



Privacy Compliance Review of the Privacy Incidents Affecting Individuals Protected by Section 1367

February 4, 2019

Contact Points

Cameron Quinn, Officer for Civil Rights and Civil Liberties

Kevin K. McAleenan, Commissioner, U.S. Customs and Border Protection

Ronald D. Vitiello, Senior Official Performing the Duties of the Director, U.S. Immigration and Customs Enforcement

L. Francis Cissna, Director, U.S. Citizenship and Immigration Services

Admiral Karl L. Shultz, Commandant, U.S. Coast Guard

David J. Glawe, Under Secretary, Office of Intelligence and Analysis

Shonnie R. Lyon, Director, Office of Biometric Identity Management

Reviewing Official

Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717



I. Background

The Department of Homeland Security (DHS) Privacy Office (PRIV) conducted a Privacy Compliance Review (PCR) to assist certain Components, as well as the Office of Intelligence and Analysis (I&A) and the Office of Biometric Identity Management (OBIM) (herein collectively referred to as Components), in identifying and mitigating risks that may be incurred by inadvertent disclosure of information protected by Title 8, United States Code (U.S.C.), Section 1367, confidentiality and prohibited source provisions (relating to applicants for and beneficiaries of Violence Against Women Act (VAWA), T visa,¹ or U visa² protections in accordance with 8 U.S.C. 1367(d) and Section 810 of the Violence Against Women Reauthorization Act of 2013, including VAWA self-petitioners³ and VAWA cancellation or removal applicants⁴ (herein collectively referred to as Section 1367 information).

Section 1367 generally prohibits Department personnel from permitting use by or disclosure of any information relating to a beneficiary of a pending or approved application for alien victim-based immigration benefits to anyone other than a sworn officer or employee of the Department, the Department of State, or the Department of Justice, unless one of several enumerated statutory exceptions apply. Section 1367 also prohibits Department personnel from making an adverse

¹ T nonimmigrant status is available to certain victims of a severe form of trafficking in persons, as defined in section 103 of the Victims of Trafficking and Violence Prevention Act (VTVPA) of 2000, who are physically present in the United States on account of trafficking and who have complied with any reasonable requests for assistance in a law enforcement investigation or prosecution (with limited exceptions). See Immigration and Nationality Act (INA) Section 101(a)(15)(T). T nonimmigrant status allows victims of human trafficking to remain in the United States for up to four years (or longer if a limited exception applies), receive work authorization, and, if certain conditions are met, apply for adjustment of status to that of a lawful permanent resident (LPR).

² U nonimmigrant status is available to certain victims of criminal activity designated in INA Section 101(a)(15)(U) (qualifying crimes) who have suffered substantial mental or physical abuse as a result of being a victim of criminal activity, possess relevant information concerning the crime, and have been helpful, are being helpful, or are likely to be helpful to law enforcement or government officials in the investigation or prosecution of the criminal activity. U nonimmigrant status allows victims to remain in the United States for up to four years (or longer if a limited exception applies), receive work authorization, and, if certain conditions are met, apply for adjustment of status to that of an LPR.

³ Under VAWA, as amended, certain persons who have been battered or subjected to extreme cruelty by a qualifying relative may self-petition, allowing them to remain in the United States, apply for LPR status as an approved VAWA self-petitioner, and eventually apply for naturalization. VAWA self-petitioners include: the spouse, child or parent of an abusive U.S. citizen; the spouse or child of an abusive LPR; the conditional resident spouse or child of an abusive U.S. citizen or LPR; the spouse or child of an alien eligible for relief under the Cuban Adjustment Act, the Haitian Refugee Immigration Fairness Act, or the Nicaraguan Adjustment and Central American Relief Act; and the spouse or child eligible for suspension of deportation or cancellation of removal due to abuse by a U.S. citizen or LPR. See INA Section 101(a)(51) (defining "VAWA self-petitioner").

⁴ Victims of domestic violence who are in removal proceedings may be eligible to apply for relief with the immigration court in the form of VAWA cancellation of removal. See INA Section 240A(b)(2) (prescribing eligibility requirements).



determination of admissibility or deportability of an alien victim using information furnished solely by a prohibited source associated with battery or extreme cruelty, sexual assault, human trafficking, or substantial physical or mental abuse and criminal activity, regardless of whether the alien victim has applied for VAWA benefits, or a T or U nonimmigrant status.

The DHS Officer for Civil Rights and Civil Liberties (CRCL) has, through Delegation 19004,⁵ the authority to provide DHS-wide guidance and oversight on the implementation of Section 1367 confidentiality and prohibited source provisions. He or she exercises this authority in part through DHS Directive 002-02, *Implementation of Section 1367 Information Provisions*; DHS Directive 215-01 and DHS Instruction 215-01-001, both titled *Disclosure Of Section 1367 Information To National Security Officials For National Security Purposes*; and DHS Instruction 215-01-002, *Disclosure Of Section 1367 Information To Law Enforcement Officials For Legitimate Law Enforcement Purposes*. Further, the Department issued DHS Directive 002-01 and Instruction 002-01-001, both titled *Council On Combating Violence Against Women*, which established a Council focusing on advancing overall knowledge of and compliance with VAWA, VTPA, subsequent authorizations to those laws, and related immigration laws and issues.

The Chief Privacy Officer (CPO), pursuant to his or her authority under Section 222 of the Homeland Security Act, and also his or her responsibilities as the Department's Senior Agency Official for Privacy under the Office of Management and Budget (OMB) Memorandum M-17-12,⁶ must determine any potential impacts a privacy incident may have on the privacy of individuals, including those protected by Section 1367.⁷ When, for instance, a Component reports a privacy incident to PRIV's Director for Incidents, that person, along with the CPO, and in consultation with the Component Privacy Officer and other appropriate parties, determines if the incident is a minor or major incident based on the context of the incident and risks to the individuals and the DHS mission.⁸ PRIV is accountable for ensuring appropriate follow-up actions are taken, such as investigation and notification, or may delegate this responsibility to the affected Component. Because of the shared responsibilities for ensuring the proper handling of Section 1367 information, PRIV and CRCL have developed a process whereby the two offices share incidents of unauthorized Section 1367 disclosures. The two offices then work together to

⁵ See Appendix A, DHS and Component Delegations, Directives, and Instructions Providing DHS-wide Guidance and Oversight on the Implementation of Section 1367 Confidentiality and Prohibited Source Provisions, for all Delegations, Directives, and Instructions listed in this paragraph.

⁶ OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

⁷ DHS Management Directive (MD) 047-01, Privacy Policy and Compliance, available at <https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01>.

⁸ See DHS policies on processing privacy incidents: DHS Privacy Policy Instruction 047-01-006, *Privacy Incident Responsibilities and Breach Response Team*, and DHS Privacy Policy instruction 047-01-008, *Privacy Incident Handling Guidance*, both available at <https://www.dhs.gov/policy>. See also OMB M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements (October 25, 2018), Section II: Incident Reporting Requirements, which defines a "major incident."



ensure the incident is appropriately investigated, addressed, and resolved. The two offices coordinated on multiple violations in Fiscal Year (FY) 2018.

In accordance with Executive Order 13392, Improving Agency Disclosure of Information, the Secretary of Homeland Security designated the CPO to serve concurrently as the Chief Freedom of Information Act (FOIA) Officer to promote efficiency, effectiveness, and statutory compliance throughout the Department. Many of the Department's FOIA offices serve a large population of requesters seeking records that document their personal interactions with immigration officials, which may contain information protected by Section 1367.

The DHS Chief FOIA Officer is drafting an instruction titled, *Freedom of Information Act and Privacy Act Guidance for Section 1367 Information*, which implements DHS Directive 002-02, *Implementation of Section 1367 Information Provisions*. The Instruction will provide guidance to DHS employees and contractors on how to respond to a FOIA or Privacy Act (PA) request to ensure that Section 1367 information is properly protected and in accordance with the law and DHS policy. DHS Instruction 002-02-001, *Implementation of Section 1367 Information Provisions*, provides general policy and guidance on disclosure of Section 1367 information, including the VAWA's eight statutory exceptions to the general nondisclosure requirement. All other sharing of personally identifiable information (PII) to third parties must be consistent with Department policy, including DHS's privacy policies and information sharing policies. DHS employees and contractors have a duty to safeguard all information in its possession, and to prevent the compromise of that PII in order to maintain the public's trust in the Department. The Instruction will address unauthorized disclosures.⁹

Section 1367 incidents are particularly sensitive, given the vulnerability of the population they are meant to protect and the potential legal liabilities for certain violations of the statute. Through this PCR, we examine Components' privacy protections and identify best practices to prevent and mitigate future privacy incidents affecting individuals protected by Section 1367.

II. Scope and Methodology

A. Scope

PRIV scoped this PCR to those DHS Components most likely to handle records of individuals protected by Section 1367 or to facilitate sharing of those records through electronic means. The following Components collect information from immigrants, including applicants, petitioners, asylees, refugees, and victims of trafficking and smuggling, and thus were determined to be in

⁹ The proposed language in the Instruction is as follows: **Notification of Unauthorized Disclosures**: In the event that any Component (1) discloses Section 1367 information in a manner inconsistent with the provisions above or (2) is informed by the recipient of Section 1367 information that the recipient has disclosed that information in an unauthorized manner, the Component Head (1) notifies the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties as soon as is practicable, but in no event later than twenty-four hours after discovery of the unauthorized disclosure, and (2) satisfies the requirements of the DHS Privacy Incident Handling Guidance.



scope: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), and the U.S. Coast Guard (USCG). The Office of Intelligence and Analysis (I&A) and the Office of Biometric Identity Management (OBIM) were included because of their role in enterprise information sharing, with the intelligence community, and with domestic and international biometric-based sharing partners, respectively.

B. Methodology

PRIV reviewed the relevant Departmental Delegation, Directives, and Instructions regarding implementation of the Section 1367 confidentiality and prohibited source provisions. They are as follows:

- Delegation Of Authority To Issue Guidance And Implement 8 United States Code 1367
Delegation Number: 19004, Issue Date: 09/23/2013¹⁰
- Council On Combating Violence Against Women
Directive Number: 002-01, Issue Date 03/14/2013
Instruction Number: 002-01-001, Issue Date 03/15/2013
- Implementation Of Section 1367 Information Provisions
Directive Number: 002-02, Issue Date: 11/01/2013
Instruction Number: 002-02-001, Issue Date: 11/7/2013
- Disclosure Of Section 1367 Information To National Security Officials For National Security Purposes
Instruction Number: 215-01, Issue Date: 11/06/2013
- Disclosure Of Section 1367 Information To Law Enforcement Officials For Legitimate Law Enforcement Purposes
Instruction Number: 215-01-002, Issue Date: 06/18/2016

PRIV reviewed the incidents involving Section 1367 protected records that Components had reported to PRIV in FY2017-FY2018. These incidents are recorded in the Enterprise Cyber Operations Portal (ECOP), managed by the PRIV Director for Incidents.

PRIV administered a questionnaire to I&A, USCIS, OBIM, USCG, ICE, and CBP to confirm application of confidentiality protections applied to 1367 records, as well as adherence to Management Directive 047-01, Privacy Policy and Compliance, specifically with regard to incident reporting and mitigation. PRIV questions focused on whether operators are able to identify which records are subject to the protections in Section 1367, as well as the ability to track the disclosure of those records.

¹⁰ See Appendix A.



The CPO sent an entrance memorandum to the Component and Office principals on May 30, 2018, which included the initial questionnaire and a request for response within 30 days. Subsequent questions and responses continued through the last Component response, received in October 2018.

III. Summary of Recommendations

Based on our findings, this PCR makes the following recommendations:

1. Directive 002-02, Directive 215-01, and Instruction 215-01-001 require each Component to develop implementing instructions, standard operating procedures (SOPs), or other policy guidance necessary to ensure compliance with the confidentiality rules under Section 1367, tailored to the specific context of each Component's mission and systems. PRIV recommends that Component-specific implementing instructions, SOPs, or policy guidance be developed in coordination with the Council on Combating Violence Against Women (CCVAW), USCIS, and CRCL, per the Delegation, Directives, and Instructions cited above. Such policies should include the following:
 - The process for how Section 1367 information is kept current in all relevant systems that contain Section 1367 information;
 - How third party access to systems must be managed to protect Section 1367 information confidentiality;
 - How disclosures are documented, including the ability to audit disclosures; and
 - How systems affix caveats to Section 1367 information.
2. By September 2019, USCIS must report system access inventory findings to PRIV and CRCL, including how it has addressed gaps in protecting Section 1367 information given confidentiality requirements.
3. USCIS must identify an Information Sharing and Access Agreement (ISAA) with the Federal Bureau of Investigation (FBI) that covers bulk sharing of Section 1367 information in accordance with DHS policy.
4. By February 2019, CBP must report to PRIV and CRCL whether all of its system interfaces and online query responses are configured to ensure only authorized users receive 1367 records, with caveats, as appropriate under the governing Memorandum of Understanding (MOU).

IV. Findings

Policy Compliance

Requirement: The review evaluated whether components complied with DHS policies established by Departmental Delegations, Directives, and Instructions regarding implementation



of the Section 1367 confidentiality and prohibited source provisions, all referenced above. When Components lacked a Component-specific policy, or when there were reported incidents, PRIV made further inquiry to determine the risk of wrongful disclosure and the need for a Component-specific policy.

General Findings: Most Components lack necessary policies for protecting 1367 records in compliance with DHS Directive 002-02, Directive 215-01, and Instruction 215-01-002

Directive 002-02, Implementation of Section 1367 Information Provisions, IV D. states that “Component Heads with any Section 1367 information that might be shared will implement and execute all applicable policies and procedures set forth in [the] Directive and develop any necessary implementing instructions or other policy guidance.”

Similar requirements are memorialized in Directive 215-01, *Disclosure Of Section 1367 Information To National Security Officials For National Security Purposes* and in Instruction 215-01-002, *Disclosure Of Section 1367 Information To Law Enforcement Officials For Legitimate Law Enforcement Purposes*. Development of Component-specific policies is also consistent with the policy and requirements of the CCVAW, the mechanism for DHS to ensure that policies combating violence against women are consistent department-wide.

Component Specific Findings:

I&A: Policy Instruction IA-903, *Disclosure of Information on Applicants or Beneficiaries Falling under T Visa, U Visa, or Violence Against Women Act Protections*, establishes I&A procedures and requirements for the disclosure of information protected by Section 1367 in support of I&A. PRIV has no reported incidents for I&A, and made no further inquiry beyond the initial questionnaire.

USCIS: Policy Memorandum PM-602-0136 covers identification and disclosure of Section 1367 information; however, PM-602-0136 does not fully comply with Directive 002-02, because it does not address how third party access to its systems should be managed to protect Section 1367 information confidentiality.

The USCIS Office of Privacy reports that numerous external entities to DHS currently have access to 1367 information through various mechanisms:

- Federal Government agencies (including subcomponents)
 - Department of State
 - Department of Justice
 - Department of the Treasury (including JP Morgan Chase for payment services)
 - Department of Labor
 - Social Security Administration
 - Department of Health and Human Services
 - Department of Education



- Several local government agencies confirming status for a variety of entitlements (including legacy connections related to Section 287(g) program)

The USCIS Privacy Office acknowledges that USCIS has not documented the external connections in a consistent fashion and states that it is setting requirements to ensure appropriate access controls are in place as USCIS moves away from legacy systems. In September 2018, the USCIS Privacy Office stated in a response to this PCR that it will begin an in-depth review of all USCIS systems to account for Special Protected Class (SPC) data, including Section 1367 information, and to ensure appropriate protections are set depending on collection type. The USCIS Privacy Office expects that this review will take approximately one year (September 2019) and will engage Components agency-wide. The USCIS Privacy Office will coordinate this effort with counterparts at the USCIS Offices of Chief Counsel and Information Technology, and the USCIS Chief Data Officer, and the respective operational units responsible for systems of records. Each system owner will be required to review each data sharing and connection agreement to ensure that authorized access has been documented properly, and any unauthorized access is terminated immediately.

The USCIS Privacy Office expects to review the following systems, but recognizes this is not an exhaustive list:

- Central Index System 2 (CIS2)
- Computer Linked Application Information Management System 3 Local Area Network (CLAIMS 3 LAN)
- Computer Linked Application Information Management System 4 (CLAIMS 4)
- Customer Profile Management System (CPMS)
- USCIS Electronic Immigration System 2 (ELIS 2)
- Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)
- Enterprise Document Management System (EDMS)
- Fraud Detection and National Security - Data System (FDNS-DS)
- National Appointment Scheduling System (NASS)
- Service Center - Computer Linked Application Information Management System (SC CLAIMS)
- USCIS Enterprise Service Bus 2 (ESB2) Person Centric Query Service (PCQS)
- USCIS RAILS
- Validation Instrument for Business Enterprise (VIBE)
- Verification Information System (VIS)

PRIV commends the USCIS Office of Privacy for initiating this report, which is an important step toward eliminating risk of wrongful disclosure.

OBIM: OBIM's Biometric Support Center (BSC) has a Standard Operating Procedure that requires BSC operators to manually check USCIS systems for 1367 protected status before



sharing information based on a latent fingerprint match. However, most of OBIM's disclosures do not occur through the BSC, but on an automated basis through its Automated Biometric Identification System (IDENT). OBIM lacks a policy specific to IDENT, but asserts that IDENT's automated data sharing settings, known as the Data Access and Security Controls (DASC), directly implement Section 1367 confidentiality provisions.

According to OBIM's Privacy Office and corroborated by the USCIS Privacy Office, OBIM receives a spreadsheet once a month from USCIS via encrypted email, which notifies OBIM of those records that belong to Section 1367 protected identities.¹¹ When OBIM receives that data, OBIM staff updates those records with a "flag," visible only to the IDENT system administrator. OBIM staff configures the DASC to filter receipt of Section 1367-flagged records according to the role of the user. Thus, authorized U.S. law enforcement and national security users have access to 1367 information, while unauthorized civil and foreign agencies do not. However, while it may be legal for law enforcement and national security users of IDENT to receive 1367 information, the absence of a caveat, as required by Instruction 215-01-001, means that officers cannot implement onward sharing protections. Without a general log-in warning on the IDENT system or a caveat in the records themselves, authorized users may inadvertently disclose 1367 information in contravention of the statute and DHS Directives and Instructions.

As a separate matter, in the course of conducting the PCR, OBIM reported an incident regarding wrongful disclosure of Section 1367 information. Prior to discovering and reporting the incident, several OBIM employees had received encrypted emails on a monthly basis from USCIS to update the Section 1367 identities in IDENT. For several months in 2018, OBIM received the spreadsheet updates of records that should receive Section 1367 protections through the encrypted emails but did not update the records appropriately because the responsible employees had since transitioned to new positions. USCIS had not been informed. OBIM reported this incident to PRIV's Director for Incidents and CRCL. This incident is now closed.

USCG: USCG has no policy with regard to identification or handling of Section 1367 information. The USCG Privacy Office stated that no policy is necessary because USCG operators do not handle Section 1367 information.

In the USCG Biometrics At Sea System program (BASS), USCG deploys a biometric capability to assist in the determination of courses of action in USCG law enforcement interdictions, e.g., repatriate, arrest, refer for prosecution, and also to disrupt and deter human smuggling.¹² While it is unlikely that a migrant interdicted at sea has already been afforded Section 1367 status, it is possible that aliens originally interdicted at sea are victims of human smuggling or trafficking,

¹¹ A recent improvement is that USCIS is now able to transmit the file on a daily basis to OBIM by email. The first daily 1367 file was sent to OBIM on August 29, 2018. USCIS and OBIM are working on an automated, real time solution. USCIS Privacy expects that the process of automated updates will be implemented by the end of the first quarter of CY2019.

¹² DHS/USCG/PIA-002 USCG Biometrics at Sea PIA available at <https://www.dhs.gov/publication/dhsuscgpia-002-uscg-biometrics-sea>.



and are later afforded 1367 protections, and that such information may be disclosed pursuant to repatriation, arrest, or prosecution. USCG systems do not receive updates of Section 1367 information from USCIS, nor do its biometrics-based sharing with IDENT provide USCG with caveats. PRIV and CRCL are unaware of any specific instances of wrongful disclosure, however, without a policy in place to at least identify Section 1367 information, as required by DHS Directive 002-02 and DHS Instruction 215-01-002, it is difficult to prove or disprove whether USCG operators handle 1367 information.

ICE: ICE has no Component-specific Section 1367 policy. ICE personnel receive training to implement the DHS Directives and Instruction on Section 1367 information. ICE Enforcement and Removal Operations (ERO) identifies aliens who are protected by Section 1367 from information provided by USCIS. USCIS transmits a daily batch file that reflects the cumulative list of all aliens USCIS has identified as applying for these protections. This information is transferred to ERO systems via an information-sharing link with USCIS systems. Once the file is received, all 1367-protected aliens on the list, who are also in the Enforcement Integrated Database (EID),¹³ are flagged in the system. This generates an alert to any user reviewing records within EID that the alien whose information they are viewing is protected by Section 1367. ICE IT systems are configured to block users of public-facing systems (e.g., Online Detainee Locator System) from accessing information about individuals with Section 1367 protection. ICE officers may also directly query USCIS's Central Index System¹⁴ to ascertain whether a particular alien has applied for Section 1367 protections on a case-by-case basis.

ICE does not have a formal form or fields in applicable case management systems devoted specifically to tracking Section 1367 disclosures. When ICE discloses Section 1367 information pursuant to a valid exception directly from a case management system, the disclosure may be documented in the open-text field of that system. Often, however, disclosures are made via email. In these cases permitted disclosures are documented in the transmitted message itself. If ICE program offices have questions about whether disclosure of Section 1367 information is appropriate, they may contact the ICE Privacy Division and the ICE Office of the Principal Legal Advisor (OPLA) for guidance. ICE reports that within its existing system configurations there are no means to perform audits of Section 1367 disclosures outside of a manual review, which would be problematic from a resource perspective, given the number of individuals who have Section 1367 confidentiality. If there is an allegation of wrongful disclosure, those investigating the allegation would review relevant ICE records to determine whether there was, in fact, an unauthorized disclosure. ICE implemented this process for two incidents that were first reported to PRIV in FY2017, both of which have since been remediated and closed.

¹³ DHS/ICE/PIA-015 Enforcement Integrated Database (EID) Criminal History Information Sharing (CHIS) Program PIA available at <https://www.dhs.gov/publication/dhsicepia-015h-enforcement-integrated-database-eid-criminal-history-information-sharing>.

¹⁴ DHS/USCIS/PIA-009 Central Index System PIA available at <https://www.dhs.gov/publication/dhsuscispio-009-central-index-system>.



CBP: CBP has no Component-specific Section 1367 policy. The CBP Privacy and Diversity Office reports that CBP has an automated exchange with USCIS supporting the identification of 1367 records for authorized data sharing purposes. Similar to ICE, CBP receives daily uploads from USCIS. CBP has created a central service to provide the file or support screening against the file in a common manner. CBP has implemented screening for most data sharing interfaces to ensure that Section 1367 records are not shared outside the authorized agencies. CBP is working to ensure that all interfaces are screened as required. CBP is also working to ensure that all on-line queries against its main information-sharing platform, TECS,¹⁵ by users outside the authorized agencies are screened against the Section 1367 records before results are returned to the end user. CBP should have this implemented by mid-FY19 (February 2019). TECS maintains transactional logs and has extensive auditing capabilities that allow CBP to review how the data is shared. TECS MOUs created over the last three years contain specific information and instructions for handling Section 1367 data.

Bulk-sharing Findings: USCIS does not comply with PM-602-0136 with regard to biometric-based bulk sharing with the FBI

USCIS currently bulk shares information to the FBI's Next Generation Identification (NGI), an electronic repository of biometric and criminal history information used for criminal justice purposes and background checks.¹⁶ USCIS PM-602-0136 requires that bulk sharing of information be covered under an ISAA that establishes the conditions and procedures for identifying, sharing, and retaining Section 1367 information. USCIS has not identified an ISAA for this sharing. Moreover, USCIS shares this information through its biometric-based IDENT connection, which does not affix the Section 1367 caveat, as discussed above.

Although PRIV has no knowledge of any specific improper disclosure of 1367 information, based on how the FBI controls responses to non-criminal justice queries, there is a possibility that information on one of the 50,000 Section 1367-protected individuals sent to NGI could be shared when a non-criminal justice agency query matches to a criminal record in NGI of an individual protected under Section 1367. In that circumstance, the individual's criminal history, plus some limited biographic information, from the Section 1367 civil records retained in NGI might be shared with the non-criminal justice agency. Disclosure of any of this information (whether civil or criminal) to a non-criminal justice agency for background checks or for other non-law enforcement needs could be a violation of Section 1367. USCIS bulk sharing with NGI is an open incident in ECOP and has been reported to CRCL.

¹⁵ DHS/CBP/PIA-021 TECS System: Platform PIA available at <https://www.dhs.gov/sites/default/files/publications/DHS-PIA-ALL-021%20TECS%20System%20Platform.pdf>.

¹⁶ NGI Privacy Impact Assessments available at <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments>.



Summary of Findings:

This PCR finds that Component-system Section 1367 information identification, updates, caveat marking, screening, and disclosure audit capabilities vary in reliability. Policies conforming to the relevant Directives and Instructions provide a clear, considered approach to updating and handling Section 1367 records, reduce the likelihood of human error, and increase confidence in system reliability. The following risks may be linked to the absence of a Component-specific policy:

- OBIM's failure to update its system with Section 1367 protected individuals resulted in months of potential unauthorized disclosures.
- USCG has not configured its systems to identify possible Section 1367 information.
- CBP has not yet implemented safeguards for all of its Section 1367 information from system users who are not authorized to receive it.
- ICE has not configured its systems to be able to account for Section 1367 information disclosures, and instead must rely on manual review in response to a wrongful disclosure allegation.

Findings also indicate that USCIS's PM-602-0316 does not address the ISAA requirements for direct third party access to USCIS systems; consequently, it is not clear whether all third party access to its systems is authorized. Component policies or SOPs should specify how third party access must be managed to protect 1367 information confidentiality, including through ISAAs, as required by Directive 002-02. ISAAs must be appropriately worded to ensure that both the system owner and the third party have assessed whether access to 1367 information is appropriate. Without documentation, there may not be an analysis of whether such users are legally authorized to receive 1367 information.

Finally, findings indicate that records shared through biometrics, including those bulk-shared by USCIS with the FBI through IDENT, are not affixed with the caveats against onward disclosure required by Instruction 215-01-001. It is unclear whether the bulk sharing with FBI is covered by an ISAA.

V. Recommendations

Based on findings described above, PRIV recommends the following:

***Recommendation 1:** Components with systems containing Section 1367 information, including all Components with a criminal justice law enforcement or immigration law enforcement mission, should develop implementing instructions, SOPs, or other policy guidance to ensure compliance with the confidentiality rules under Section 1367, tailored to the specific context of their missions and systems.*



This is already required under Directive 002-02, Directive 215-01, and Instruction 215-01-001. Component-specific implementing instructions or policy guidance should be developed in coordination with USCIS and CRCL, per Instruction 215-01-001. Such policies should include:

- a. The process for how Section 1367 information is identified and kept current in all relevant systems that contain Section 1367 information.
- b. Instruction on how to manage third party system access to Section 1367 information.
- c. How Section 1367 disclosures are reviewed and documented and, if feasible, a means to audit those disclosures.
- d. How systems affix caveats to Section 1367 information.

Recommendation 2: By September 2019, USCIS must report system access inventory findings to PRIV and CRCL, including how it has addressed gaps in 1367 confidentiality protections.

The USCIS Privacy Office PCR response indicates that numerous external entities to DHS currently have access to Section 1367 information through various means, and that the access is not documented in a consistent fashion. As of September 2018, USCIS Privacy began conducting an in-depth review of all USCIS systems to account for SPC related information, including 1367 information, and to ensure appropriate protections are in place. PRIV commends USCIS for initiating this report. Submission of the findings to PRIV and CRCL is consistent with coordination requirements in the Directives and Instructions outlined above.

Recommendation 3: USCIS must identify an ISAA with FBI that covers bulk sharing.

USCIS must address the possible risk of sharing bulk information with FBI's NGI without an ISAA that addresses identification and handling of Section 1367 information. PM-602-0136 5. B. states that bulk sharing of information is accomplished pursuant to an ISAA coordinated among DHS OGC, PRIV, and CRCL. The terms of the ISAA must be consistent with DHS Directive 215-001 and Instruction 215-01-002.

Recommendation 4: By February 2019, CBP will report to PRIV and CRCL whether all of its system interfaces and online query responses are configured to ensure only authorized users receive 1367 records, with caveats, as appropriate.

CBP must address the risk of sharing 1367 information with unauthorized recipients through its system interfaces and online query capabilities. It must also ensure that authorized recipients are aware that they are receiving 1367 information, either through caveats affixed to the records or through another means identified under the relevant DHS Directive or Instruction cited above. CBP has stated that all of its system interfaces and online query responses should be configured to ensure only authorized users receive 1367 records, with caveats, as appropriate, by mid-FY19. The report may include an audit of TECS transactions to demonstrate the changes to configurations.



VI. Conclusion

The existing Departmental Delegation, Directives, and Instructions direct Components to draft and implement policies for protecting Section 1367 information. The recommendations of this PCR are intended to provide Components with a means to improve compliance and further enhance the privacy-protective processes for 1367 information. CRCL, USCIS, and the CCVAW provide leadership and resources to assist Components in this endeavor. The DHS Privacy Office will continue to monitor Section 1367 incidents and will determine the need for future PCRs through discussions with CRCL, USCIS, and the CCVAW. As such, the DHS Privacy Office requests that CBP, ICE, USCIS, USCG, I&A, and OBIM Privacy Offices:

- Monitor the implementation of the recommendations of this PCR, and
- Provide PRIV and CRCL a written report on the implementation status of all recommendations within one year of this PCR's publication date. For any recommendation not implemented in that timeframe, or that a Component chooses not to implement, including any best practice recommendation, please explain why the recommendation was not implemented.

VII. Privacy Compliance Review Approval

Responsible Officials

Cameron Quinn, Officer for Civil Rights and Civil Liberties

Kevin K. McAleenan, Commissioner, U.S. Customs and Border Protection

Ronald D. Vitiello, Senior Official Performing the Duties of the Director, U.S. Immigration and Customs Enforcement

L. Francis Cissna, Director, U.S. Citizenship and Immigration Services

Admiral Karl L. Shultz, Commandant, U.S. Coast Guard

David J. Glawe, Under Secretary, Office of Intelligence and Analysis

Shonnie R. Lyon, Director, Office of Biometric Identity Management



**Homeland
Security**

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security



**Homeland
Security**

APPENDIX A

**DHS and Component Delegations, Directives, and Instructions Providing DHS-wide
Guidance and Oversight on the Implementation of Section 1367 Confidentiality and
Prohibited Source Provisions**

**DELEGATION OF
AUTHORITY TO ISSUE
GUIDANCE AND
IMPLEMENT
8 UNITED STATES CODE
1367**

I. Purpose

This Delegation vests the authority described herein in the DHS Officer for Civil Rights and Civil Liberties.

II. Delegation

Subject to my oversight, direction, and guidance, I hereby delegate to the Officer for Civil Rights and Civil Liberties the authority to provide DHS-wide guidance and oversight on the implementation of 8 United States Code (U.S.C.) Section 1367 confidentiality and prohibited source provisions (relating to applicants for and beneficiaries of Violence Against Women Act (VAWA), T visa, or U visa protections) in accordance with 8 U.S.C. 1367(d) and Section 810 of the Violence Against Women Reauthorization Act of 2013, provided that such authority will be exercised only in accordance with policies and procedures established by implementing departmental Directives or Instructions.

III. Re-delegation

Unless re-delegation is otherwise prohibited by Law or Executive Order, the authorities, responsibilities, and functions delegated herein may be re-delegated in writing to any appropriate subordinate official.

IV. Authorities

A. Title 8, U.S.C., Section 1367, "Penalties for disclosure of information" (originally enacted as Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA));

B. Section 102 of the Homeland Security Act of 2002, Pub. L. No. 107-296, as amended, Title 6 U.S.C. § 112;

C. Immigration and Nationality Act, Pub. L. No. 82-414, as amended, Section 103(a), 8 U.S.C. § 1103(a);

D. 8 Code of Federal Regulations 2.1

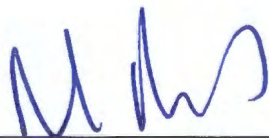
E. Violence Against Women Reauthorization Act of 2013 (VAWA 2013), Public Law 113-4, Section 810, "Disclosure of Information for National Security Purposes."

V. Definitions

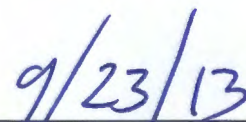
The term "1367 Information" refers to any information relating to aliens who are seeking or have been approved for immigrant status as battered spouses, children and parents under provisions of the Violence Against Women Act (VAWA), as victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T visa), or as victims of certain criminal activity who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities (U visa). This definition includes records or other information that does not specifically identify the individual as an applicant for or beneficiary of the T visa, U visa, or VAWA protections.

VI. Office of Primary Interest

The Office for Civil Rights and Civil Liberties, U.S. Citizenship and Immigration Services, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement are the Components of primary interest in this Delegation.



Rand Beers
Acting Secretary of Homeland Security



Date

COUNCIL ON COMBATING VIOLENCE AGAINST WOMEN

I. Purpose

This directive establishes the Department of Homeland Security (DHS) Council on Combating Violence Against Women ("Council") and its membership, and outlines the Council functions, coordination responsibilities, and operating procedures.

The Council focuses on advancing overall knowledge of and compliance with the Violence Against Women Act (VAWA), the Victims of Trafficking and Violence Protection Act (VTVPA), subsequent reauthorizations of those laws, and related immigration laws and issues, as well as the provision of training and resources to stakeholders and the public as appropriate.

II. Scope

This directive applies to the following DHS Components: Office of Policy, Office of General Counsel, Office of Policy's Office for State and Local Law Enforcement, Office for Civil Rights and Civil Liberties, Office of Intergovernmental Affairs, Office of Legislative Affairs, Office of the Citizenship and Immigration Services Ombudsman, Office of Public Affairs, U.S. Citizenship and Immigration Services, U.S. Immigration and Custom Enforcement, Customs and Border Protection, the Federal Law Enforcement Training Center, the Office of the Secretary, including a member from the DHS Blue Campaign, the Office of Health Affairs, and any other Component who has programming and policy responsibilities that relate to the protection of individuals who are the victims of domestic violence and other crimes enumerated in the VAWA or VTVPA and their reauthorizations, such as the U.S. Coast Guard, as they relate to the administration of our immigration laws.

III. Authorities

- A. The Homeland Security Act of 2002, codified in Title 6, United States Code (U.S.C.) Pub. L. 107-296, 116 Stat. 2135 (2002).

- B. Violence Against Women Act of 1994, codified in Title 6, §§ 40001-40703 of the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. 103-322, 108 Stat. 1902
- C. Victims of Trafficking and Violence Protection Act of 2000, 22 U.S.C. 7101, Pub. L. 106-386, 114 Stat. 1464
- D. Trafficking and Victims Protection and Reauthorization Act of 2003, Pub L. 108-193 (2003)
- E. Violence Against Women Reauthorization Act of 2005, Pub. L. 109-162, (2005)
- F. William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA), Pub. L. 110-457, 122 Stat. 5044 (2008)

IV. Responsibilities

- A. The Co-Chairs manage the execution of this Directive. The **Office of Policy's Assistant Secretary for State and Local Law Enforcement** and an **appointee designated by the Secretary** are the appointed co-chairs of the Council.
- B. The enumerated **Component heads**:
 - 1. Appoint an individual(s) responsible for coordinating DHS efforts on the Council to combat violence against women.
 - 2. Develop a written process for evaluating their component's efforts in support of this Directive.

V. Policy and Requirements


Policy. Through the Council, DHS ensures that policies combating violence against women are consistent department-wide. As "One DHS", it is important to ensure that the Department continues to work together to address these issues. By identifying opportunities to build consensus on challenging issues across the Department's components, implementing best practices throughout the Department, and coordinating efforts Department-wide, this Council supports the Department's missions of effectively administering the laws preventing violence against women and enhancing homeland security for all. This Council also formally recognizes the important steps the Department has taken to place protections in effect that prevent and combat violence against women, including domestic violence and other crimes.

Requirements:

- A. The Council:
 - 1. Coordinates with the White House and Federal agencies to support DHS strategies to combat violence against women and children.
 - 2. Engages with the public to discuss issues that impact the protection of victims of domestic violence and other crimes.
 - 3. Develops and coordinates the implementation of strategies to support compliance with immigration laws and addresses affiliated issues as they relate to victims of domestic violence and other crimes enumerated in the VAWA and VTVPA.
 - 4. Makes recommendations to the Secretary on an as needed basis.
- B. All Components submit quarterly reports to the Council identifying efforts, priorities and accomplishments related to combating violence against women.
- C. The Co-Chairs report bi-annually to the Secretary.

VI. Questions

Address any questions or concerns regarding this Directive to the Assistant Secretary of the Office of State and Local Law Enforcement.



Rafael Borrás
Under Secretary for Management

3/14/13
Date

THE COUNCIL ON COMBATING VIOLENCE AGAINST WOMEN

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 002-01, The Council on Combating Violence Against Women (“Council”) and its membership, and outlines the Council functions, coordination responsibilities, and operating procedures.

The Council focuses on advancing overall compliance with, and knowledge about, the Violence Against Women Act (VAWA), the Victims of Trafficking and Violence Protection Act (VTVPA), subsequent reauthorizations of those laws, and related immigration laws and issues, and the provision of training and resources to stakeholders and the public as appropriate.

II. Scope

This Instruction applies to the following DHS Components: Office of Policy, Office of General Counsel, Office of Policy’s Office for State and Local Law Enforcement, Office for Civil Rights and Civil Liberties, Office of Intergovernmental Affairs, Office of Legislative Affairs, Office of the Citizenship and Immigration Services Ombudsman, Office of Public Affairs, U.S. Citizenship and Immigration Services, U.S. Immigration and Custom Enforcement, Customs and Border Protection, the Federal Law Enforcement Training Center, the Office of Health Affairs, the immediate Office of the Secretary, including a member of the DHS Blue Campaign, and any other component who has programming and policy responsibilities that relate to the protection of individuals who are the victims of domestic violence and other crimes enumerated in the VAWA or VTVPA and their reauthorizations, such as U.S. Coast Guard, as they relate to the administration of our immigration laws.

III. References

- A. The Homeland Security Act of 2002, codified in Title 6, United States Code (U.S.C.) Pub. L. 107-296, 116 Stat. 2135 (2002).

- B. Violence Against Women Act of 1994, codified in Title 6, §§ 40001-40703 of the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. 103-322, 108 Stat. 1902.
- C. Victims of Trafficking and Violence Protection Act of 2000, 22 U.S.C. 7101, Pub. L. 106-386, 114 Stat. 1464.
- D. Trafficking and Victims Protection and Reauthorization Act of 2003, Pub L. 108-193 (2003).
- E. Violence Against Women Reauthorization Act of 2005, Pub. L. 109-162, (2005).
- F. William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA), Pub. L. 110-457, 122 Stat. 5044 (2008).

IV. Definitions

- A. **Department of Health and Human Service (HHS) Family Violence Prevention and Services Program:** The primary Federal funding stream dedicated to the support of emergency shelter and related assistance for victims of domestic violence and their dependents. Funding to the States, Territories, and Tribes provides core support to more than 1,500 community-based domestic violence programs.
- B. **Department of Justice (DOJ) Office of Violence Against Women (OVW):** The administrator of financial and technical assistance to communities across the country that are developing programs, policies, and practices aimed at ending domestic violence, dating violence, sexual assault, and stalking.
- C. **Co-Chairs of the Council:** Consists of the Office of Policy, Assistant Secretary for State and Local Law Enforcement and an appointee designated by the Secretary.

V. Responsibilities

- A. The **Co-Chairs of the Council:**
 - 1. Manage the Council, ensuring it is staffed appropriately, and may rotate staffing responsibilities.
 - 2. Develop strategies to support Department compliance with VAWA and TVPRA and identify and address additional issues as they

relate to victims of domestic violence and other crimes enumerated in the VAWA and VTVPA.

3. Implements and oversees DHS policies regarding combating violence against women and works with the Components to integrate all programs used within the Department.
4. Coordinate an annual DHS agenda that supports the implementation of strategies to combat violence against women, and addresses related issues.
5. Lead the formulation of annual goals and objective, along with projected outcomes, for the Council.
6. Determine annually the appropriate evaluation methods for the goals and objectives to be utilized by the Council.
7. Coordinate with Component Heads to facilitate appropriate designations for representation on the Council.
8. Report bi-annually to the Secretary on the Council's priorities and accomplishments.

B. The **Component Heads:**

1. Appoint a representative(s) of the component to the Council, who is familiar with programming, legal, and policy issues that relate to the protection of victims under VAWA and the VTVPA.
2. Develop quarterly reports to the Council identifying efforts, priorities and accomplishments related to combating violence against women
3. Ensure compliance in their agency with VAWA Confidentiality provisions.

C. The **Component Representatives:**

Identify gaps and systemic issues in the protection of battered immigrants, including women and children, and coordinate efforts to address these issues, including, but not limited to VTVPA and VAWA issues and other issues of special impact on women.

1. Facilitate DHS collaboration and communication about related issues with stakeholders, including federal, state, and local law enforcement, other federal, state, and local government partners,

and advocates for women, and relevant officials from the Executive Office of the President.

2. Coordinate inter-agency communication and partnerships between their component and Federal government partners including, but not limited to, the White House, the Department of Health and Human Service's Family Violence Prevention and Services Program, and the Department of Justice's Office of Violence against Women.
3. Coordinate with the DHS Office of Public Affairs and, subsequently, the White House Council on Women and Girls to educate the public about DHS efforts to combat violence against women.
4. Contribute comments and suggestions to relevant components during development of legislation and regulations related to VAWA and VTVPA and reauthorizations, and other relevant legislation or regulations.

VI. Content and Procedures

A. Council Membership

1. The Council consists of one representative from the following components: Customs and Border Protection (CBP), Office of the Citizenship and Immigration Services Ombudsman (CISOMB), Office for Civil Rights and Civil Liberties (CRCL), Federal Law Enforcement Training Center (FLETC), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Office of the General Counsel (OGC), Office of Intergovernmental Affairs (IGA), Office of Public Affairs (OPA), Office of the Secretary (OSEC), Office of Policy (PLCY), Office of Policy's Office for State and Local Law Enforcement (OSLLE), Office of Legislative Affairs (OLA), the Office of Health Affairs (OHA), the Immediate Office of the Secretary, including a member of the DHS Blue Campaign, any other component who has programming and policy responsibilities that relate to the protection of individuals who are the victims of domestic violence and other crimes enumerated in the VAWA or VTVPA and their reauthorizations, such as U.S. Coast Guard.

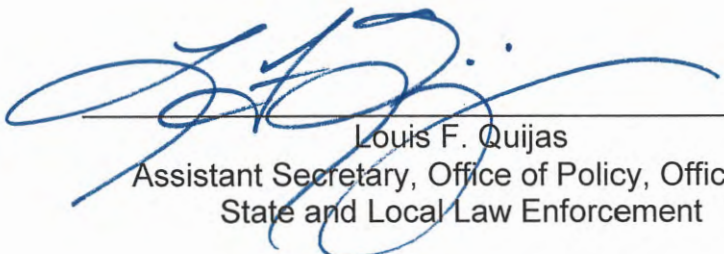
B. Operating Procedures

1. The Council meets at least quarterly. Council Committees may meet in addition to the quarterly meetings.

2. Council Meetings should be announced to the participants in advance and be held during normal working hours.
3. Council members:
 - a. Attend all meetings personally or through a designated surrogate.
 - b. Monitor the progress of efforts in their own component or office and update the Council on the initiatives, policy announcements and related information.
 - c. Bring SMEs from their office or component as needed.

VII. Questions

Address any questions or concerns regarding this Directive to the Assistant Secretary of the Office for State and Local Law Enforcement.



Louis F. Quijas
Assistant Secretary, Office of Policy, Office for
State and Local Law Enforcement



Date

IMPLEMENTATION OF SECTION 1367 INFORMATION PROVISIONS

I. Purpose

This directive establishes a single Department of Homeland Security (DHS) policy regarding the implementation of Title 8, United States Code (U.S.C.), Section 1367, Violence Against Women Act (VAWA) confidentiality provisions and provides guidance as instructed by 8 U.S.C. 1367(d), as amended by the Violence Against Women Reauthorization Act of 2013, Public Law 113-4, section 810.

II. Scope

This directive applies throughout DHS, particularly those employees who work with applicants for victim-based immigration relief or who have access to protected information, such as United States Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP).

III. Authorities

- A. Public Law 101-649, "Immigration and Nationality Act" (INA) Section 101(a)(51), as codified in 8 U.S.C. Section 1101(a)(51)
- B. Public Law 103-322, "Violence Against Women Act (VAWA) of 1994"
- C. Public Law 106-386, "Victims of Trafficking and Violence Protection Act of 2000." (VTVPA)
- D. Public Law 109-162, "Violence Against Women and Department of Justice Reauthorization Act of 2005," Section 817, "VAWA Confidentiality Nondisclosure." (VAWA 2005)
- E. Public Law 113-4, "Violence Against Women Reauthorization Act of 2013," Section 810, "Disclosure of Information for National Security Purposes." (VAWA 2013)
- F. Section 239(e) of the Immigration and Nationality Act (INA) (8 U.S.C. 1229(e)), "Certification of compliance with restrictions on disclosure"

- G. Section 240A(b)(2) of the Immigration and Nationality Act (INA) (8 U.S.C. 1229(b)), “Special Rule for Battered Spouse or Child”
- H. Title 8, U.S.C., Section 1367, “Penalties for disclosure of information” (originally enacted as Section 384 of the Illegal Immigrant Reform and Immigrant Responsibility Act of 1996 (IIRIRA))
- I. Title 42, U.S.C., Section 13925(a), “Definitions and grant provisions” (as re-designated and amended by Section 3 of VAWA 2013), Public Law 113-4
- J. Delegation 19004, Delegation of Authority to Implement Section 1367 Information
- K. Instruction 002-02-001, Implementation of Section 1367 Information Provisions
- L. DHS Privacy Incident Handling Guidance (Jan. 26, 2012)

IV. Responsibilities

All responsible parties listed below are to help ensure compliance with applicable policies and procedures set forth in this Directive.

- A. The **Chief Privacy Officer** is the senior official within the Department with primary responsibility for privacy compliance and policy.
- B. The **Officer for Civil Rights and Civil Liberties (CRCL)** directs and oversees the implementation of the integration of civil rights and civil liberties across the Department and has the delegated authority to issue this Directive and Instruction.
- C. The **General Counsel** is responsible for ensuring legal compliance and has final authority and responsibility for legal policy determinations within the Department and its Components.
- D. The **Component Heads** with any Section 1367 information that might be shared will implement and execute all applicable policies and procedures set forth in this directive, and will develop any necessary implementing instructions or other policy guidance to the extent permitted by and consistent with their authorities and any restrictions imposed by statute, executive order, presidential or other Instruction, or national or departmental policy.
- E. The **Council on Combating Violence Against Women** works to ensure that policies and practices for combating violence against women and

children are consistent Department-wide. By identifying opportunities to build consensus on challenging issues across Components, sharing best practices, and coordinating efforts Department-wide, the Council supports the Department's missions of effectively administering the laws preventing violence against women and children. The Council collects information on a quarterly basis and conduct after-action reviews on cases where exceptions have been applied to disclose information and where enforcement actions have been taken at sensitive locations. The Council is also responsible for assisting in developing all implementing policies that are created by Components.

- F. The **Federal Law Enforcement Training Center (FLETC)** ensures the computer-based training module, *VAWA: Confidentiality and Immigration Relief*, is available to all Components for promulgation through their Learning Management Systems and provides assistance to keep the training updated and current, as necessary.

V. Policy and Training Requirements

Policy: The policy is comprised of three confidentiality requirements:

- A. All DHS officers and employees are generally prohibited from permitting use by or disclosure to anyone other than a sworn officer or employee of DHS, Department of State (DOS), or Department of Justice (DOJ) of any information relating to a beneficiary of a pending or approved application for victim-based immigration benefits, including a battered spouse or child hardship waiver, VAWA self-petition, VAWA cancellation of removal or suspension of deportation case, or T or U nonimmigrant status, including the fact that they have applied for such benefits. There are certain exceptions to the general nondisclosure requirement, such as information to be used solely for a legitimate national security purpose in a manner that protects the confidentiality of such information. (Please note that different procedures apply for the disclosure of information to national security officials and can be found at Instruction 215-01-001, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes).
- B. Adverse determinations of admissibility or deportability against an alien are not made using information furnished solely by prohibited sources associated with the battery or extreme cruelty, sexual assault, human trafficking or substantial physical or mental abuse, regardless of whether the alien has applied for VAWA benefits, or a T or U visa. For a more information on what qualifies as a VAWA benefit, refer to Instruction 002-02-001, Implementation of Section 1367 Provisions. If a DHS employee receives adverse information about a victim of domestic violence, sexual assault, human trafficking or an enumerated crime from a prohibited

source, DHS employees should treat the information as inherently suspect and exercise all appropriate prosecutorial discretion with respect to pursuing the adverse information. Further, DHS employees receiving information solely from a prohibited source do not take action on that information unless there is an independent source of corroboration.

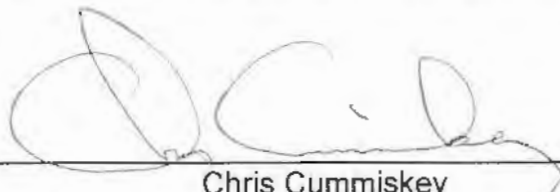
- C. DHS employees complete a certification of compliance in cases where enforcement actions leading to a removal proceeding are taken at sensitive locations, as required by INA 239(e) (8 U.S.C. 1229(e)). The certification includes the Notice to Appear, which affirms compliance with the Section 1367 Information and prohibited source provisions.

Component requirements: Components with access to Section 1367 Information that might be shared with those outside of the DHS develop any necessary implementing instructions or other policy guidance to the extent permitted by and consistent with their authorities and any restrictions imposed by statute, executive order, presidential or other instruction, or national or departmental policy. Components coordinate with the Council in the development of implementing policy. Moreover, any Component with access to Section 1367 information creates ways to identify those individuals protected by Section 1367 confidentiality, such as through a Central Index System (CIS) database check, and develops safeguards to protect this information in the relevant systems.

Training requirement: All DHS employees who, through the course of their work may come into contact with victim applicants or have access to information covered by 8 U.S.C. 1367 complete the *VAWA: Confidentiality and Immigration Relief* training, which is currently on Component's Learning Management Systems (LMS). The VAWA Training was developed by FLETC in collaboration with subject-matter experts from several DHS Components, including USCIS, ICE and CBP. No later than 180 days after the enactment of this policy, and on an annual basis thereafter, the Component Heads, or his or her delegates, of CIS OMB, CRCL, USCIS, ICE and CBP report to the Review Committee the rate of compliance for this training.

VI. Questions

Address any questions or concerns regarding this Directive to CRCL.


Chris Cummiskey
Acting Under Secretary for Management


Date

DISCLOSURE OF SECTION 1367 INFORMATION TO NATIONAL SECURITY OFFICIALS FOR NATIONAL SECURITY PURPOSES

I. Purpose

This Directive serves as the principal reference for disclosing any information related to applicants for or beneficiaries of T Visa, U Visa, or Violence Against Women Act (VAWA) protections ("Section 1367 information") for National Intelligence (including Foreign Intelligence and Counterintelligence) purposes to elements of the Intelligence Community or for counterterrorism purposes to elements of the Intelligence Community, other Federal departments and agencies, and foreign government entities.

II. Scope

This Directive applies throughout the Department of Homeland Security (DHS). It does not affect the disclosure of Section 1367 information in accordance with Title 8, United States Code (U.S.C.), Section 1367(b)(1)-(7).

III. Authorities

- A. Title 6, United States Code (U.S.C.), Section 112, "Secretary; functions"
- B. Title 8 U.S.C., Sections 1101(a)(15)(T), (a)(15)(U), (a)(51)
- C. Title 8, U.S.C., Section 1103, "Powers and duties of the Secretary, the Under Secretary, and the Attorney General"
- D. Title 8, U.S.C., Section 1367, "Penalties for Disclosure"
- E. Title 50, U.S.C., Chapter 15, "National Security Act of 1947," as amended
- F. Executive Order (E.O.) 12,333, "U.S. Intelligence Activities," as amended
- G. E.O. 13,388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans"

- H. Privacy Incident Handling Guidance (Jan. 26, 2012)
- I. DHS Directive 002-02, "Implementation of Section 1367 Information Provisions"
- J. DHS Instruction 002-02-001, "Implementation of Section 1367 Information Provisions"

IV. Responsibilities

- A. The **Officer for Civil Rights and Civil Liberties (CRCL)** directs and oversees the implementation of the integration of civil rights and civil liberties across the Department, serving as the foundational DHS organization through which all Department-wide civil rights and civil liberties activities are overseen, defined, and measured, including the disclosure of Section 1367 Information. The Officer for CRCL manages the execution of this Directive.
- B. The **Under Secretary for Intelligence and Analysis (I&A)** serves as the Chief Intelligence Officer for the Department, exercising leadership and authority over intelligence policy and programs throughout the Department and, acting in conjunction with, and without preempting the authorities of the DHS Chief Information Officer and the DHS Chief Security Officer, exercising leadership over information sharing and safeguarding policy and programs throughout the Department in partnership with the Heads of Components, including with respect to the disclosure of information related to applicants for or beneficiaries of T Visa, U Visa or VAWA protections.
- C. The **Director of U.S. Citizenship and Immigration Services (USCIS)** oversees lawful immigration to the United States by establishing national immigration services policies and priorities, including with respect to the maintenance and disclosure of information related to applicants for or beneficiaries of T Visa, U Visa or VAWA protections.
- D. The **Chief Privacy Officer** is the senior official within the Department with primary responsibility for privacy compliance and policy, including with respect to the disclosure of information related to applicants for or beneficiaries of T Visa, U Visa or VAWA protections.
- E. The **Heads of Components** implement and execute all applicable policies and procedures set forth in this Directive and any implementing instructions or other policy guidance to the extent permitted by and consistent with their authorities and any restrictions imposed by statute, executive order, presidential or other directive, or national or departmental

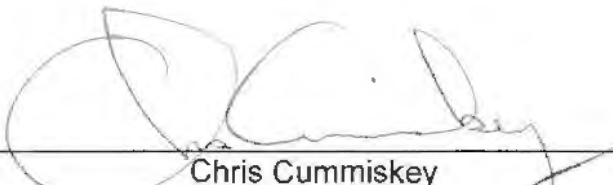
policy.

V. Policy and Requirements

- A. Consistent with applicable law, presidential directive, regulation, and national and departmental policy, Component Heads or their designees, in coordination with the Director of USCIS or his designees, disclose Section 1367 information to other Federal departments or agencies and foreign entities solely in furtherance of those entities' authorized counterterrorism functions, or to elements of the Intelligence Community for authorized intelligence functions in support of national missions or counterterrorism functions, and only in accordance with procedures for the Component jointly developed by the Component, I&A, USCIS, and CRCL.
- B. Only Section 1367 information that constitutes terrorism information (or, with respect to elements of the Intelligence Community outside the Department, as information determined to be relevant to the element's authorized intelligence function(s) in support of national missions) is permanently retained by the entity to which the information is disclosed.

VI. Questions

Address any questions or concerns regarding this Directive to CRCL.


Chris Cummiskey
Acting Under Secretary for Management

11/6/13
Date

DISCLOSURE OF SECTION 1367 INFORMATION TO NATIONAL SECURITY OFFICIALS FOR NATIONAL SECURITY PURPOSES

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 215-01, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes Title 8, United States Code (U.S.C.), Section 1367(b)(8), with respect to the disclosure of any information related to applicants for or beneficiaries of T Visa, U Visa or Violence Against Women Act (VAWA) protections ("Section 1367 information") for National Intelligence (including Foreign Intelligence and Counterintelligence) purposes to elements of the Intelligence Community or for counterterrorism purposes to elements of the Intelligence Community, other Federal departments and agencies, and foreign government entities.

II. Scope

This Instruction applies throughout DHS. It does not affect the disclosure of Section 1367 information in accordance with Title 8, United States Code (U.S.C.), Section 1367(b)(1)-(7).

III. References

- A. Title 6, U.S.C., Section 112, "Secretary; functions"
- B. Immigration and Nationality Act (INA), Title 8, U.S.C., Sections 1101(a)(15)(T), (a)(15)(U), (a)(51)
- C. INA, Title 8, U.S.C., Section 1103, "Powers and duties of the Secretary, the Under Secretary, and the Attorney General"
- D. INA, Title 8, U.S.C., Section 1367, "Penalties for Disclosure"
- E. Title 50, U.S.C., Chapter 15, "National Security Act of 1947," as amended
- F. Executive Order (E.O.) 12,333, "U.S. Intelligence Activities," as amended

- G. E.O. 13,388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans"
- H. DHS Privacy Incident Handling Guidance (Jan. 26, 2012)
- I. DHS Directive 002-02, "Implementation of Section 1367 Information Provisions"
- J. DHS Instruction 002-02-001, "Implementation of Section 1367 Information Provisions"

IV. Definitions

- A. **Counterintelligence**: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
- B. **Foreign Intelligence**: Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.
- C. **Information**: Any knowledge such as facts or opinions, data, numbers, or graphics, whether in digital, textual, oral or other forms, and whether maintained in any medium, including but not limited to computerized data bases, paper, microform, magnetic tape, and other digital storage solutions.
- D. **Intelligence**: A collection of acquired, analyzed, and synthesized information, that is of tactical, operational, or strategic value. It includes foreign intelligence and counterintelligence as defined by Executive Order 12333, December 4, 1981, as amended, or by a successor order.
- E. **Intelligence Community**: The United States Intelligence Community as defined at Title 50, United States Code, Section 401a, "Definitions," and Executive Order No. 12,333, "United States Intelligence Activities, Section 3.5, as amended.
- F. **National Intelligence**: All Intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that (1) pertains to more than one United States government agency; and (2) that involves (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use

of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security.

- G. **Section 1367 Information:** Any information relating to aliens who are seeking or have been approved for immigrant status as battered spouses, children and parents under provisions of the Violence Against Women Act (VAWA), as victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities, or as aliens who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities. This definition includes records or other information that do not specifically identify the individual as an applicant or beneficiary of the T Visa, U Visa, or VAWA protections. Section 1367 covers information relating to beneficiaries of applications for a number of immigration benefits, not just the Form I-360 VAWA self-petition. For the purpose of this guidance if an alien is the beneficiary of a pending or approved application for one or more of the victim-based benefits described below, the requirements of 8 U.S.C. 1367 is followed:

1. VAWA self-petitioner, which incorporates the following applications or petitions:
 - a. I-360 Self-petition - self-petitioners under INA sec. 204
 - b. I-751 Hardship waiver - battered spouse or child hardship waiver
 - c. VAWA CAA - abused Cuban Adjustment Act applicants
 - d. VAWA HRIFA - abused Haitian Refugee Immigration Fairness Act applicants
 - e. VAWA NACARA - abused Nicaraguan Adjustment and Central American Relief Act applicants
 - f. VAWA Suspension of Deportation
2. VAWA Cancellation of Removal applicants under INA section 240A(b)(2)
3. I-914 T Nonimmigrant Status - victim of a severe form of trafficking in persons under INA section 101(a)(15)(T)
4. I-918 U Nonimmigrant Status - victim of certain serious criminal activity under INA section 101(a)(15)(U)

- H. **Terrorism:** Any activity that—(A) involves an act that—(i) is dangerous to

human life or potentially destructive of critical infrastructure or key resources; and (ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (B) appears to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

- I. **Terrorism Information**: All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (1) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (2) threats posed by such groups or individuals to the United States, United States Persons, or United States interests, or to those of other nations; (3) communications of or by such groups or individuals; or (4) groups or individuals reasonably believed to be assisting or associated with such groups or individuals. The term includes Weapons of Mass Destruction Information.
- J. **Weapons of Mass Destruction Information**: Information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

V. Responsibilities

- A. The **Officer for Civil Rights and Civil Liberties** directs and oversees the implementation of the integration of civil rights and civil liberties across the Department, serving as the foundational DHS organization through which all Department-wide civil rights and civil liberties activities are overseen, defined, and measured, including the maintenance and disclosure of Section 1367 information. The Officer for Civil Rights and Civil Liberties manages the execution of this Instruction.
- B. The **Under Secretary for Intelligence and Analysis** serves as the Chief Intelligence Officer for the Department, exercising leadership and authority over intelligence policy and programs throughout the Department and, acting in conjunction with, and without preempting the authorities of the DHS Chief Information Officer and the DHS Chief Security Officer,

exercising leadership over information sharing and safeguarding policy and programs throughout the Department in partnership with the Heads of Other Components, including with respect to the disclosure of Section 1367 information.

- C. The **Director of U.S. Citizenship and Immigration Services** oversees lawful immigration to the United States by establishing national immigration services policies and priorities, including with respect to the maintenance and disclosure of Section 1367 information.
- D. The **Chief Privacy Officer** is the senior official within the Department with primary responsibility for privacy compliance and policy, including with respect to disclosure of Section 1367 information.
- E. The Component **Heads** implement and execute all applicable policies and procedures set forth in this instruction and any implementing instructions or other policy guidance to the extent permitted by and consistent with their authorities and any restrictions imposed by statute, executive order, presidential or other directive, or national or departmental policy.

VI. Content and Procedures

A. **Content:**

- 1. Consistent with applicable law, regulation, presidential and other directives, and national and departmental policies, Component Heads (or their designees, provided that any such designee is adequately trained on applicable protections and policies), in coordination with the Director of U.S. Citizenship and Immigration Services or his designees, are permitted to disclose Section 1367 Information under the following circumstances:
 - a. To elements of the United States Intelligence Community outside the Department in furtherance of those elements' authorized National Intelligence (including foreign intelligence and counterintelligence) or counterterrorism functions, provided that disclosure is made in furtherance of the recipient's authorized National Intelligence or counterterrorism function and the information provided is used only for the authorized purpose for which it was provided.
 - b. To other Federal departments or agencies possessing a counterterrorism function, provided that disclosure is made in furtherance of the recipient's authorized counterterrorism

function and the information provided is used only for the authorized purpose for which it was provided.

- c. To foreign governments or any entities thereof possessing a counterterrorism function, provided that disclosure is made in furtherance of the recipient's authorized counterterrorism function and the information provided is used only for the authorized purpose for which it was provided.
 - d. Disclosure by a Component Head or his or her designee to any of the entities described in Section VI.A.1.a-VI.A.1.c of this Instruction is permissible only in accordance with Component-specific procedures for disclosing Section 1367 information jointly developed by the Component, the Office of Intelligence and Analysis, the U.S. Citizenship and Immigration Services, and the Office for Civil Rights and Civil Liberties.
- 2. Except as provided under the terms and conditions of any applicable preexisting information-sharing arrangements between the Department and requestors of Section 1367 information, the Under Secretary for Intelligence and Analysis serves as the Department's point of contact for new requested information sharing arrangements of the type described in Section VI.A.1.a-VI.A.1.c of this Instruction.
 - 3. This Instruction is not intended to contradict or abrogate other protections afforded to applicants for or beneficiaries of T Visa, U Visa, or VAWA protections under law, regulation, presidential or other directive, international agreement, or national or departmental policy, including but not limited to Title 5, U.S.C., Section 552a, "Privacy Act of 1974," Office of Management and Budget (OMB) Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006, and DHS Instruction No. 047-01, "Privacy Policy and Compliance," July 7, 2011.

B. **Procedures:**

- 1. **Information Requests:** Component Heads are authorized to disclose Section 1367 information only in accordance with the procedures and requirements set forth below and in accordance with Component-specific processes and procedures for disclosing Section 1367 information jointly developed by the Component, the Office of Intelligence and Analysis, the U.S. Citizenship and

Immigration Services, and the Office for Civil Rights and Civil Liberties.

- a. As a general matter, requests for Section 1367 information are made in writing (whether in paper or electronic format) and received by the Department prior to disclosure of the information.
 - i. If exigent circumstances prevent a requestor from submitting a written request for Section 1367 information in advance of receipt of that information, the requirement of Section VI.B.1.a of this instruction may be waived in the discretion of the Component Head, but subject to the requirement that the requestor confirm its request in writing as soon as possible, and in any event no later than thirty days after receipt of the information.
 - ii. The exception set forth in Section VI.B.1.a.i of this Instruction does not apply to requests for a large volume of data containing Section 1367 information (i.e., "bulk data"), which, under any circumstances, are required to be made in writing (whether in paper or electronic format) and received by the Department prior to disclosure of the information, and recurring transfers of such information are not provided until the parties sign an information sharing access agreement.
- b. The written request includes the following information:
 - i. Confirmation that the requestor seeks the information in connection with its authorized counterterrorism (or, with respect to elements of the Intelligence Community outside the Department, National Intelligence) function(s);
 - ii. Where possible, supporting information giving rise to the request (e.g., a case number in a terrorism investigation);
 - iii. A description of the requestor's safeguards in place to prevent any unlawful or unauthorized disclosure of the information to third parties; and
 - iv. Confirmation that the written request has been

authorized by the head of the recipient entity or an official delegated or designated with the authority to make such a request on behalf of the head of the recipient entity.

- c. The procedures set forth in Section VI.B.1.a-VI.B.1.b of this Instruction do not apply under the following circumstances:
 - i. In accordance with the terms and conditions of any applicable preexisting information sharing arrangement between the Department and the recipient of Section 1367 information; or
 - ii. To the extent such information has been appropriately disclosed to the public or a State, tribal, territorial, or local government entity in furtherance of a criminal or civil investigation or prosecution and where the Component Head has coordinated such a disclosure with the Director of U.S. Citizenship and Immigration Services and other Component Heads, as appropriate; or
 - iii. Where the Component Head seeks to proactively disclose such information for eligible purposes to eligible recipients and in compliance with the procedures and requirements set forth below and in accordance with Component-specific processes and procedures for disclosing Section 1367 information jointly developed by the Component, the Office of Intelligence and Analysis, the U.S. Citizenship and Immigration Services, and the Office for Civil Rights and Civil Liberties.

2. Identification of Section 1367 Information

- a. Prior to disclosing any information in response to a request for information from a national security official for national security purposes, or proactively seeking to make such a disclosure to eligible entities for those purposes, Component Heads or their designees are responsible for determining whether any information intended to be disclosed is Section 1367 information.
 - i. Consequently, disclosures of information in response to requests for information from national security officials for national security purposes, or proactive

disclosures of information to eligible entities for those purposes, are permissible only to the extent permitted by and consistent with processes and procedures for identifying and disclosing Section 1367 information jointly developed by the Component, the Office of Intelligence and Analysis, the U.S. Citizenship and Immigration Service, and the Office for Civil Rights and Civil Liberties.

- ii. Section VI.B.2.a.i of this Instruction does not apply to any Component until the processes and procedures described in that section are executed or 180 days after the execution of this instruction, whichever occurs first.
 - b. When a national security official outside DHS requests information in bulk from DHS or requests account access to a DHS system of records for national security purposes, such bulk information or account access is provided only to the extent permitted by and consistent with the processes and procedures described in Section VI.B.2.a.i of this Instruction, and only to the extent permitted by and consistent with an applicable information sharing access agreement memorializing the procedures for identifying Section 1367 information and the limitations placed on the use and third-party disclosure of such information.
3. **Retention:** Disclosing officials possess the discretion to disclose Section 1367 information when the intended recipient of such information acknowledges and agrees to abide by the following retention restrictions:
- a. For information determined to constitute terrorism information (or, with respect to elements of the Intelligence Community outside the Department, as information determined to be relevant to the element's authorized National Intelligence function(s)) at the time of disclosure, retention is in accordance with the intended recipient's applicable retention restrictions.
 - b. For information that has not been determined to constitute terrorism information (or, with respect to elements of the Intelligence Community outside the Department, as information determined to be relevant to the element's authorized National Intelligence function(s)) at the time of disclosure, (1) retention is in accordance with the terms and

conditions of any applicable information sharing access agreement, except that, notwithstanding the terms and conditions of any such agreement, the information is retained for one year or less from the date of receipt of the information; or (2) in the absence of an applicable information sharing access agreement, retention may be authorized for a period no later than thirty days from the date of receipt of the information.

- c. For Section 1367 information not identified as terrorism information (or, with respect to elements of the Intelligence Community outside the Department, as information determined to be relevant to the element's authorized National Intelligence function(s)) at the time of disclosure, the intended recipient documents in writing as soon as is practicable, but in no event later than the date of the expiration of the temporary retention period described above, any determination made by the intended recipient that the information constitutes terrorism information (or, with respect to elements of the Intelligence Community outside the Department, is relevant to the element's authorized National Intelligence function(s)), and inform the relevant Component Head of that determination.

- 4. **Third-Party Dissemination:** Component Heads disclose Section 1367 information only when the intended recipient of such information acknowledges and agrees that such information is only further disclosed to a third-party recipient in accordance with the provisions of Title 8, U.S.C., Section 1367, "Penalties for disclosure," and where the conditions described below are satisfied, and only where the standard warning against further disclosure set forth in Appendix A to this instruction is provided in writing, in conjunction with the information being disclosed.

- a. Section 1367 information may be disclosed by the recipient of such information to a third party with the written permission (whether in paper or electronic format) of the Secretary, or the Component Head who originally disclosed the information acting in coordination with the Director of U.S. Citizenship and Immigration Services and other Component Heads, as appropriate, provided that Component Heads only permit recipients of Section 1367 information to share such information under circumstances where the Component Heads could directly share that information with the intended third-party recipient.

- b. Each Component Head that discloses Section 1367 information pursuant to this instruction alerts the recipient that current departmental policy does not permit the further disclosure of Section 1367 information to a person, group, or entity except as permitted by 8 U.S.C. §1367, this Instruction and any other applicable departmental guidance, including, but not limited to, other Federal, or foreign partners without the written consent of the applicant (if the applicant is an adult) or the explicit authorization of the Secretary or the Component Head who originally disclosed the information, acting in coordination with the Director of the U.S. Citizenship and Immigration Services and any other Component Head, as appropriate.
- 5. **Unauthorized Disclosures:** Component Heads disclose Section 1367 information only when the intended recipient of such information acknowledges and agrees that the requirements set forth below are satisfied.
 - a. Recipients of Section 1367 information ensure that any such information in their possession is accessed only by authorized personnel with a need to know the information and is safeguarded and marked, as appropriate, consistent with the Department's policy on controlled unclassified information and any other applicable requirements concerning the handling of such information. These safeguards include procedures to document proper accounting for access to and disclosure of the information.
 - b. Recipients of Section 1367 information who make unauthorized disclosures are not considered for future information sharing until they have conducted an internal audit to determine how the unauthorized disclosure occurred and submit to the Director of U.S. Citizenship and Immigration Services any remedial measures that have been taken to prevent additional unauthorized disclosures in the future. The Director of U.S. Citizenship and Immigration Services then decides if information sharing should resume based upon the results of the requestor's internal audit and the remedial measures undertaken by the recipient.
- 6. **Notification of Unauthorized Disclosures:** In the event that any Component (1) discloses Section 1367 information in a manner inconsistent with the provisions above or (2) is informed by the recipient of Section 1367 information that the recipient has disclosed that information in an unauthorized manner, the Component Head for that Component (1) notifies the Chief Privacy

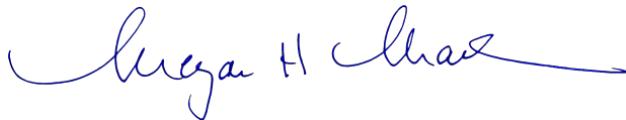
Officer and the Officer for Civil Rights and Civil Liberties as soon as is practicable, but in no event later than twenty-four hours after discovery of the unauthorized disclosure, and (2) satisfies the requirements of the DHS Privacy Incident Handling Guidance.

VII. Questions

Address any questions or concerns regarding this Instruction to the Office for Civil Rights and Civil Liberties.

Appendix A: Standard Warning Against Further Disclosure to Outside Entities

Appendix B: Standard Requirement for Notification of Determination of Terrorism Information or other Intelligence Information



Megan Mack
Officer for Civil Rights and Civil Liberties

11/7/13

Date

Appendix A: Standard Warning Against Further Disclosure to Outside Entities Language

Any other federal departments or agencies or foreign governments to whom information is disclosed receives a warning against further disclosure of the information beyond those entities. The warning text to be included is as follows:

As the new custodian of Section 1367 information, you agree to be bound by the confidentiality protections established by 8 U.S.C § 1367. You may not disclose this information to other parties without the permission of the U.S. Citizenship and Immigration Services and in accordance with 8 U.S.C § 1367 as implemented in DHS Instruction No. 215-01-001, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes.

Appendix B: Standard Requirement for Notification of Determination of Terrorism Information or other National Intelligence

Any other federal departments or agencies or foreign governments to whom DHS discloses Section 1367 information that DHS has not yet determined to constitute terrorism information (or, with respect to elements of the Intelligence Community outside the Department, as information determined to be relevant to the element's authorized National Intelligence function(s)) receives a condition that the recipient informs DHS if the recipient intends to permanently retain the information. The condition text to be included as follows:

- DHS has not yet determined whether this information constitutes terrorism information or information relevant to an Intelligence Community element's authorized National Intelligence function. The recipient of this information is required to document in writing as soon as is practicable, but in no event later than the date of the expiration of the temporary retention period described in DHS's transmission, any determination made by the requestor that the information constitutes terrorism information (or, with respect to elements of the Intelligence Community outside the Department, is relevant to the element's authorized National Intelligence function(s)), and inform the relevant Component Head of that determination, so that DHS may take action, as appropriate.

Issue Date: 6/18/2016

DISCLOSURE OF SECTION 1367 INFORMATION TO LAW ENFORCEMENT OFFICIALS FOR LEGITIMATE LAW ENFORCEMENT PURPOSES

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 002-02 with respect to the disclosure to Law Enforcement Officials for Legitimate Law Enforcement Purposes any information relating to applicants for or beneficiaries of T nonimmigrant status applications (“T visa”), U nonimmigrant status petitions (“U visa”), or applications for immigration relief under the Violence Against Women Act (VAWA) (“Section 1367 Information”). Title 8, United States Code (U.S.C.), Section 1367(a)(2), (b)(2).

II. Scope

This Instruction applies throughout DHS. It does not affect the disclosure of Section 1367 Information in accordance with other exceptions enumerated in Title 8, U.S.C., Section 1367(b).

III. References

- A. Section 102(b)(1) of the Homeland Security Act of 2002; Title 6, U.S.C., Section 112(b)(1)
- B. Sections 101(a)(15)(T), (15)(U), (51), 240A(b)(2) of the Immigration and Nationality Act (INA); Title 8, U.S.C., Sections 1101(a)(15)(T), (15)(U), (51), 1229b(b)(2)
- C. Section 103(a) of the INA; Title 8, U.S.C., Section 1103(a)
- D. Title 8, U.S.C., Section 1367, “Penalties for disclosure of information”
- E. 8 C.F.R. § 2.1

- F. DHS Privacy Incident Handling Guidance (Jan. 26, 2012)
- G. DHS Directive 002-02, "Implementation of Section 1367 Information Provisions"
- H. DHS Instruction 002-02-001, "Implementation of Section 1367 Information Provisions"

IV. Definitions

- A. **Information**: Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape.
- B. **Law Enforcement Official**: An officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, a foreign government or international organization, or an Indian tribe, who is empowered by law to:

- (1) Investigate or conduct an official inquiry into a potential violation of criminal, civil or administrative law or
- (2) Prosecute; or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

The term includes individuals who provide technical, administrative, or other authorized support to law enforcement officers, but does not include emergency, fire, or public officials who are not acting in a law enforcement capacity.

- C. **Legitimate Law Enforcement Purpose**: Preventing, detecting, investigating, or prosecuting, an offense or civil or administrative violation or a potential offense or civil or administrative violation, or assisting a law enforcement agency or Law Enforcement Official in such prevention, detection, investigation, or prosecution, provided that these purposes fall within that law enforcement agency or Law Enforcement Official's lawful enforcement authority. This does not include personal or collateral purposes not related to the official functions of the Law Enforcement Official.
- D. **Section 1367 Information**: Any information relating to aliens who are seeking or have been approved for nonimmigrant or immigrant status as

(1) battered spouses, children, or parents under provisions of the Violence Against Women Act (VAWA); (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T nonimmigrant status); or (3) victims who have suffered substantial physical or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of that activity (U nonimmigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because 8 U.S.C. § 1367 applies to any information about a protected individual, this definition includes records or other information that do not specifically identify the individual as an applicant for or beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA. Section 1367 Information covers information relating to applicants for and beneficiaries of the immigration benefits described below:

(1) Immigration relief under the Violence Against Women Act (VAWA), including VAWA self-petitioners as defined in section 101(a)(51) of the INA. The following is a non-exhaustive list of forms that may be used by VAWA self-petitioners:

- a. Form I-360, *Petition for Amerasian, Widow, or Special Immigrant*, where the petition is filed as the self-petitioning spouse, parent, or child of a U.S. citizen or lawful permanent resident.
- b. Form I-751, *Petition to Remove the Conditions of Residence*, where a waiver of the joint petition requirement is requested because of battery or extreme cruelty by certain family members.

(2) VAWA cancellation of removal under section 240A(b)(2) of the INA.

(3) T nonimmigrant status ("T visa"), as defined in section 101(a)(15)(T) of the INA.

- a. Form I-914, *Application for T Nonimmigrant Status*, and relevant supplements.

(4) U nonimmigrant status ("U visa"), as defined in section INA 101(a)(15)(U) of the INA.

- a. Form I-918, *Petition for U Nonimmigrant Status*, and relevant supplements.

- b. Form I-929, *Petition for Qualifying Family Member of a U-1 Nonimmigrant*.

V. Responsibilities

- A. The **Officer for Civil Rights and Civil Liberties** directs and oversees the implementation of the integration of civil rights and civil liberties across the Department. The Office for Civil Rights and Civil Liberties serves as the foundational DHS organization through which all Department-wide civil rights and civil liberties activities are overseen, defined, and measured, including the maintenance and disclosure of Section 1367 Information. The Officer for Civil Rights and Civil Liberties manages the execution of this Instruction.
- B. The **Under Secretary for Intelligence and Analysis** serves as the Chief Intelligence Officer for the Department, exercising leadership and authority over intelligence policy and programs throughout the Department and, acting in conjunction with, and without preempting the authorities of the DHS Chief Information Officer and the DHS Chief Security Officer, exercising leadership over information sharing and safeguarding policy and programs throughout the Department in partnership with the Heads of other Components, including with respect to the disclosure of Section 1367 Information.
- C. The **General Counsel** is the final legal authority within the Department, who participates in and decides any legal matter within the Department and provides legal advice to all Components of the Department on any legal matter that arises within the Department.
- D. The **Director of U.S. Citizenship and Immigration Services** oversees lawful immigration to the United States by establishing national immigration services policies and priorities, including with respect to the maintenance and disclosure of Section 1367 Information.
- E. The **Chief Privacy Officer** is the senior official within the Department with primary responsibility for privacy compliance and policy, including assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personally identifiable information.
- F. The **Component Heads** implement and execute all applicable policies and procedures set forth in this instruction and any implementing instructions or other policy guidance to the extent permitted by and consistent with their authorities and any restrictions imposed by statute,

executive order, presidential or other directive, or national or departmental policy.

- G. The **Council on Combating Violence Against Women (CCVAW)** works to ensure that policies and practices for combating violence against women and children are consistent Department-wide. By identifying opportunities to build consensus on challenging issues across Components, sharing best practices, and coordinating efforts Department-wide, the Council supports the Department's missions of effectively administering the laws preventing violence against women and children.

VI. Content and Procedures

A. **Content:**

(1) Consistent with applicable law, regulation, presidential and other directives, and national and departmental policies, Component Heads (or their designees, provided that any such designee is adequately trained on applicable protections and policies), in coordination with the Director of U.S. Citizenship and Immigration Services (USCIS) or his designees, are permitted to disclose Section 1367 Information to Law Enforcement Officials, provided that disclosure is made in furtherance of the Department's or the recipient's Legitimate Law Enforcement Purpose in a manner that protects the confidentiality of such information and the recipient agrees not to further disseminate the information or use it for a purpose other than the purpose for which it was provided absent express authorization.

- a. This provision is not intended to limit the further use or sharing of Section 1367 Information by the Department, where such use or further sharing is required by law or otherwise consistent with national and departmental policies.
- b. If exigent circumstances (e.g., a credible and imminent threat to the homeland) require the immediate disclosure of Section 1367 Information to Law Enforcement Officials for a Legitimate Law Enforcement Purpose, disclosure is permissible without advance coordination with the Director of USCIS so long as USCIS is notified of the disclosure and the circumstances surrounding the disclosure within 24 hours of the disclosure. Any such disclosure must otherwise be consistent with this

Instruction, including the use of standard warning caveats.

- c. In accordance with Section 1367(a)(2), Components may disclose Section 1367 Information within DHS and to any sworn officer or employee of the Department of Justice or the Department of State, or any agency or bureau thereof, for any legitimate Department, agency or bureau purpose, including a Legitimate Law Enforcement Purpose. This guidance is not intended to govern such lawful disclosures.

(2) Except for sharing described in Section VI.A.1.c, disclosure by a Component Head or their designee(s) to any of the entities described in Section VI.A.1. of this Instruction is permissible only in accordance with Component-specific procedures for disclosing Section 1367 Information jointly developed by the Component, U.S. Citizenship and Immigration Services, and the Office for Civil Rights and Civil Liberties, including any exemptions and alternate procedures developed for particular component activities.

(3) This Instruction is not intended to contradict or abrogate other protections covering information relating to applicants for or beneficiaries of T nonimmigrant status, U nonimmigrant status, or immigration relief under VAWA under law, regulation, presidential or other directive, international agreement, or national or departmental policy, including but not limited to Title 5, U.S.C., Section 552a, "Privacy Act of 1974," Office of Management and Budget (OMB) Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006, and DHS Instruction No. 047-01, "Privacy Policy and Compliance," July 7, 2011.

- B. **Procedures:** When disclosing Section 1367 Information under the law enforcement exemption, Component Heads or their designees comply with the following procedures:

(1) Identification of Section 1367 Information

- a. Prior to disclosing any information outside the Department under the law enforcement exception, Component Heads or their designees are responsible for determining whether any information intended to be disclosed is Section 1367

Information.

- i. Disclosures of information to Law Enforcement Officials for Legitimate Law Enforcement Purposes are permissible only to the extent permitted by and consistent with processes and procedures for identifying and disclosing Section 1367 Information jointly developed by the Component, U.S. Citizenship and Immigration Services, and the Office for Civil Rights and Civil Liberties.
- ii. Section VI.B.1.a.i of this Instruction does not apply to any Component until the processes and procedures described in that section are executed or 180 days after the execution of this Instruction, whichever occurs first.

(2) Disclosure of Section 1367 Information:

- a. Component Heads and their designees have the discretion to disclose Section 1367 Information under the law enforcement exception only when the intended recipient of such information acknowledges and agrees not to further disseminate the information or use it for a purpose other than the purpose for which it was provided absent express authorizations, and to delete it once it is no longer needed for that purpose.
- b. Component Heads and their designees have the discretion to disclose Section 1367 Information only when the intended recipient of the information agrees to delete any Section 1367 Information that is subsequently determined by the recipient to be unrelated to the initial purpose for sharing as soon as possible, but no later than 24 hours after such a determination has been made.
- c. Prior to disclosing Section 1367 Information outside of DHS, Component Heads or their designees must affix (or verbalize during briefings) the appropriate caveat against onward disclosure set forth in Appendix A in a manner that clearly identifies the specific information that must be protected.

- d. Bulk sharing of information is accomplished pursuant to an Information Sharing and Access Agreement (ISAA) coordinated with the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties. The terms of any ISAA establish the conditions and procedures for identifying, sharing, and retaining Section 1367 Information that may be shared pursuant to the ISAA.
- e. The procedures referenced in Section VI.B.1.a.i of this Instruction are not intended to supersede any provision addressing the sharing of Section 1367 Information in existing ISAA's, provided that any such provision comports with 8 U.S.C. § 1367.

(3) Third-Party Dissemination: Component Heads and their designees disclose Section 1367 Information only when the intended recipient of such information acknowledges and agrees that such information is only further disclosed to a third-party recipient in accordance with 8 U.S.C. § 1367 and where the conditions described below are satisfied.

- a. Section 1367 Information may be disclosed by the recipient of such information to a third party with the written permission (whether in paper or electronic format) of the Secretary, or the Component Head or designee who originally disclosed the information acting in coordination with the Director of USCIS and other Component Heads or their designees, as appropriate, provided that Component Heads or their designees only permit recipients of Section 1367 Information to share such information under circumstances where the Component Heads or their designees could directly share that information with the intended third-party recipient.
- c. Each Component Head or designee that discloses Section 1367 Information pursuant to this Instruction alerts the recipient that current departmental policy does not permit the further disclosure of Section 1367 Information to a person, group, or entity except as permitted by 8 U.S.C. § 1367, this Instruction, and any other applicable departmental guidance, without the

explicit authorization of the Secretary or the Component Head or his or her designee who originally disclosed the information, acting in coordination with the Director of USCIS and any other Component Head, as appropriate. The Component Head or designee alerts the recipient they must include the standard warning against further disclosure set forth in Appendix A in conjunction with the recipient's approved disclosure to the third party.

(4) Protecting against Unauthorized Disclosures: Component Heads or their designees disclose Section 1367 Information only when the intended recipient of such information acknowledges and agrees that the requirements set forth below are satisfied.

- a. Recipients of Section 1367 Information ensure that any such information in their possession is: (i) accessed only by authorized personnel that need to know the information; (ii) safeguarded and marked, as appropriate, consistent with the Department's policy on sensitive but unclassified information; and (iii) safeguarded according to any other applicable requirements concerning the handling of such information. These safeguards include procedures to document proper accounting for access to and disclosure of the information.
- b. Recipients of Section 1367 Information who make unauthorized disclosures are not considered for future information sharing until they have conducted an internal audit to determine how the unauthorized disclosure occurred and submitted to the Director of USCIS any remedial measures that have been taken to prevent additional unauthorized disclosures in the future. The Director of USCIS then decides if information sharing should resume based upon the results of the requestor's internal audit and the remedial measures undertaken by the recipient.

(5) Notification of Unauthorized Disclosures: In the event that any Component (1) discloses Section 1367 Information in a manner inconsistent with the provisions above, or (2) is informed by the recipient of Section 1367 Information that the recipient has disclosed that information in an unauthorized manner, the Component (1) notifies the Chief Privacy Officer and the Officer for

Civil Rights and Civil Liberties as soon as is practicable, but in no event later than 24 hours after discovery of the unauthorized disclosure, and (2) satisfies the requirements of the DHS Privacy Incident Handling Guidance.

VII. Questions

Address any questions or concerns regarding this Instruction to the Office for Civil Rights and Civil Liberties.

Appendix A: Standard Warning Against Further Disclosure to Outside Entities



Megan H. Mack
Officer for Civil Rights and Civil Liberties

6/8/16

Date

Appendix A: Standard Warning Against Further Disclosure to Outside Entities

Any Law Enforcement Official who receives Section 1367 Information for a Legitimate Law Enforcement Purpose receives the following warning against further disclosure of the information:

This information [has been determined to be/ may be] protected under 8 U.S.C. § 1367. You may not disclose this information to third parties or use it for purposes other than the purpose for which it was provided without the permission of U.S. Citizenship and Immigration Services and the originating agency, as applicable, and in accordance with 8 U.S.C. § 1367 and DHS policy. You may request permission by contacting the DHS Single-Point-of-Service Desk (dhs-sps-rfi@hq.dhs.gov, dhs-sps-rfi@dhs.sgov.gov, or dhs-sps-rfi@dhs.ic.gov) before onward sharing of the information. Section 1367 Information that is subsequently determined by the recipient to be unrelated to the initial individual of interest, investigation, or threat, must be deleted as soon as possible, but no later than 24 hours after such a determination has been made.