal, state, and local law enforcement result from the new Policy?**

- a. The new Policy, subject to the Judicial Redress Act or confidentiality provisions provided by statute or regulation, permits the sharing of information about immigrants and non-immigrants with federal, state, and local law enforcement. The Policy requires that such sharing conform to an analysis based upon the Fair Information Practice Principles that demonstrates a consistent relationship between the purpose for collection of the information and intended use.

**7. What are the Fair Information Practice Principles (FIPPs)?**

- a. The Fair Information Practice Principles (FIPPs) are principles that were first promulgated by the Department of Health, Education, and Welfare in 1973 and have guided federal government information practices going forward. The concepts are integral to many privacy laws, including both the Privacy Act of 1974 and to the E-Government Act of 2002, which also governs agency use of new technology. The eight foundational principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. For a discussion see question 8.

**8. How do the FIPPs inform the use and protection of information by DHS?**

- a. The FIPPs inform the use and protection of information by DHS as follows:
  - i. **Transparency** requires that DHS give public notice to its actions to collect information (e.g., System of Records Notices and Privacy Impact Assessments, which are located on the DHS Privacy Office Website, and signage [see, [www.dhs.gov/privacy](http://www.dhs.gov/privacy).]);
  - ii. **Individual Participation** requires that, when appropriate, DHS involve the person in the decision whether or not to provide personal information to DHS (i.e., make a choice);
  - iii. **Purpose Specification** requires that DHS inform the public of its authority to collect the information that it seeks—in other words, say what information is sought, why it is being sought, and whether or not it's submission is voluntary;
  - iv. **Data Minimization** requires that DHS only seek to collect the information that it needs, based upon its authority and based upon the mission or operation that requires the information;
  - v. **Use Limitation** requires that DHS use the information that it collects in a manner compatible with the purpose and authority that permit the collection;
  - vi. **Data Quality and Integrity** require that DHS has means to ensure the accuracy of the information it collects, provides measures to maintain the data free from corruption, and allow for corrections to data that become inaccurate or stale;
  - vii. **Security** requires that DHS ensure its data systems are protected against intrusion, that user access is determined by mission assignments, and that remedial procedures exist to address the possibility of breach or data spills;
  - viii. **Accountability and Auditing** require that DHS maintains the integrity of its systems such that it may find, use, and report upon the data

residing in those systems, and so that it may allow for independent audits to verify the accuracy of its reporting and its satisfaction of the prior seven principles.

**9. What access to records is available to immigrants and non-immigrants?**

- a. Immigrants and non-immigrants may access their records through the Freedom of Information Act (FOIA). Any person, irrespective of immigration status, may file a FOIA request with DHS for information about him or herself that DHS has in its possession and systems; he or she is entitled to a response that details the search for information about the person and informs him or her whether or not the records about them are released in full, released with certain portions masked in accordance with exemptions under the FOIA, or withheld in full.

**10. May immigrants and non-immigrants amend their records, which are held by DHS?**

- a. Immigrants and non-immigrants may not request amendment of their records in accordance with the Privacy Act. DHS, however, as a matter of efficiency and accurate recordkeeping strives to keep all information in its possession current. When DHS becomes aware and is able to confirm that information in its possession is inaccurate or no longer relevant it may choose to update or dispose of such information in accordance with the terms of the Federal Records Act records disposition schedules that apply to the particular records under review.

**11. What impact does the new Policy have on immigrants and non-immigrants access to redress through the DHS Traveler Redress Inquiry Process (DHS TRIP)?**

- a. The new Policy has no impact upon an immigrant or non-immigrant's access to Redress through DHS TRIP. DHS TRIP provides traveler redress to all persons irrespective of immigration status. Individuals, including foreign nationals, or persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by DHS may submit a redress request through DHS TRIP. DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports, seaports and train stations, or at U.S. land borders. For more information see, [www.dhs.gov/trip](http://www.dhs.gov/trip).



U.S. Immigration  
and Customs  
Enforcement

MEMORANDUM FOR: Assistant Directors  
All Deputy Assistant Directors  
All Special Agents in Charge

FROM: Marcy M. Forman  
Director, Office of Investigations

MAR 5 2007

SUBJECT: Field Guidance on Handling Detained or Seized Electronic Media  
from Persons of National Security Interest at Ports of Entry

This memorandum provides guidance and clarifies responsibilities related to the detention or seizure of electronic media from persons of national security interest at Ports of Entry (POE), and serves as a reminder of current U.S. Immigration and Customs Enforcement (ICE) policies regarding the use of border search authority as it relates to electronic media. ICE's ability to exploit this media represents a unique opportunity to collect, analyze and disseminate valuable information that directly supports the missions of ICE and the Department of Homeland Security (DHS).

BORDER SEARCHES

In accordance with customs border search authorities, pursuant to section 1582 of Title 19, United States Code, ICE may conduct routine stops and searches of merchandise and persons at the U.S. border without any individualized suspicion. Additionally, pursuant to immigration authorities found in sections 1225 and 1357 of Title 8, United States Code, ICE may inspect all aliens who apply for admission; take and consider evidence concerning the privilege of any person to enter, pass through, or reside in the United States that is material or relevant to enforcement of immigration laws; and conduct a search without a warrant of any person and the personal effects in their possession when there is reasonable cause to suspect a basis for denying admission to the United States. The objective of a border search is generally twofold: (1) to inspect for merchandise being imported contrary to law; and (2) to obtain information or evidence relating to an individual's admissibility. ICE may detain or seize anything that may be evidence of a crime or indicates criminal activity. Computers, cellular phones, and other electronic media are considered closed containers with regard to border search authority and are subject to being opened and searched by ICE. Regardless of citizenship, all persons seeking admission to the United States, and their merchandise are subject to border search. There is no requirement that this search be conducted with the knowledge of the person possessing the electronic media.

ICE may review, copy, image, detain or seize, and disseminate electronic media if a violation of law is immediately evident, if further review by ICE is needed to make such a determination, or if technical assistance (e.g., translation services) is deemed necessary. Electronic media detained or seized during a border search shall not be retained by ICE longer than is necessary to determine its relevance to furthering the law enforcement mission of ICE. Any information deemed relevant will be evaluated periodically to determine its continuing significance.

Subsequent to a border search, ICE may share obtained information relating to national security with law enforcement and intelligence agencies. It is important to note that any electronic media obtained through border search authority must be searched by ICE and deemed to be of law enforcement or intelligence interest prior to any sharing with an outside agency. Pursuant to current authorities, law enforcement information may be exchanged between the law enforcement components of DHS and other local, state, Federal, and foreign law enforcement agencies in accordance with specific agreements and other legal authorities. All requests for information from the intelligence community must be coordinated with the ICE National Security Integration Center (NSIC).

#### ELECTRONIC MEDIA – PERSONS OF NATIONAL SECURITY INTEREST/CONCERN

Pursuant to existing referral agreements between ICE and U.S. Customs and Border Protection (CBP), all CBP interdiction matters related to terrorism or threats to national security are referred to ICE and the local Joint Terrorism Task Force (JTTF). CBP also notifies the National Targeting Center (NTC) and, through that venue, the ICE representative at the NTC will notify the ICE JTTF duty agent in the field to respond, as appropriate, per ICE policy. In most cases, the ICE JTTF duty agent will respond to the POE to interview the subject. An ICE JTTF duty agent and/or ICE Computer Forensics Agent (CFA) may conduct a cursory search of the subject's electronic media and detain or image the electronic media to conduct a more thorough examination. (NOTE: Electronic media that contains data or images that are obviously contraband should be seized in accordance with established procedures.)

In each case, the CFA (or ICE JTTF duty agent if no CFA is available) shall document the search and/or retention of information contained on the electronic media of persons of national security interest by posting a Significant Incident Report (SIR) in the Significant Event Notification System. When electronic media is physically detained, rather than merely making a forensic image of such media, that detention should be documented in the Seized Asset and Case Tracking System, as per existing ICE policy. The TECS seizure number should be referenced in the SIR.

Due to terrorist organizations' use of sophisticated measures (embedded documents/images, passwords, etc.), and routine need for translation services, the ICE JTTF duty agent may request additional technical assistance prior to determining if the electronic media contains contraband or evidence of a violation of law. In these cases, the agent should contact NSIC to arrange for additional technical assistance or review.

Questions regarding the search, detention and/or seizure of electronic media from persons of national security interest can be directed to Program Manager Richard Sabatini, ICE NSIC, at (202) 616-2192 or via email at [Richard.Sabatini@dhs.gov](mailto:Richard.Sabatini@dhs.gov).

Page 03 of 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 04 of 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 10 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 11 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act



Page 12 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 13 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 14 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 15 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 16 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 17 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 18 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act

Page 19 of 19

Withheld pursuant to exemption  
Referred to Another Agency/Component  
of the Freedom of Information and Privacy Act





## **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](http://www.dhs.gov/privacy), on DHSConnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	<b>Giant Oak Search Technology (GOST)</b>		
<b>Component:</b>	Immigration and Customs Enforcement (ICE)	<b>Office or Program:</b>	Homeland Security Investigations (HSI), National Security Investigations Division (NSID), and International Operations
<b>Xacta FISMA Name (if applicable):</b>	N/A	<b>Xacta FISMA Number (if applicable):</b>	N/A
<b>Type of Project or Program:</b>	IT System	<b>Project or program status:</b>	Existing
<b>Date first developed:</b>	N/A	<b>Pilot launch date:</b>	September 4, 2014
<b>Date of last PTA update</b>	N/A	<b>Pilot end date:</b>	Click here to enter a date.
<b>ATO Status (if applicable)</b>	In progress	<b>ATO expiration date (if applicable):</b>	<b>TBD</b>

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	(b)(6); (b)(7)(C)		
<b>Office:</b>	CTCEU	<b>Title:</b>	National Program Manager
<b>Phone:</b>	(703) 232-(b)(6); (b)(7)(C)	<b>Email:</b>	(b)(6); (b)(7)(C)@ice.dhs.gov

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	(b)(6); (b)(7)(C)		
<b>Phone:</b>	(703) 842-(b)(6); (b)(7)(C)	<b>Email:</b>	(b)(6); (b)(7)(C)@giantoak.com

### SPECIFIC PTA QUESTIONS



## **1. Reason for submitting the PTA: New PTA**

HSI NSID and International Operations identify and eliminate vulnerabilities in the nation's security through programs including the Counterterrorism and Criminal Exploitation Unit (CTCEU) and the Visa Security Program (VSP). The Office of Professional Responsibility (OPR) ensures the integrity and safety of the ICE workforce. CTCEU, OPR, and VSP utilize commercial vendor Giant Oak's off-the-shelf, web-based platform called Giant Oak Search Technology (GOST) to monitor publicly available information via open-source websites and publicly available social media accounts for investigative leads. Targets of investigation are non-US persons, but information regarding associates who may be US citizens or LPRs may be collected in the course of an investigation.

### **HSI Use**

CTCEU and VSP users (hereafter, HSI users) access GOST through the Giant Oak web portal. HSI users upload data schemas to the web portal as a CSV file containing 30-50 data points about persons of interest from HSI cases in Leadtrac. Available data fields include biographical information, contact information, college and course of study information

Using the data points included in the HSI data schemas, GOST searches the internet for publicly available information from open source and social media sites belonging to the subjects. GOST searches three types of datasets:

1. Open Source information: All information that would be searchable using public search engines.
2. Proprietary/Deep Web information: Information that at one time was publicly available, but was harvested by GOST and stored due to its determined importance to GOST searches and the likelihood that it would be de-indexed and therefore unsearchable in the future.
3. Paid data sources: Publicly available information collated by third party search engines, such as LexisNexis, ThomsonReuters, Transunion, and international news organizations. The ultimate list of subscriptions is proprietary to GOST and unknown to ICE. The sources of the information from those returns from third party search engines will be noted in GOST.

Social Media accounts and postings could appear in a search of any of the three types of data. Social media accounts retrieved include, but are not limited to: Facebook, Google+, LinkedIn, Pinterest, Tumblr, Instagram, VK, Flickr, Myspace, and Twitter. GOST does not use any social media account to access information. It also does not violate any site paywall restrictions or circumvent any social media account's privacy settings.

GOST returns its findings to the web portal, broken into five categories:

(b)(7)(E)



(b)(7)(E)

Once GOST has returned its search results to the Giant Oak web portal, HSI users review the information to determine whether the information returned pertains to the correct individual, and whether the information is of value. Users can also run reverse image searches of photographs found by GOST to determine if the same image is posted elsewhere on the internet. GOST also allows for a user to run a facial recognition algorithm on all images collected in a search for an individual to help determine if the individual is depicted in associated images. The facial recognition algorithm can only be conducted on images already returned by GOST for a particular subject.

Users will select relevant information in the results that will then automatically be added to a report that can be exported from the web portal. The act of selecting information by a user as valuable informs the GOST search algorithms for Ranking future searches.

CTCEU uses Giant Oak to assist the visa overstay/lead vetting process, primarily to discover location information of a subject, but also for evidence of criminal activity or national security concerns. CTCEU also monitors student visa holders to determine whether students have changed their field of study to a sensitive area that may have military applications or counterproliferation concerns, as defined by the Department of State. GOST is used as a monitoring tool, and CTCEU's open source team (OST) will manually search open source materials to exhaust leads prior to entering an individual into GOST. When GOST alerts CTCEU of new open source material that may be posted, OST will re-initiate checks against government systems and again manually search for additional open source information prior to entering information into LeadTrac. Subject information downloaded or documented in LeadTrac will additionally be stored in a secure Microsoft Access database located on a DHS shared drive for use in assigning tasks to OST analysts.

(b)(7) users parse out a subset of visa application data and upload this data to the Giant Oak web portal mentioned above. All information determined to be of value will be documented manually in (b)(7)(E). (b)(7)(E) can also refer to CTCEU for continuous monitoring of a subset of subjects (i.e., F, M, J, B1, and B2 visa applicants from pre-designated consular posts). CTCEU will use Giant Oak to engage in continuous evaluation of the subject. The vetting is confined to searches for evidence of criminal and national security concerns. CTCEU users will not actively vet these subjects, but will set threshold alerts within GOST.



Excluding ad hoc search results, which are removed on a weekly basis, information will be removed from the Giant Oak web portal when HSI determines that the individual to whom it pertains is no longer subject to analysis

HSI users may also export the search results, excluding photographs, to a CSV file. This CSV file cannot be downloaded, but may be burned onto a CD and then transferred to a LeadTrac-attributed computer. Photographs may separately be saved to a CD, and then transferred to a LeadTrac-attributed computer.

**OPR Use**

OPR uses GOST for purposes of situational awareness and protection of ICE property and personnel. Instead of searching for individuals through GOST, OPR sets search parameters based on keyword searches. OPR has determined a set of words that may imply violence toward ICE as well as names of ICE leaders or personnel determined to be under threat. GOST issues daily reports of posts that contain the pre-determined keywords. The daily reports are not saved within GOST, and OPR personnel do not have user accounts for GOST. Reports only contain a screenshot of the post that contained the keyword, to include the account name of the poster. That report is analyzed by OPR personnel and forwarded on to OPR’s investigative unit if it is determined that the threat is credible. OPR will store the credible reports on a shared drive. If any posts deemed to be credible lead to an investigation by OPR, they will upload the report to their case management system, U.S. Customs and Border Protection’s (CBP’s) Joint Integrity Case Management System (JICMS).

<p><b>2. Does this system employ any of the following technologies:</b></p> <p><i>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.</i></p>	<p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input checked="" type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal<sup>1</sup> (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</p>
---	--

<p><b>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</b></p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information<sup>2</sup></p>
--	---

<sup>1</sup> 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.

<sup>2</sup> 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.



<i>Please check all that apply.</i>	<input checked="" type="checkbox"/> Members of the public <input checked="" type="checkbox"/> DHS employees/contractors (list components): ICE <input checked="" type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
-------------------------------------	--

<b>4. What specific information about individuals is collected, generated or retained?</b>	
<b>Members of the Public:</b>	
<p>Information contained in the HSI data schemas that are uploaded to the Giant Oak web portal includes: name; date of birth; country of birth and country of citizenship; aliases information; affiliate and associate names, dates of birth, relation, countries, and occupations; vehicle and license plate information; driver's license or state identification number; LeadTrac number; social security number (SSN); address information; phone number; e-mail address; IP address; web identity (i.e. account name, social media handle); and college and course of study information. GOST's search results depend on the amount of information available on open-source and social media for each subject, but all results can be broken into five categories:</p> <ol style="list-style-type: none"> <li>1. Web locations at which information about the person of interest was found, including a short summary of the finding, an image of the site, and a link to the site;</li> <li>2. Links to open-source and social media accounts belonging to the person of interest;</li> <li>3. Images of the person of interest;</li> <li>4. Social Graph: a visualization of connections of family and known associates derived from a GOST search; and</li> <li>5. Location information, including addresses associated with the person of interest.</li> </ol>	
<b>ICE Employees/Contractors</b>	
GOST collects username and contact information from GOST users to allow for access and authorization to use the system.	
<b>4(a) Does the project, program, or system retrieve information by personal identifier?</b>	<input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: Data stored in GOST is retrievable by Name, LeadTrac ID number, immigration status, or assignee (ICE employee or contractor).
<b>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes.



<b>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</b>	Immigration and Nationality Act sections 328 and 329; U.S.A. PATRIOT Act of 2001, Public Law 107-56; the Border Security Act, Public Law 107-173; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53
<b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b>	CTCEU uses SSNs to ensure clarity in identity resolution of the subjects of investigation and their associates. The more certain CTCEU can be as to the actions and connections of the subjects of investigation, the more likely the investigation will result in a viable lead. CTCEU's primary focus is locating and tracking subjects of investigations, which is directly affected by the quality of identity resolution.
<b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b>  <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
<b>4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.</b>	
N/A	

<b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list:  GOST does not have a system-to-system connection with any system. Data elements used for GOST searches are derived from LeadTrac and (b)(7)(F)- (b)(7)(E) Investigative information obtained
--	--

<sup>3</sup> 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.

<sup>4</sup> 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.



	from GOST searches is manually uploaded to LeadTrac, JICMS, and (b)(7)(E)
<b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</b>	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:
<b>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</b>	Please describe applicable information sharing governance in place:  N/A.
<b>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?</b>	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:
<b>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?</b>	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: Information generated through GOST will be manually uploaded to LeadTrac and (b)(7)(E) (b)(7)(E) and any disclosures would occur from LeadTrac/(b)(7)(E) rather than GOST. <input type="checkbox"/> Yes. In what format is the accounting maintained:
<b>9. Is there a FIPS 199 determination?<sup>4</sup></b>	<input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:  Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Integrity: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Availability:

<sup>4</sup> 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.





	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	--

## PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b)(6), (b)(7)(C)
<b>Date submitted to Component Privacy Office:</b>	<b>February 19, 2019</b>
<b>Date submitted to DHS Privacy Office:</b>	May 8, 2019
<b>Component Privacy Office Recommendation:</b>	
<i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
<p>GOST is a privacy sensitive system in that it collects, uses, and maintains PII from members of the public. All searches executed by GOST are in compliance with the ICE Criminal and Administrative Immigration Law Enforcement SMOUT executed 12/5/2016. ICE recommends updating this SMOUT to reflect the addition of the LeadTrac PIA and SORN in its operational use, as well as clarifying OPR's routine use of social media for officer safety.</p> <p>The forthcoming ICE Social Media PIA will cover the privacy risks inherent in using GOST. Interim coverage is provided by:</p> <ul style="list-style-type: none"> <li>DHS/ICE/PIA-044 LeadTrac PIA, which assesses the privacy risks of collecting open source data for investigative leads</li> <li>DHS/CBP/PIA-044 Joint Integrity Case Management System, which discusses the inclusion of open source data in the system.</li> <li>DHS/ICE/PIA-011(a) Visa Security Program Tracking System -Network Version 2.0 covers the system collecting open source information in VSP's vetting process.</li> </ul> <p>The information input into GOST comes from HSI's investigative case files. Results derived from GOST are evidentiary in nature and used in ICE investigations. ICE recommends</p> <ul style="list-style-type: none"> <li>Current coverage under DHS/ICE-009 – External Investigations SORN, as all data collected and maintained is for the purpose of supporting investigations of criminal activity. ICE will include in its next update that open source information and social media posts as categories of records for further transparency.</li> <li>Coverage for information entered into Leadtrac under DHS/ICE-015 LeadTrac SORN</li> </ul>	



- Coverage for information entered into (b)(7)(E) under (b)(7)(E) (b)(7)(E) SORN, which covers public records obtained during a visa security review.

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

<b>DHS Privacy Office Reviewer:</b>	(b)(6), (b)(7)(C)
<b>PCTS Workflow Number:</b>	<b>1180593</b>
<b>Date approved by DHS Privacy Office:</b>	June 12, 2019
<b>PTA Expiration Date</b>	June 12, 2022

**DESIGNATION**

<b>Privacy Sensitive System:</b>	Yes If “no” PTA adjudication is complete.
<b>Category of System:</b>	IT System If “other” is selected, please describe: Click here to enter text.
<b>Determination:</b>	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
<b>PIA:</b>	<b>System covered by existing PIA</b> If covered by existing PIA, please list: (b)(7)(E) Forthcoming ICE Social Media PIA; DHS/ICE/PIA-044 LeadTrac and forthcoming appendix updates; DHS/ICE/PIA-011(a) Visa Security Program Tracking System -Network Version 2.0; DHS/CBP/PIA-044 JICMS



<b>SORN:</b>	<p>SORN update is required.</p> <p>If covered by existing SORN, please list: Forthcoming update to DHS/ICE-009 External Investigations January 5, 2010 75 FR 404;  DHS/ICE-012 (b)(7)(E) September 30, 2009 74 FR 50228;  DHS/ICE-015 LeadTrac System of Records, August 9, 2016, 81 FR 52700</p>
<p><b>DHS Privacy Office Comments:</b>  Please describe rationale for privacy compliance determination above.</p>	
<p>ICE is submitting this PTA to discuss the Counterterrorism and Criminal Exploitation Unit (CTCEU), (b)(7)(E) and Office of Professional Responsibility (OPR) use of Giant Oak Search Technology (GOST). CTCEU and (b)(7)(E) GOST to monitor publicly available information via open-source websites and publicly available social media accounts for investigative leads. Targets of investigation are non-U.S. persons, but information regarding associates who may be U.S. citizens or LPRs may be collected in the course of an investigation.</p> <p>OPR uses GOST for purposes of situational awareness and protection of ICE property and personnel. Instead of searching for individuals through GOST, OPR sets search parameters based on keyword searches. GOST issues daily reports of posts that contain the pre-determined keywords. The daily reports are not saved within GOST, and OPR personnel do not have user accounts for GOST.</p> <p>The DHS Privacy Office finds this is a privacy sensitive system, requiring PIA coverage. ICE is currently drafting a Social Media PIA to cover ICE uses of open source and social media information, and that PIA will include discussion of GOST and should also include specific discussion of the use of facial recognition in searching. Coverage will also be provided by the forthcoming PATRIOT PIA, and forthcoming updates to the appendices of DHS/ICE/PIA-044 LeadTrac.</p> <p>SORN coverage is also required, as information is retrieved by identifier. ICE is currently updating DHS/ICE-009 External Investigations, and should include social media and open source information. Coverage for information entered into LeadTrac is provided by DHS/ICE-015 LeadTrac, and coverage for information entered into (b)(7)(E) is provided by DHS/ICE-012 (b)(7)(E)</p> <p>ICE should submit an updated the ICE Criminal and Administrative Immigration Law Enforcement SMOUT, and PRIV recommends submission of a separate SMOUT for OPR’s situational awareness use of social media.</p> <p>This PTA will expire in one year. Two additional years of coverage will be provided upon completion of the required PIA and SORN updates.</p>	
<p>After a review of recently published documents, PRIV finds that coverage is provided by the recently published (b)(7)(E) DHS/ICE-009 External Investigations is in the process of being updated to include social media and is near completion, and ICE has recently submitted appendix updates to the LeadTrac PIA.</p> <p>More comprehensive coverage for ICE use of social media will continue to be provided by the forthcoming ICE social media PIA. <b>The DHS/ICE/PIA-054 ICE Use of Facial Recognition Services was recently published which outlines the use of facial recognition services (FRS) that require the collection, maintenance, and use of PII.</b></p>	



**Homeland  
Security**

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717, [pia@dhs.gov](mailto:pia@dhs.gov)  
[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 12 of 12*

**LETTER OF COOPERATION**

**Between the Federal Bureau of Investigation of the  
Department of Justice of the United States of America  
And the Department of Homeland Security of the United States of America  
And the Royal Brunei Police Force of the Prime Minister's Office**

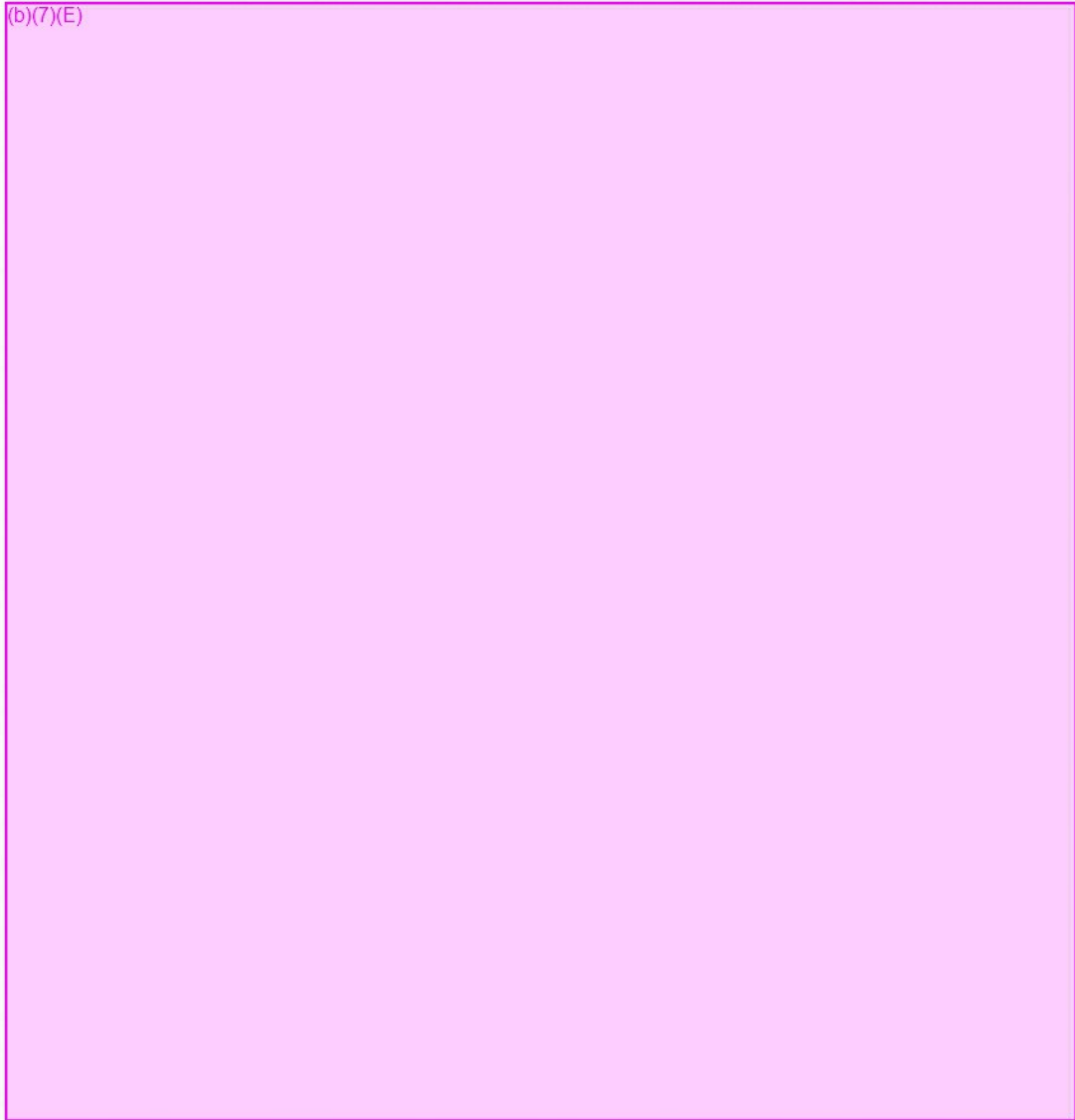
(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



**Federal Bureau of Investigation**  
of the  
**Department of Justice**  
of the  
**United States of America**

**The Royal Brunei Police Force**  
of the  
**Prime Minister's Office**

and the

**Department of Homeland Security**  
of the  
**United States of America**

(b)(6); (b)(7)(C)

Signature

14 Jan 2013

Date

Signature

14/01/2013

Date



MEMORANDUM OF UNDERSTANDING

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY

AND

THE NATIONAL COUNTERTERRORISM CENTER

REGARDING

THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (U//FOUO)

1. (U) INTRODUCTION AND PURPOSE.

(U//FOUO) The U.S. Department of Homeland Security (DHS), through the National Protection and Program Directorate's (NPPD) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, and the National Counterterrorism Center (NCTC), hereinafter collectively referred to as the "Parties," have entered into this Memorandum of Understanding ("MOU" or "Agreement") to govern the information sharing, use and safeguarding of data within the Arrival and Departure Information System (ADIS) for the purpose of identifying information within ADIS as terrorism information.

2. (U) BACKGROUND.

(U//FOUO) Pursuant to the National Security Act of 1947, as amended, NCTC "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." 50 U.S.C. § 404o. In order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 25, 2005), which provides that the head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the head of each other agency that has counterterrorism functions.

(U//FOUO) NCTC maintains the (b)(7)(E) which serves as the central knowledge bank for all-source information on international terrorist identities for use by the Intelligence Community (IC), law enforcement community, and others.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U//FOUO) At NCTC, the Information and Incidents Analysis Group is responsible for, among other things, identifying terrorism information from data sets that may also include non-terrorism information to facilitate the identification of known or suspected terrorists and terrorist activities. The Terrorist Travel Branch provides all-source strategic analysis on how terrorists circumvent border controls and provides analytic support to U.S. visitor screening. The Pursuit Group was stood up after the December 25<sup>th</sup>, 2009 terrorist attempt to identify and examine, as early as possible, leads that could become terrorist threats to the Homeland and US interests abroad.

(U//FOUO) ADIS is a system for the storage and use of biographic, biometric indicator, and encounter data on aliens who have applied for entry, entered, or departed the United States. ADIS consolidates information from various sources such as U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services, to provide a repository of data held by DHS for pre-entry, entry, status management, and exit tracking of immigrants and non-immigrants. Its primary use is to facilitate the investigation of subjects of interest who may have violated their immigration status by remaining in the United States beyond their authorized stays. The information is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies.

(U//FOUO) ADIS is described in a published Privacy Act System of Record Notice (SORN) 72 FR 47057 (August 22, 2007). Disclosure of ADIS information pursuant to this MOU is authorized by law and as contemplated under the routine uses set for that SORN; specifically ADIS Data is being provided to NCTC to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks.

(U//FOUO) ADIS includes data collected by DHS pursuant to 8 U.S.C. §§ 1103-1104, 1158, 1187(a)(11), (h)(3), 1201, 1202, 1221, 1225, 1324, 1357, 1360, 1365a, 1365a note, 1365b, 1372, 1379, 1732; 8 C.F.R. Part 204, § 215.8, 217.5, 231.1, 235.1; 44 U.S.C. § 44909; 19 CFR §§ 122.49a-c; 122.75a-b. The majority of ADIS Data has no nexus to terrorism and is not terrorism information as defined in both section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, and Executive Order 13388. As described in the ADIS SORN, DHS provides visitors to the United States with certain administrative privacy protections and safeguards of the Privacy Act.

(U//FOUO) The Parties are members of the Information Sharing Environment (ISE). Each Party will conduct its activities under this MOU in accordance with its own ISE Privacy and Civil Liberties Protection Policy.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

3. (U) DEFINITIONS.

(U) As used in this Agreement, the following terms will have the following meanings:

- A. (U) ADIS Data: For the purposes of this MOU, includes biographic, biometric indicator, and encounter data on aliens who have applied for entry, entered, or departed the United States as defined by the specific data fields identified in Appendix A.
- B. (U) ADIS Record: ADIS Data associated with an individual.
- C. (U) Alien: Any person not a citizen or national of the United States. 8 U.S.C. § 1101(a)(3).
- D. (U) Asylum-seeker: an asylum seeker is an alien at a U.S. port of entry or who has already entered the United States who seeks protection under 8 U.S.C. §§ 1158 or 1231(b)(3) or 8 C.F.R. §§ 208.16 or 208.17. This includes individuals who have been referred to USCIS for a credible fear interview under 8 U.S.C. § 1225 or a reasonable fear interview under 8 C.F.R. § 208.31.
- E. (U) Asylee: An alien who has been granted asylum under 8 U.S.C. § 1158.
- F. (U) Lawful Permanent Resident: An alien who has obtained the status of having been lawfully accorded the privilege of residing permanently in the United States, such status not having changed. 8 U.S.C. § 1101(a)(20).
- G. (U) Personally Identifiable Information: Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual. This definition applies regardless of whether the individual is a U.S. citizen, lawful permanent resident, or visitor to the U.S.
- H. (U) Refugee: An alien who has been granted refugee status under 8 U.S.C. § 1157.
- I. (U) Special Protected Classes: For the purposes of this MOU, the term special protected classes refers to classes of aliens for which there are additional statutory, regulatory, or policy protections. Data pertaining to these classes of aliens may have handling or use requirements different from U.S. Person data or other alien data. The classes of aliens covered under this definition include asylum-seekers; asylees; refugees; S, T, and U visa holders; individuals covered under the Violence Against Women Act; aliens with Temporary Protected Status; Legalization and Seasonal Agricultural Worker program applicants; and other individuals so designated by the U.S. Citizenship and Immigration Services.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- J. (U) Terrorism Information: Refers to information within the scope of the “information sharing environment,” as that term is defined in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L.108-458, § 1016(a)(3); 6 U.S.C. § 485(a)(3), as amended, and includes the definition of “terrorism information” reflected in the Memorandum of Understanding “Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing” (March 4, 2003).
- K. (U) U. S. Person: As defined in 50 U.S.C. § 1801(i), includes, for purposes of this MOU, a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8). The primary focus of U.S. Person information exchanged under this MOU will be ADIS information concerning aliens lawfully admitted for permanent residence.

**4. (U) AUTHORITY.**

(U) The information sharing and enhanced cooperation among the Parties to this Agreement is authorized under and complies with the provisions of:

- A. (U) Homeland Security Act of 2002, as amended;
- B. (U) 50 U.S.C. §§ 404o, 404o note, and 501 note;
- C. (U) Privacy Act of 1974, as amended (5 U.S.C. § 552a);
- D. (U) 8 U.S.C. §§ 1103-1104, 1202, 1365a, 1365a note, 1365b, and 1379;
- E. (U) The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001;
- F. (U) Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended;
- G. (U) National Security Act of 1947, as amended;
- H. (U) Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007; 8 U.S.C. § 1187(a)(11), (h)(3); 8 C.F.R. § 217.5.
- I. (U) 8 U.S.C. §1367(a)(2) (Information Relating to Violence Against Women Act (VAWA) Claimants and U and T visa holders).
- J. (U) 8 U.S.C. §1255a(c)(4)-(5) and 8 C.F.R. §§ 210.2(e), 245a.2(t), 245a.3(n), and 245a.21 (Information related to Legalization/Seasonal Agricultural Worker claims);
- K. (U) 8 U.S.C. §1254a(c)(6) and 8 C.F.R. § 244.16 (Information Relating to Temporary Protected Status claims);

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- L. (U) Executive Order 12333, as amended;
- M. (U) Executive Order 13231, 66 Fed. Reg. 53063, Oct. 16, 2001, as amended;
- N. (U) Executive Order 13354, National Counterterrorism Center, 69 Fed. Reg. 53589, dated Aug. 27, 2004;
- O. (U) Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, 70 Fed. Reg. 62023, dated Oct. 25, 2005;
- P. (U) HSPDs-2, -6, and -11, all of which direct the strengthening of screening and analysis programs to detect, identify, and interdict individuals entering or already within the United States who pose a terrorist threat to national security;
- Q. (U) 8 C.F.R. § 208.6;
- R. (U) Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and DHS Concerning Information Sharing, dated March 4, 2003;
- S. (U) Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism, as amended by Addendum B, effective Jan. 2007;
- T. (U) Memorandum from the Secretary of DHS, Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies, dated April 18, 2007;
- U. (U) Routine use "H" of the Arrival and Departure Information System (ADIS) System of Records Notice, 72 Federal Register 47057, dated August 22, 2007;
- V. (U) The DHS Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy, Privacy and Civil Liberties Guidance Memorandum 2009-01;
- W. (U) The NCTC Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy
- X. (U) ODNI Instruction No. 2006-3, Protection of Privacy and Civil Liberties, 22 February 2006.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**5. (U) RESPONSIBILITIES.**

(U//FOUO) The following roles and responsibilities have been defined for each of the parties to this MOU.

**A. (U//FOUO) DATA SENSITIVITY.**

(U//FOUO) DHS considers the data transmitted to NCTC's Information and Incidents Analysis Group, the Terrorist Travel Branch and the Pursuit Group as Unclassified//For Official Use Only, abbreviated as "U//FOUO." Specific technical and security details are set forth in the SAFEGUARDS section, below.

(U//FOUO) NCTC's Information and Incidents Analysis Group, the Terrorist Travel Branch and the Pursuit Group will transmit data and other responsive information back to DHS under this MOU in accordance with NCTC policies and procedures concerning the handling of sensitive information, including, as appropriate, applicable rules governing the safeguarding of sensitive unclassified information and Classified National Security information. The fact of classification, alone, shall not be a prohibition upon sharing with appropriately cleared DHS personnel.

**B. (U) DELIVERY OF DATA.**

(U//FOUO) Data Sets: DHS will deliver appropriate ADIS Data, as identified and in accordance with specific procedures described in Appendix A (along with applicable reference/lookup tables and non-PII metadata to support processing of the data), in two separate ADIS Data Sets:

(U//FOUO) Data Set 1: All ADIS Records, except those associated with individuals known by DHS/US-VISIT to be U.S. Persons, refugees, and asylum seekers.

(U//FOUO) Data Set 2: ADIS Records associated with individuals known by DHS/US-VISIT to be U.S. Persons, refugees, and asylum seekers.

(U//FOUO) These Data Sets will be delivered according to the terms outlined in Appendix B, until an automated transfer method is established.

(U//FOUO) NCTC will process and handle ADIS Records associated with U.S. Persons, Asylum Seekers and Refugees (Data Set 2) separately from all other ADIS Records (Data Set 1), and in accordance with separate, additional handling and retention rules.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U//FOUO) Treatment of U.S. Person/Asylum/Refugee Information: NCTC will process ADIS Records associated with known U.S. Persons, asylum seekers, and refugees within 30 calendar days of receipt from DHS to determine whether a nexus to terrorism exists. This process will be audited as required in Section M of this Agreement. NCTC will review, retain, and disseminate ADIS records associated with known U.S. Persons, refugees and asylum seekers in accordance with procedures approved for NCTC by the Attorney General in accordance with section 2.3 of Executive Order 12333 and any additional terms specified in addendum D.

(U//FOUO) Special Class Restrictions: No ADIS Records or other ADIS Data pertaining to special protected class individuals covered under 8 U.S.C. 1367 (VAWA, "T" and "U" visa) will be provided to NCTC under this agreement.

(U//FOUO) Technical Updates: As soon as practicable, but no later than 180 days of the effective date of this MOU, both Parties will initiate discussions to develop a capability to transmit the ADIS data addressed in this agreement in an automated manner. Subsequently agreed to procedures for such automated transmission will be outlined in documentation, as appropriate, and properly appended to this MOU prior to the implementation of automated data transfers.

C. (U) USE.

(U//FOUO) Authorized Uses: NCTC's Information and Incidents Analysis Group in coordination with the NCTC Terrorist Travel Branch and the Pursuit Group shall use ADIS Data delivered pursuant to section B, above, for three purposes only:

1. (U//FOUO) To identify terrorism information within ADIS Records, in support of screening activities and the enhancement or enrichment of associated or related records already in (b)(7)(E) and
2. (U//FOUO) To facilitate recurrent vetting based on new threat-based information to detect and prevent emergent terrorist threats.
3. (U//FOUO) To identify and confirm travel information of known or suspected terrorist that would be used to either supplement (b)(7)(C) records or, where appropriate, buttress intelligence assessments that would be shared with DHS.

(U//FOUO) Notification, Marking, and Coordination Requirements: NCTC's Information and Incidents Analysis Group in coordination with the NCTC Terrorist Travel Branch and the Pursuit Group may use any ADIS Record it identifies as containing terrorism information in any manner consistent with its authorities and in accordance with applicable policies and procedures, including those reflected elsewhere in this MOU.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U//FOUO) NCTC will notify DHS, through appropriate channels, of all ADIS Records identified as possibly containing terrorism information and otherwise having possible links to terrorism. Specifically, NCTC must notify and coordinate with DHS in a timely manner the validation of potential matches of ADIS Data to terrorism information. NCTC will immediately notify the DHS Office of Intelligence and Analysis (I&A) of confirmed/validated matches of ADIS information to terrorism information, consistent with the existing protocols and procedures agreed to between the Parties, so that I&A may inform and facilitate the appropriate DHS operational response. Finally, NCTC will provide DHS a copy of all intelligence reports it creates and disseminates when related to, based on, or otherwise including information derived from ADIS Data provided by DHS.

(U//FOUO) NCTC shall appropriately mark the origin and source of ADIS Data incorporated into intelligence reports, (b)(7)(E) or other authorized reports or databases, as derived from the DHS ADIS. Notwithstanding any finding by NCTC, DHS reserves the right to make independent findings regarding ADIS Records or other records originating from DHS data holdings, and to take appropriate actions based on those independent findings. At all times, DHS will undertake efforts mindful of and in accordance with its obligations to protect sensitive sources and methods.

(U//FOUO) NCTC may only utilize ADIS Data that does not constitute terrorism information received under this MOU for the purposes authorized by this MOU.

**D. (U) RECORDS RETENTION.**

(U//FOUO) Terrorism Information: NCTC may retain an ADIS Record containing terrorism information, in accordance with NCTC authorities and policies, applicable law, and the terms of this MOU.

(U//FOUO) Non-Terrorism Information: NCTC may retain an ADIS Record not containing terrorism information and not associated with U.S. Persons, refugees or asylees only in accordance with the ADIS System of Records Notice (SORN) and the National Archives and Records Administration retention schedule for ADIS, which is presently 75 years. NCTC will review, retain, and disseminate ADIS records associated with known U.S. Persons, refugees and asylum seekers in accordance with procedures approved for NCTC by the Attorney General in accordance with section 2.3 of Executive Order 12333 and attached addendum D.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U//FOUO) Changes in Status: The Parties will create and implement a process to identify ADIS Records provided to NCTC that concern an individual who has changed in status from a non-U.S. Person to a U.S. Person (e.g., when an alien adjusts status to become an LPR), until such time as a system-to-system connection shall automatically update changes in status. Upon receiving notification that an individual has become a U.S. Person, NCTC will review, retain and disseminate the ADIS record associated with the known U.S. Person in accordance with procedures approved for NCTC by the Attorney General in accordance with section 2.3 of Executive Order 12333 and attached addendum D.

E. (U) DISSEMINATION.

(U//FOUO) Terrorism Information: NCTC may disseminate ADIS Records identified as terrorism information consistent with its authorities, without the need for DHS approval, provided such dissemination is to other appropriate U.S. government authorities and for counterterrorism purposes. NCTC shall maintain a copy of the information that was disseminated, to whom, and the purpose for the dissemination in accordance with applicable audit requirements pursuant to Section M, Auditing.

(U//FOUO) Protection of Asylum and Refugee Applicants: In accordance with the April 18, 2007, Memorandum from the Secretary of the Department of Homeland Security entitled, "Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies," due to the potential risk of harm from foreign governments to Asylees and Refugees, NCTC may not further disseminate asylum- or refugee-related information it receives from DHS (to include the fact that an individual is an Asylee or Refugee) to another agency without the prior approval of DHS, or to any foreign government agency, official, representative, employee, agent, or contractor without the specific authorization of the Secretary, Deputy Secretary, or other DHS official to whom disclosure authority under 8 C.F.R. § 208.6(a) has been delegated. To that end, NCTC will coordinate with DHS prior to including asylum- or refugee-related information in (b)(7)(E) Upon request to put information regarding an asylee or refugee in (b)(7)(E) DHS will get back to NCTC within 10 working days.

(U//FOUO) Non-Terrorism Information: NCTC may not share information derived from an ADIS Record that it does not identify as containing terrorism information.

(U//FOUO) If there is a question on ADIS information and its relationship to terrorism, NCTC may request in writing that DHS allow the provision of that information to other IC agencies for further judgment. Upon such a request, DHS will get back to NCTC within 10 working days.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U//FOUO) Control of Records: DHS will be deemed to have retained control over ADIS Records provided to NCTC under this MOU for the purposes of the Freedom of Information Act, Privacy Act, and any other legal proceeding. Any requests or demands for information received by NCTC will be referred immediately to DHS for processing by or otherwise in coordination with the appropriate DHS Component(s) or element(s) with whom the requested data originated.

F. (U) SUPPORT.

(U//FOUO) DHS, through US-VISIT, will regularly provide NCTC's Information and Incidents Analysis Group with successor data to ADIS Data should the format of data collection be changed or modified, provided such transmission continues to be authorized by law and regulation.

G. (U) SAFEGUARDS.

(U//FOUO) The Parties agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the information shared under this Agreement against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification or deletion. Neither Party will use data provided to it under this MOU in affidavits, subpoenas, or submissions in legal, judicial, or administrative proceedings unless authorized by the providing Party.

H. (U) TRAINING.

(U//FOUO) The Parties shall be appropriately trained regarding the proper treatment of personally identifiable information (PII) and proper care of the information systems to ensure the overall safeguarding of the information, in addition to applicable U.S. Person rules. Each Party will ensure that its employees, including contractors with access to any of the other Party's data, have completed privacy training on the handling of PII.

(U//FOUO) DHS/US-VISIT will provide training to NCTC personnel on proper interpretation of the data contained in ADIS and on proper treatment of data from certain categories which require special handling, such as asylum, refugee, and U.S. Person data.

I. (U) PRIVACY.

(U//FOUO) The collection, use, disclosure, and retention of PII shall be limited to that which is necessary for purposes of the Parties as set forth in this Agreement. PII shall be protected by administrative, technical and physical safeguards appropriate to the sensitivity of the information. PII will only be disclosed to authorized individuals with a need to know and only for uses that are consistent with the stated purposes under this Agreement and for which the information was originally collected.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

J. (U) CORRECTION AND REDRESS.

(U//FOUO) PII shared and maintained under this MOU shall, to the extent feasible, be as accurate, complete, and up-to-date as necessary for the purposes identified in this agreement. The Parties shall cooperate with each other in this regard. NCTC will, in a timely manner, take appropriate action with regard to any request made by DHS for additions, changes, deletions, or corrections of PII. In addition, NCTC will, in a timely manner, notify DHS of any data errors that it discovers.

(U//FOUO) NCTC shall maintain an ability to locate and update specific ADIS Records identified by DHS as requiring correction. Additionally, NCTC shall correct any disseminated information based on ADIS Data that is later deemed to be erroneous. Location and correction of records shall be accomplished in not more than 14 calendar days and NCTC will provide written confirmation to DHS of the corrections made.

K. (U) COOPERATION/DECONFLICTION.

(U) The Parties shall work together to the greatest extent possible to achieve the maximum preventative, preemptive, and disruptive effect on potential threats, including coordinating simultaneous and complementary activities when appropriate. The parties further agree to coordinate operational activities to the greatest possible extent when based upon the information exchanged pursuant to this MOU. Specifically, each party shall take all reasonable steps to ensure coordination and de-confliction of homeland security-related law enforcement or intelligence, or other activities under its authority, with such activities of the other party.

(U//FOUO) Where the Parties have a mutual interest based on information shared pursuant to this Agreement, the Parties will coordinate with each other to determine the appropriate course of action. In such matters, unless there are exigent circumstances requiring immediate action, NCTC will verify information and coordinate with DHS before taking action on leads or disseminating intelligence products developed as a result of information shared pursuant to this Agreement. In the event of exigent circumstances, NCTC will notify the designated CBP representative as soon as possible and no longer than 24 hours after taking the action.

L. (U) REPORTING AND COMPLIANCE.

(U) Each organization will report privacy or security incidents in accordance with their own privacy or security procedures. However, the Parties must notify each other immediately by telephone and e-mail once a Party becomes aware of any breach in security, especially those that result in unauthorized use or disclosure of any PII or other information shared under this MOU.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U//FOUO) NCTC must notify the US-VISIT Information System Security Manager (ISSM) and Privacy Officer immediately by telephone at (202) 298-5200 and via e-mail at us-visitbreachnotification@dhs.gov and usvisitprivacyofficer@dhs.gov. US-VISIT must notify NCTC, Information Sharing Policy Office by telephone at (703) 275-2708 or the NCTC Legal Office at 571-280-5644.

(U) NCTC must perform system audits to identify any security breaches and ensure that any PII is shared consistent with applicable laws, regulations, and guidelines. Where a privacy or security incident, including the unauthorized disclosure of information specifically involves data related to asylum seekers, refugee applicants, Asylees, or Refugees, NCTC must notify USCIS, ICE, and the Chief Privacy Officer, within 24 hours after becoming aware of the incident.

(U) To further safeguard the privacy, security, confidentiality, integrity and availability of the connected systems and the information they store, process and transmit, the Parties agree to maintain records of information provided to each other under the terms of this Agreement consistent with applicable law, as well as established records retention policies and guidance of the respective Parties.

(U) The Parties shall designate responsible officials to meet annually, or at the request of any Party, to discuss and review the implementation of this MOU. Any disagreement over the implementation of this MOU shall be resolved in accordance with Section 10 Issue Resolution, below.

(U) NCTC must develop methods to track and report results from the use of ADIS data to DHS on a quarterly basis. The content of these reports will be detailed in this MOU's Appendix C.

M. (U) AUDITING.

(U) Both Parties shall work together to develop review standards to conduct audits of their compliance with the privacy, redress, and security requirements set forth in this Agreement. When these review standards are developed, they will be incorporated as an appendix to this agreement.

(U//FOUO) NCTC's Information and Incidents Analysis Group shall develop methods to track and report to DHS on a quarterly basis the information identified in Appendix C as it relates to its use of ADIS.

(U//FOUO) DHS shall develop methods to review NCTC's identification of terrorism information on a quarterly basis.

(U//FOUO) In order to ensure that data is only used for the purposes described in this MOU, DHS shall have the right to independently review NCTC audit records and to audit and inspect NCTC's use of ADIS Data, including ensuring that the U.S. Person data has been deleted, who has accessed the data, what reports have been generated based on the ADIS Data, and to whom the reports have been disseminated.

**6. (U) POINTS OF CONTACT.**

(U) The individuals responsible for overseeing implementation of this MOU and the identification and resolution of issues hereunder shall be:

Director, Information Sharing and Intelligence Enterprise Management Division  
Department of Homeland Security  
245 Murray Lane SW, Bldg 14,  
Washington DC 20528

(b)(6); (b)(7)(C)

Assistant Director for Program Integration and Mission Services  
National Protection and Programs Directorate/US-VISIT Program  
Department of Homeland Security  
1616 N. Fort Myer Drive  
Arlington, VA 22209

(b)(6); (b)(7)(C)

Chief, Information Sharing Program Office  
National Counterterrorism Center

(b)(6); (b)(7)(C)

**7. (U) SEVERABILITY.**

(U//FOUO) Nothing in this agreement is intended to conflict with current law or regulation or the directives of the DHS or NCTC. If a term of this agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

**8. (U) NO PRIVATE RIGHT.**

(U//FOUO) This MOU is an internal agreement between DHS and NCTC. It does not create or confer any right or benefit, substantive or procedural, enforceable by any third party against the Parties, the United States, or the officers, employees, agents, or associated personnel thereof. Nothing in this MOU is intended to restrict the authority of either party to act as provided by law, statute, or regulation, or to restrict any party from administering or enforcing any laws within its authority or jurisdiction.

**9. (U) FUNDING.**

(U) This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each Party shall bear its own costs in relation to this MOU. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

**10. (U) ISSUE RESOLUTION.**

(U) Throughout the course of this agreement, issues such as scope of the agreement, interpretation of its provisions, unanticipated technical matters, including improvements, and other proposed modifications can be expected. Both parties agree to appoint their respective points of contact to work in good faith towards resolution.

**11. (U) EFFECTIVE DATE.**

(U) The terms of this agreement will become effective upon the signature of the second party to this MOU.

**12. (U) MODIFICATION.**

(U) This agreement or any appendices thereto may be modified upon the mutual written consent of the parties, which shall be recorded and incorporated into this MOU as a separate appendix.

**13. (U) TERMINATION.**

(U) The terms of this agreement, as modified with the consent of both Parties, will remain in effect for three (3) years from the EFFECTIVE DATE. The agreement may be extended by mutual written agreement of the parties. Either Party upon thirty (30) days' written notice to the other Party may terminate this agreement.

**14. (U) ENTIRE AGREEMENT.**

(U) This MOU, and any concurrently or subsequently approved appendices, constitutes the entire agreement between the parties.

**(U) APPROVED BY:**

(U) This MOU represents the understanding reached between DHS and NCTC. By signing below, the Parties have caused their duly authorized representatives to execute this MOU.

FOR THE U.S. DEPARTMENT OF HOMELAND SECURITY

(b)(6); (b)(7)(C)

8/26/10  
[Date]

Deputy Under Secretary for Intelligence & Analysis  
(Plans, Policy, and Performance Management)

(b)(6); (b)(7)(C)

AUG 27 2010  
[Date]

Director  
US-VISIT Program

FOR THE NATIONAL COUNTERTERRORISM CENTER

(b)(6); (b)(7)(C)

27 Aug 2010  
[Date]

Deputy Director, Information Sharing and Knowledge Development

(b)(6); (b)(7)(C)

27 Aug 2010  
[Date]

Deputy Director for Intelligence

APPENDIX A (U//FOUO)

**(U//FOUO) APPENDIX A: List of ADIS Data Elements**

(b)(7)(E)





APPENDIX B (U)

**(U) APPENDIX B: ADIS Data Transfer, Processing and Handling Procedures**

(U//FOUO) In instances where NCTC identifies information within the dataset as terrorism information, the Information and Incidents Analysis Group may request additional data elements maintained in the relevant ADIS record.

(U) DELIVERY OF DATA.

(b)(7)(E)



(b)(7)(E)



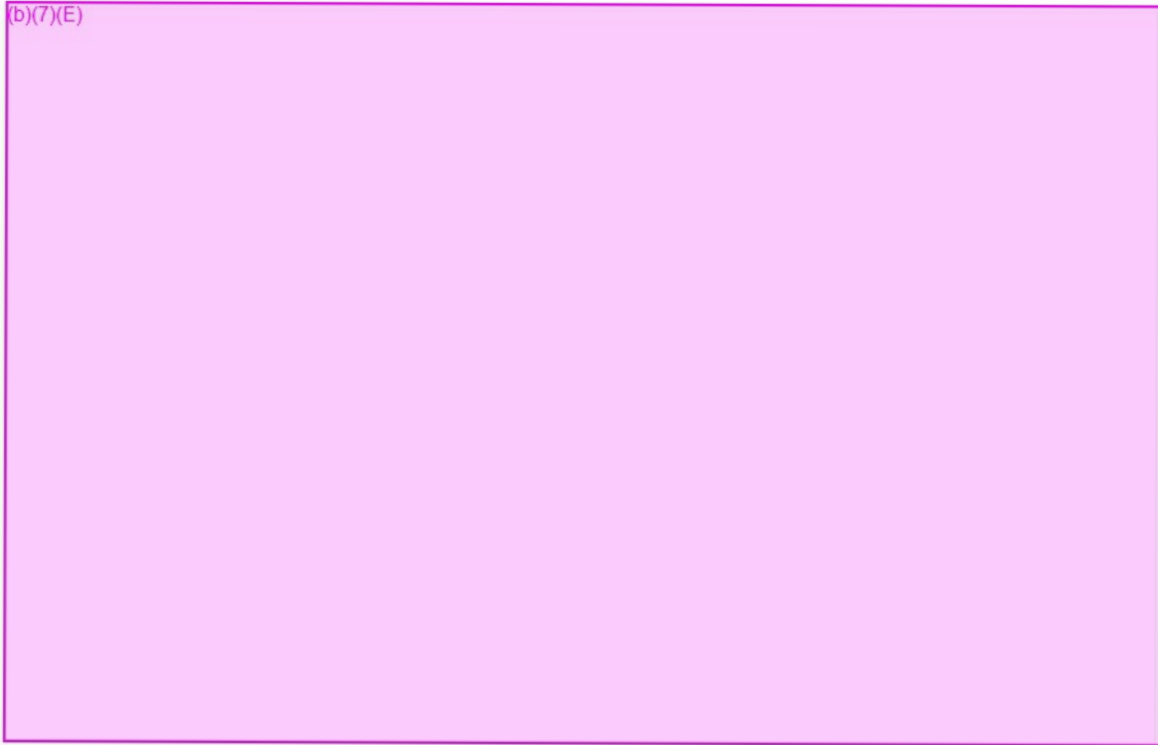
(b)(7)(E)



(U//FOUO) Records of Transfer: The Parties agree to maintain a log of all information received and sent, including names of recipients and senders, as well as the date and type of information used for transfer.

APPENDIX C (U)

**(U//FOUO) APPENDIX C: NCTC Reporting Requirements**



APPENDIX D (U)

**(U) APPENDIX D: NCTC AG Guidelines Implementing Instructions**

(U) APPENDIX D: NCTC Implementing Instructions for the MOA between the AG and the DNI on Guidelines for Access, Retention, Use and Dissemination by the NCTC of Terrorism Information Contained within Datasets Identified as Including Non-terrorism Information and Information pertaining Exclusively to Domestic Terrorism, November 2008

(U) With respect to the Department of Homeland Security's provision of United States person, refugee, or asylee information from their Arrival and Departure Information System, NCTC will review and process all the provided information within 30 calendar days of receipt from DHS to determine whether the information, in whole or in part, constitutes terrorism information. Records determined to be terrorism information will be retained, used and disseminated according to the conditions set forth in the underlying agreement. Records determined not to constitute terrorism information will be immediately deleted within 30 days of receipt.



## **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](http://www.dhs.gov/privacy), on DHSConnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	ESTA Social Media Tool 2 Pilot Evaluation		
<b>Component:</b>	Customs and Border Protection (CBP)	<b>Office or Program:</b>	OFO (b) (7)(E)
<b>Xacta FISMA Name (if applicable):</b>	(b) (7)(E)	<b>Xacta FISMA Number (if applicable):</b>	(b) (7)(E)
<b>Type of Project or Program:</b>	Pilot	<b>Project or program status:</b>	Pilot
<b>Date first developed:</b>	January 1, 2017	<b>Pilot launch date:</b>	January 8, 2018
<b>Date of last PTA update:</b>	N/A	<b>Pilot end date:</b>	December 31, 2018
<b>ATO Status (if applicable):</b>	Complete	<b>ATO expiration date (if applicable):</b>	January 25, 2020

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	(b) (6), (b) (7)(C)		
<b>Office:</b>	OFO	<b>Title:</b>	Director
<b>Phone:</b>	(b) (6), (b) (7)(C)	<b>Email:</b>	(b) (6), (b) (7)(C) @cbp.dhs.gov

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	(b) (6), (b) (7)(C)		
<b>Phone:</b>	(b) (6), (b) (7)(C)	<b>Email:</b>	(b) (6), (b) (7)(C) @cbp.dhs.gov



## SPECIFIC PTA QUESTIONS

### 1. Reason for submitting the PTA: New PTA

CBP is submitting this PTA to test a secondary Electronic System Travel Authorization (ESTA) social media vetting tool, (b) (7)(E) CBP previously conducted the ESTA Social Media Tool Pilot Evaluation (June 11, 2016-September 9, 2016) in which CBP supported DHS S&T's lead testing the efficacy of an initial commercial capability in this space. The PTA for that effort was adjudicated August 15, 2016.

(b) (7)(E)

During this pilot, which will occur from January 8, 2018 to December 31, 2018, CBP will evaluate ESTA cases in the following scenarios:

1. ESTA Cases Referred for Manual Review (including those being considered for a waiver)
  - a. In these cases, CBP officers working on ESTA vetting have requested social media review internally within CBP (b) (7)(E) (b) (7)(E) to help determine eligibility and admissibility under the Visa Waiver Program.
  - b. The operational pilot will assist with the review of these cases using this new tool to support adjudicatory decisions by (b) (7)(E) responsible for adjudication of the applications in question who will manually review the results.
2. Other ESTA Cases that may require additional review by the ESTA team (e.g. cases of concern for (b) (7)(E)

a. (b) (7)(E)

b. (b) (7)(E)

(b) (7)(E), (b) (5)



In all cases, CBP will access publicly available information in accordance with its authorities. This means that all searches will be conducted using open source material and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available.

<p><b>2. Does this system employ any of the following technologies:</b> <i>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.</i></p>	<p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input checked="" type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal<sup>1</sup> (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</p>
--	--

<p><b>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</b> <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information<sup>2</sup></p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p>
--	--

<p><b>4. What specific information about individuals is collected, generated or retained?</b></p>
<p>(b) (7)(E)</p> <p>As part of this pilot, CBP will also collect publicly available information from social media platforms to assist in assessing the eligibility of ESTA applicants to travel under Visa Waiver Program (VWP). Any derogatory information collected from social media and deemed operationally relevant will be stored in ATS-TF.</p>

<sup>1</sup> 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.

<sup>2</sup> 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.



<p>The full list of ESTA application fields is below:</p> <ul style="list-style-type: none"> <li>• Full name (first, middle, and last);</li> <li>• Other names or aliases, if available;</li> <li>• Date of birth;</li> <li>• City and country of birth;</li> <li>• Gender;</li> <li>• Email address;</li> <li>• Telephone number (home, mobile, work, other);</li> <li>• Home address (address, apartment number, city, state/region);</li> <li>• Internet protocol (IP) address;</li> <li>• ESTA application number;</li> <li>• Country of residence;</li> <li>• Social media handles</li> </ul>	
<p><b>4(a) Does the project, program, or system retrieve information by personal identifier?</b></p>	<p><input type="checkbox"/> No. Please continue to next question.  <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: (b) (7)(E) [REDACTED]</p>
<p><b>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</b></p>	<p><input checked="" type="checkbox"/> No.  <input type="checkbox"/> Yes.</p>
<p><b>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</b></p>	<p>Click here to enter text.</p>
<p><b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b></p>	<p>Click here to enter text.</p>
<p><b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b></p> <p><i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p>	<p><input checked="" type="checkbox"/> No. Please continue to next question.  <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.</p>
<p><b>4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.</b></p>	
<p>Click here to enter text.</p>	

<sup>3</sup> 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.





<p><b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>Any PII or potentially derogatory information identified and retained will be stored within ATSTF.</p>
<p><b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>Information regarding ESTA applications will be loaded into (b) (7)(E)</p> <p><b>(b) (7)(E)</b></p>
<p><b>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</b></p>	<p>Existing</p> <p>Please describe applicable information sharing governance in place: (b) (7)(E)</p> <p><b>(b) (7)(E)</b></p>
<p><b>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?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>All CBP Officers, Agents, Analysts, and Contractors using Social Media for operational purposes must complete the CBP Social Media Training and Rules of Behavior.</p> <p><b>(b) (7)(E)</b></p>



<p><b>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/agencies who have requested access to their PII?</b></p>	<p><input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting:</p> <div style="background-color: black; color: white; text-align: center; padding: 10px; font-size: 2em; font-weight: bold;">(b) (7)(E)</div> <p><input type="checkbox"/> Yes. In what format is the accounting maintained:</p>
<p><b>9. Is there a FIPS 199 determination?<sup>4</sup></b></p>	<p><input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p><b>Confidentiality:</b> <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p><b>Integrity:</b> <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p><b>Availability:</b> <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p>

### PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	<b>(b) (6), (b) (7)(C)</b>
<b>Date submitted to Component Privacy Office:</b>	<b>December 6, 2017</b>

<sup>4</sup> 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.



<b>Date submitted to DHS Privacy Office:</b>	December 20, 2017
<b>Component Privacy Office Recommendation:</b>	
<i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b) (5), (b) (7)(E)	

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

<b>DHS Privacy Office Reviewer:</b>	(b) (6), (b) (7)(C)
<b>PCTS Workflow Number:</b>	1155460
<b>Date approved by DHS Privacy Office:</b>	January 5, 2018
<b>PTA Expiration Date</b>	January 5, 2021

**DESIGNATION**

<b>Privacy Sensitive System:</b>	Yes If "no" PTA adjudication is complete.
<b>Category of System:</b>	IT System If "other" is selected, please describe: Click here to enter text.



<b>Determination:</b>	
<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.	
<b>PIA:</b>	<b>System covered by existing PIA</b> If covered by existing PIA, please list: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA)
<b>SORN:</b>	System covered by existing SORN If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713
<b>DHS Privacy Office Comments:</b>	
<i>Please describe rationale for privacy compliance determination above.</i>	
CBP is submitting this PTA to discuss the next update for the ESTA Social Media Pilot. This update involves use of a new social media vetting tool. (b) (7)(E)	
<div style="background-color: black; color: white; font-size: 48pt; padding: 20px;">(b) (7)(E)</div>	
The DHS Privacy Office finds this initiative privacy-sensitive.  Coverage is provided by DHS/CBP/PIA-007 ESTA and the DHS/CBP-009 ESTA. The Privacy Office agrees that coverage for this pilot is also provided under DHS/CBP/PIA-006 ATS, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, this PIA outlines the querying of publicly available information in support of the vetting process. The DHS Privacy Office also agrees that SORN coverage is provided by the DHS/CBP-006 ATS SORN, which notes that CBP collects information on	



# Homeland Security

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

**Privacy Threshold Analysis**  
**Version number: 01-2014**  
*Page 10 of 10*

individuals whom may be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination, as well as those who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law.

In all cases, CBP will access publicly available information in accordance with its authorities. This means that all searches will be conducted using open source material and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available.

Policy Number: 10082.1  
FEA Number: 360-112-002b


Office of the Director

U.S. Department of Homeland Security  
500 12<sup>th</sup> Street, SW  
Washington, DC 20536

JUN 28 2012



**U.S. Immigration  
and Customs  
Enforcement**

MEMORANDUM FOR: Law Enforcement Personnel  
FROM: John Morton  
Director   
SUBJECT: Use of Public and Non-Public Online Information

Purpose

This memorandum provides U.S. Immigration and Customs Enforcement (ICE) law enforcement personnel guidance on the acceptable use of online information within the scope of their law enforcement duties.

Background

On December 8, 2010, Secretary Napolitano approved a decision memorandum titled, "Use of Public and Non-Public Online Information for Law Enforcement, Situational Awareness, and Intelligence Purposes," ("The Online Information Memorandum") that adopted a recommendation whereby the Department of Homeland Security (DHS), except members of the Intelligence Community governed by Executive Order 12333, would "follow the Department of Justice (DOJ) 1999 guidelines for online investigative and situational awareness activities." The Online Information Memorandum also suggested that DHS Components develop supplementary guidance, as necessary, for their mission-specific purposes consistent with DHS policy.

Discussion

Pursuant to the Online Information Memorandum, ICE law enforcement personnel should follow the below principles for the use of public and non-public online information, which have been adapted from the online investigative principles outlined in DOJ's 1999 Online Investigative Principles for Federal Law Enforcement Agents.<sup>1</sup>

---

<sup>1</sup> Law enforcement personnel are ICE employees who conduct and support criminal, civil, and administrative law enforcement investigations and operations. Examples include special agents and other law enforcement officers, law enforcement investigative support personnel, intelligence research specialists, criminal research specialists, and attorneys prosecuting criminal, civil or administrative matters.

To implement these core principles, ICE directorates and program offices may establish guidance and/or modify existing guidance, as necessary, or reference the DOJ guidance as applicable to the activities in question.

#### ICE Principles for Law Enforcement Use of Public and Non-Public Online Information:

1. **Obtaining Information from Unrestricted Sources.** Law enforcement personnel may obtain information from publicly accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.
2. **Obtaining Identifying Information about Users or Networks.** There are widely available software tools for obtaining publicly available identifying information about a user or a host computer network. Law enforcement personnel may use such tools in their intended lawful manner under the same circumstances in which ICE guidelines and procedures permit them to look up similar identifying information (e.g., a telephone number) through non-electronic means. However, law enforcement personnel may not use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.
3. **Real-Time Communications.** Law enforcement personnel may passively observe and log real-time electronic communications open to the public under the same circumstances in which they may attend a public meeting.
4. **Accessing Restricted Sources.** Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space.
5. **Online Communications Generally.** Law enforcement personnel may use online services to communicate as they may use other types of communication tools, such as the telephone and the mail. Law enforcement personnel should retain the contents of a stored electronic message if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.
6. **Undercover Communications.** Law enforcement personnel communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when ICE guidelines would require such disclosure if the communication were taking place in person or over the telephone. Law enforcement personnel may communicate online under a non-identifying name or fictitious identity if ICE guidelines and procedures would authorize such communications in the physical world. For purposes of ICE undercover guidelines, each discrete conversation online constitutes a separate undercover activity or contact, but such a conversation may comprise more than one transmission between the law enforcement personnel and another person.

7. **Online Undercover Activities.** Just as law enforcement agencies may establish physical-world undercover entities, they also may establish online undercover facilities, such as bulletin board systems and Web sites, which covertly offer information or services to the public. Online undercover facilities, however, can raise novel and complex legal issues, especially if law enforcement personnel seek to use the system administrator's powers for criminal investigative purposes. Further, these facilities may raise unique and sensitive policy issues involving privacy, international sovereignty, and unintended harm to unknown third parties. Because of these concerns, a proposed online undercover facility, like any undercover entity, may be established only if the operation is authorized pursuant to ICE's guidelines and procedures for evaluating undercover operations.
8. **Communicating Online Through the Use of the Identity of a Cooperating Witness, with Consent.** Law enforcement personnel may ask a cooperating witness to communicate online with other persons in order to further an investigation if agency guidelines and procedures authorize such a consensual communication in person, over the telephone, or through other non-electronic means. Law enforcement personnel may communicate online using the identity of another person if that person consents, if the communications are within the scope of the consent, and if such activity is authorized by ICE guidelines and procedures. Personnel who communicate online through the identity of a cooperating witness are acting in an undercover capacity.
9. **Appropriating Online Identity.** "Appropriating online identity" occurs when law enforcement personnel electronically communicate with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. Appropriating identity is an intrusive law enforcement technique that should be used infrequently and only in serious criminal cases. When assuming an online identity, law enforcement personnel must follow all applicable ICE policies and guidelines.
10. **Activity by Law Enforcement Personnel during Personal Time.** While not on duty, law enforcement personnel are generally free to engage in personal online pursuits. If, however, the off-duty online activity directly and substantially relates to a law enforcement investigation, operation, or prosecution, law enforcement personnel are bound by the same restrictions regarding the use of online information as would apply when on duty.
11. **International Issues.** Unless gathering information from online facilities configured for public access, law enforcement personnel conducting investigations should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever an item or person is located abroad, law enforcement personnel should follow ICE's policies and procedures for international investigations.

Personnel who conduct and support criminal and civil law enforcement investigations and/or operations must adhere to the above principles when using information gathered online in support of an official agency criminal or civil law enforcement investigations and/or operations.



The principles that address the use of the Internet for undercover activities apply only to ICE personnel with the authority to conduct undercover investigations.

Personnel who conduct civil and criminal law enforcement activities for Enforcement and Removal Operations should also adhere to the above principles when using information gathered online in support of their law enforcement activities. Such personnel should remain mindful that the principles that address the use of the Internet for undercover activities apply only to those vested with such authority.

Attorneys with the Office of the Principal Legal Advisor should also adhere to the above principles, except those that are applicable to undercover activities, when using information gathered online in support of their handling of criminal, civil, or administrative matters.

**No Private Right of Action**

This memorandum is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter.