Privacy Impact Assessment
for the

Preventing and Combating Serious Crime Agreements - Greece and Italy

DHS/ALL/PIA-064

April 3, 2018

Contact Point
Michael Scardaville
Office of Policy
Department of Homeland Security
202-282-8321

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

Abstract

In 2009, the United States entered into two separate Enhancing Cooperation in Preventing and Combating Serious Crime Agreements (PCSC Agreements) with the Hellenic Republic (Greece) and the Italian Republic (Italy). PCSC Agreements permit the United States and its partner countries to cooperatively exchange biometric and biographic data in the course of preventing and combating serious crimes and terrorist activities. The U.S. Department of Homeland Security (DHS) owns and maintains the Automated Biometric Identification System (IDENT), which is responsible for processing automated fingerprint queries to determine if a person of interest encountered by a partner country has also been encountered by DHS. While existing PCSC agreements between DHS and its partners allow for the exchange of criminal justice data, the agreements with Greece and Italy also enable DHS to share non-criminal justice data from U.S. Citizenship and Immigration Services (USCIS). The DHS Privacy Office is publishing this Privacy Impact Assessment (PIA) to identify risks and mitigations associated with this information sharing, and to discuss the legal and policy justifications for sharing non-criminal justice data from the USCIS with Greece and Italy under the Greece and Italy PCSC Agreements, for purposes of immigration vetting and criminal justice, including border enforcement processes.

Introduction

This PIA discusses the: 1) PCSC Agreements from a DHS perspective; 2) Greece and Italy PCSC Agreements and Implementing Arrangements (collectively referred to herein as PCSC Agreements), which present unique challenges in light of the European migration crises; and 3) policy determination that the exceptional circumstances in Greece and Italy warranted sharing USCIS's non-criminal justice data with foreign criminal justice agencies under the PCSC Agreements.

IDENT is DHS's biometric system for storing and processing biometric and limited biographic data for national, law enforcement, immigration, intelligence, and other DHS mission-related functions. IDENT is managed by DHS's National Protection and Programs Directorate (NPPD), Office of Biometric Identity Management (OBIM). Existing country-specific PCSC Agreements are summarized in appendices to the IDENT PIA.[1] However, since OBIM is sharing USCIS non-criminal justice data sets for immigration vetting and criminal justice purposes, through IDENT automated filtering under the Greece and Italy PCSC Agreements, the DHS Privacy Office is publishing this standalone PIA to explain the exceptional circumstances that led the Department's policy decision to share this information, and the associated privacy risks and mitigations.

---

[1] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) and IDENT Appendices, *available at* www.dhs.gov/privacy.

Preventing and Combating Serious Crime Agreements (PCSC Agreements)

PCSC Agreements fulfill one of the eligibility requirements for the Visa Waiver Program (VWP),[2] as identified in Section 217 of the Immigration and Nationality Act (INA) (including as amended most recently by the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015), which requires a VWP country to execute an agreement with the United States to share information on persons traveling to the United States who may represent a threat to the security or welfare of the United States or its citizens.[3]

The United States began entering into PCSC Agreements in 2008, primarily with countries that participate or seek to participate in the VWP.[4] PCSC Agreements are intended to automate and expedite the sharing of information about persons for whom a government has an official need to inquire for purposes of preventing or combating serious crime, while requiring measures to ensure individual privacy is protected. As recognized by the Government Accountability Office, "PCSC Agreements contain numerous provisions pertaining to the handling, sharing, and retention of relevant data, all designed to ensure privacy and data protection."[5]

The information sharing process under PCSC Agreements begins when one country (herein "querying country") encounters a specific person of interest and determines there is an official need to inquire for purposes of preventing or combating serious crime. The querying country collects the fingerprints of the person of interest and queries the automated biometric system of the other country (herein "receiving country") to determine if the receiving country has previously encountered this individual. Encounter information available to PCSC partners include DHS, Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) enforcement actions, CBP border crossing data, certain USCIS application information, and other OBIM IDENT enrollments. Queries are made on an individual case-by-case basis and in compliance with the querying party's national laws. The receiving country indicates whether a fingerprint match exists in its automated biometric system by automatically responding "match" or "no match" to the querying country.

In the event of a fingerprint match, Personally Identifiable Information (PII) may be shared, including, but not limited to: first and last names, former names, other names, aliases, alternative

---

[2] VWP, administered by DHS in consultation with the Department of State, permits citizens of participating countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those countries must permit U.S. citizens and nationals to travel to their countries for a similar length of time without a visa for business or tourism purposes, *available at* https://www.dhs.gov/visa-waiver-program. Currently, there are 38 participating countries.
[3] 8 U.S.C. 1187 (c)(2)(F).
[4] See DHS/NPPD/PIA-002 *Automated Biometric Identification System* (IDENT), *available at* www.dhs.gov/privacy.
[5] *Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security*, Government Accountability Office (GAO), note 38, GAO-16-498 (May 2016), *available at* https://www.gao.gov/assets/680/676948.pdf.

spelling of names, gender, date and place of birth, photographs current and former nationalities, passport data, numbers from other identity documents, immigration history, descriptions of past enforcement actions, and encounter information (e.g., transaction-identifier data including the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information). *See Appendix A* for a full list of data elements shared under the Greece and Italy agreements.[6]

In the event of a match, the querying country may also share its PII and other encounter data about the person of interest with the receiving country. The receiving country may only provide further biographic information when permitted by its national law and defined as serious criminal activity. Serious criminal activity includes those crimes that may have the effect of rendering an individual inadmissible or removable from the United States. Serious criminal activity excludes minor criminal offenses, and is defined in the Greece and Italy PCSC Agreements as those crimes punishable by a sentence of more than one (1) year of incarceration.

Although each query goes through IDENT as a single query, the system may receive multiple queries at one time. PII is retained only as long as necessary for the specific purpose for which the data were provided, as determined by each country's national law. If there is no fingerprint match, then the queried fingerprints are not retained by the receiving country.

PCSC Agreements also generally permit each country to provide PII to the other country, without a prior query or request, if there is suspicion that a person:

- will commit (or may be planning to commit), or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association; or
- is undergoing or has undergone training to commit terrorist or terrorism related offenses, or offenses related to a terrorist group or association; or
- will commit (or may be planning to), or has committed a serious criminal offense or participates in an organized criminal group or association.

---

[6] Greece PCSC Agreement and Implementing Arrangement: *Agreement Between the Government of the United States of America and the Government of the Hellenic Republic on Enhancing Cooperation in Preventing and Combating Serious Crime (Greece Agreement) (June 28, 2009);* and the *Implementing Arrangement under the Hellenic Republic on Enhancing Cooperation in Preventing and Combating Serious Crime* (Greece Implementing Arrangement) (November 7, 2016) (collectively both are referred to as the Greece Agreement).
Italy PCSC Agreement and Implementing Arrangement: *Agreement Between the Government of the United States of America and the Government of the Italian Republic on Enhancing Cooperation in Preventing and Combating Serious Crime (Italy Agreement) (May 28, 2009);* and the *Implementing Arrangement under the Agreement Between the Government of the United States of America and the Government of the Italian Republic (October 20, 2017) (Italy Implementing Arrangement) (*collectively both are referred to as the Italy Agreement*).*

The country providing this data may impose conditions on its use. In such situations, the receiving country, with the consent of the partner country, may enroll and retain the information even if there is no match, consistent with its own national law and other applicable restrictions.[7]

PCSC Automated Query and Response Capability

Greece uses the Secure Real-Time Platform (SRTP) to share biometrics and biographic data. Italy will use the SRTP when it becomes operational in 2018. SRTP is an automated biometric and biographic data sharing capability for IDENT that uses a combination of the public Internet and high security encryption protocols to provide biometric query and response capabilities. SRTP will eventually be used to transmit data for all PCSC Agreements.

SRTP uses the U.S. Custom and Border Protection's (CBP) Unified Passenger System (UPAX), a module of CBP's Automated Targeting System (ATS), which acts as a proxy between IDENT and a foreign partner's automated biometric system. A Virtual Private Network (VPN) connection over the public Internet is established between each foreign partner and UPAX.[8] All message requests and responses from Greece and Italy's automated biometric systems to IDENT are to first pass through UPAX. DHS plans to establish a future capability to send all requests and responses *from* IDENT to Greece and Italy's automated biometric systems through UPAX (referred to as the "reciprocal process"). Although DHS is currently not able to query Greece's or Italy's automated biometric systems, both countries are working closely with DHS to develop the technical connections that would allow DHS to move toward a reciprocal process.

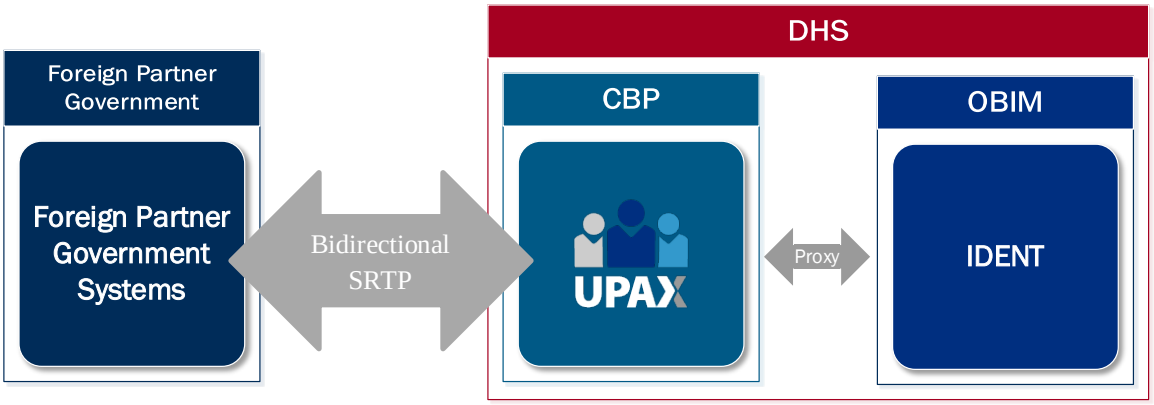
Generally, the querying country sends DHS a fingerprint of a person of interest to search IDENT for a match. If there is *no match*, IDENT returns a "no match" response. If there is a fingerprint match that is permissible to share, then IDENT returns an automated match response, with approved shareable biographic data (*See Appendix A*). If the queried party's domestic law prohibits the disclosure of information that would normally constitute a "match," the queried party will return a "no match" response. For example, IDENT would return a "no match" response when there is a biometric match to an individual in a special protected class, such as Violence Against Women Act (VAWA), T visa nonimmigrant status (victims of human trafficking), and those applying for U visa nonimmigrant status (victims of qualifying crimes), because such individuals are protected by law.[9]

Similarly, the queried country, after sharing its information, may seek reciprocity. The querying country may send its data on the person of interest. The foreign partner will, if technically feasible, respond automatically with approved biographic data elements for that person of interest.

---

[7] *Greece Agreement*, Article 11; *Italy Agreement*, Article 10.
[8] *See* DHS/CBP/PIA-006 Automated Targeting Systems and subsequent updates, *available at* www.dhs.gov/privacy.
[9] 8 U.S.C. § 1367.

Since UPAX is only a proxy to the IDENT system, CBP does not retain a copy of data passing through UPAX or for additional queries. UPAX records transaction details used for auditing purposes only. The DHS Privacy Office recommends that CBP include verification that is does not retain a copy of data passing through UPAX in its forthcoming ATS privacy evaluation. The diagram below depicts the future state of SRTP with bi-directional (two-way) flow of information.



The following is the planned SRTP incremental rollout schedule for Greece and Italy, which is based on each foreign partner's technical capabilities:

Phase I: Greece or Italy submit biometric requests to IDENT through UPAX. IDENT will respond through UPAX with biographic information on biometric matches that are allowed to be shared with the foreign partner. UPAX relays the biographic information to the foreign partner over a VPN. Phase I began for Greece on January 13, 2017, and Italy is expected to begin in 2018.

Phase II: UPAX / IDENT automatically requests additional information from Greece or Italy after it has matched to a biometric query. This is also known as the reciprocal process. For every biometric match in Phase I, IDENT will automatically query, through UPAX, for the biographic PII held by the foreign partner. The foreign partner will respond with the additional biographic PII to UPAX. UPAX will send the biographic data to IDENT.

Phase III: DHS uses UPAX / IDENT to submit biometric queries to Greece or Italy. This is the reverse process of Phase 1 and Phase 2, which allows IDENT - through UPAX - to submit biometric queries to foreign partners. Similarly, when there is a fingerprint match, foreign partners will be able to submit biographic queries to IDENT through UPAX.

Sharing under the Greece and Italy PCSCs

In 2009, the United States entered into two separately negotiated PCSC Agreements with Greece and Italy. This occurred prior to the humanitarian and mass migration crises stemming

primarily from the conflicts in Syria and Iraq.[10] DHS and Greece's automated sharing became operational in December 2016, after the crisis began. DHS expects to begin sharing with Italy in 2018.

As described below, in light of U.N. Security Council Resolutions and the European Commission's declared migration crises in both countries, Greece may query any immigrant against IDENT, in addition to suspected criminals, which is typically the scope of PCSC Agreements. Italy will similarly use the Agreement, once it becomes operational in 2018. USCIS is making its data available under the Greece and Italy PCSC Agreements due to the exceptional circumstances posed by these twin crises, and represents an exception -not the rule- for DHS's information sharing under PCSC Agreements. This information sharing is consistent with United Nations Security Council Resolutions 1373 (2001),[11] 2178 (2014)[12], and 2396 (2017),[13] which call upon Member States to prevent the movement of terrorists or terrorist groups by effective border controls.

In both the Greece and Italy agreements, "serious crimes" are those punishable by more than one (1) year of incarceration. Offenses that meet that definition vary among the partners. The Greece agreement permits each country to provide a list of serious crimes for which each country *will not* be obligated to supply PII if there is a fingerprint match.[14] By contrast, in the Italian agreement, Italy and the United States agreed on a comprehensive list of offenses that will serve as the basis for cooperation under their respective national laws.[15]

Determination to Share USCIS Non-Criminal Justice Data for Criminal Justice Purposes

USCIS is a civil agency focused on administering the nation's lawful immigration system, and in doing so, collects personal information to ensure that an applicant is qualified to receive a benefit – and not explicitly for a criminal justice purpose. However, as a matter of policy, DHS determined that the exceptional circumstances surrounding the Greek and Italian migrant crises warranted the temporary sharing of USCIS non-criminal justice data with criminal justice agencies for border enforcement and immigration vetting purposes.This practice is consistent with international best practices issued by the United Nations High Commissioner for Refugees that reaffirms terrorists and other serious criminals should not receive international protection as a

[10] The information sharing practices and approaches described herein are only DHS's information sharing practices and approaches, and does not necessarily reflect those of other U.S. Federal Executive Branch agencies that separately share information with Greece and Italy under PCSC Agreements.
[11] United Nations Security Council Resolution 1373 (2001), *available at* https://undocs.org/S/RES/1373(2001).
[12] United Nations Security Council Resolution 2178 (2014), *available at* https://undocs.org/S/RES/2178(2014).
[13] United Nations Security Council Resolution 2396 (2017), *available at* https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf.
[14] *Greece Agreement*, Article 2.
[15] *Italy Agreement*, Article 5(2); *Italy Implementing Arrangement, Technical Annex.*

refugee and that all states should institute measures to prevent criminals and terrorists from obtaining such benefits.

USCIS may share records covered by two USCIS System of Records Notices (SORN), pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, with Greece and Italy for purposes of immigration-border enforcement: Background Check Service[16] and Biometric Storage System.[17] That is, the purpose for the collection of these records by USCIS is compatible with such purposes of sharing USCIS records to Greece and Italy, and permitted to be disclosed by the following routine uses:[18]

DHS/USCIS-002 *Background Check Service*, Routine Use G:

To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where USCIS believes the information would assist enforcement of civil or criminal laws.[19]

DHS/USCIS-003 *Biometric Storage System*, Routine Use F:

To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.[20]

Other applicable DHS SORNs include the ICE Criminal Arrest Records and Immigration Enforcement Records (CARIER),[21] CBP Automated Targeting System.[22], and the forthcoming External Biometric Records.[23]

---

[16] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[17] DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 6, 2007).
[18] The USCIS Office of Privacy is in the process of consolidating DHS/USCIS-002 Background Check Service and DHS/USCIS-003 Biometric Storage System SORNs into a new SORN, titled the *Immigration Biometric and Background Check SORN*, to holistically cover biometric and biographic screening and background checks for USCIS customers and international partners. Once this consolidated SORN is published in the Federal Register, it will also be *available at* www.dhs.gov/privacy.
[19] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[20] DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 6, 2007).
[21] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016).
[22] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[23] The DHS Privacy Office is in the process of developing a new SORN, titled the External Biometric Records SORN, to allow DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic, for the following purposes pursuant to formal or informal information sharing agreements or arrangements ("external information"), or with the express approval of the entity from which the Department received biometric and associated biographic information: law enforcement; national security;

The Greece and Italy PCSC Agreements can be interpreted as supporting screening and vetting of migrants and asylum seekers, particularly at the international border and in other circumstances as part of an admissibility decision, when screening and vetting serve law enforcement purposes and the protection of public security. In the event of a match to USCIS data, Greece and Italy will use USCIS data during its screening and vetting processes to verify the identity of individuals as part of individual cases in an effort to detect serious crime and to identify and apprehend criminals. This is consistent with international law, which recognizes the right of every sovereign state to control its borders in order to prevent the entry of unwanted persons and goods posing a threat to its security – that is, to detect crime at the international border and therein.

Also, the use of USCIS data by Greece and Italy subjects individuals to a thorough check under the European Union's Schengen Border Code, which constitutes a "further inspection," as stated in the Greece and Italy PCSC Agreements,[24] for the purposes of preventing and combating crime through the detection of criminals and terrorists at the Schengen border.[25] It is clear that comparing information collected as part of an asylum application or border crossing against terrorism and criminal information constitutes an effort to detect criminal offenders and/or criminal identification activities in order to prevent crime. For this reason, DHS may disclose specified USCIS data to Greece and Italy under these particular PCSC Agreements.

However, there are U.S. legal prohibitions that would prevent DHS from providing certain USCIS information to Greece and Italy. Some individuals applying for or receiving USCIS benefits are afforded additional confidentiality protections by statute, regulation, or policy. When individuals belong to "special protected classes," they are protected by, among other provisions, 8 U.S.C. § 1367, which pertains to those protected under the Violence Against Women Act (VAWA),[26] those applying for T visa nonimmigrant status (victims of human trafficking), and those applying for U visa nonimmigrant status (victims of qualifying crimes);[27] other special

---

immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. Once this SORN is published in the Federal Register, it will also be available at www.dhs.gov/privacy.

[24] *Greece Agreement*, Article 5(2); *Italy Agreement*, Article 2(2).

[25] See Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules government the movement of persons across borders (Schengen Borders Code) (codification) art. 8.3, amended by Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders. The Schengen Borders Code requires that "all persons must undergo a minimum check," and that such checks "shall be the rule for persons enjoying the right of free movement under Union law." *Schengen Border Code*, art. 8.2(a). It also provides that, on entry or exit, all non-EU nationals "shall be subject to thorough checks." *Id.* art. 8.3. These "thorough checks" comprise the same kinds of checks performed on persons enjoying the right of free movement under Union law, plus a few other checks, such as checks against the Visa Information System (VIS). *Id.* art. 8.3(b). All "checks" are intended to verify that the non-EU nationals are "not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States." *Id.* art. 8.2(b), 8.3(a)(i), 8.3(g)(iii).

[26] 42 U.S.C. § 13701 through 14040.

[27] 8 U.S.C. § 1367.

protected classes include asylees, those who receive credible fear/reasonable fear screenings, and refugees (see 8 C.F.R. § 208.6 and DHS policy[28]); those with Temporary Protected Status (see 8 U.S.C. § 244 and 8 C.F.R. § 244.16); Special Agricultural Workers; and those with benefits under Legalization and the Legal Immigration Family Equity Act (LIFE Act) (see INA § 245A(c)(4), (5); INA § 210(b)(5), (6); 8 C.F.R. § 210.2(3)(e)). Thus, if the queried party's domestic law prohibits the disclosure of information that would normally constitute a "match," the queried party will return a "no match" response.

All information pertaining to any individual protected by 8 U.S.C. § 1367 is generally protected from disclosure to third parties, except in very limited circumstances. This statutory prohibition applies to *all* IDENT encounters pertaining to a protected individual, not only the encounters specific to a protected benefit type. These individuals will be excluded from responses to Greece and Italy. Asylum, credible fear/reasonable fear, and refugee-related information is also prohibited from disclosure to foreign countries, unless there is a waiver for such sharing issued by the Secretary of the Department of Homeland Security.[29] There is currently no such Secretarial waiver for sharing asylum or refugee-related information with either Greece or Italy.

In order to ensure legal and policy compliance with the sharing of selected USCIS data sets under these exceptional circumstances, DHS's OBIM will generate metrics to gauge the continued value in sharing USCIS data with Greece and Italy. Contingent on the technical capabilities of Greece and Italy, OBIM will provide the DHS Privacy Office with a metrics report within six (6) months of OBIM being technically capable of obtaining these metrics from Greece and Italy. To the extent possible, this metrics report may include, but is not limited to, the following data points:

- Number of fingerprint matches in which a responding data element (e.g., passport number) shared with Greece or Italy is found in a USCIS data set;
- The number of times additional information (i.e., biographic) was provided to Greece and Italy after queried fingerprints matched against USCIS fingerprints (expressed both as a number and percentage of all USCIS data shared with Greece and Italy);
- The number of times a querying country, after a match is made, provides additional information on the data subject that results in OBIM establishing a new encounter in IDENT (expressed both as a number and percentage of all USCIS data shared with Greece and Italy); and

[28] DHS Instruction 262-02-001, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, November 21, 2016.
[29] The Secretary of the Department of Homeland Security, under 8 C.F.R. §208.6, has the discretion to authorize asylum and refugee-related information to foreign countries. Currently, this information is only authorized to be shared with Canada, Australia, New Zealand, and the United Kingdom, all of which are trusted partner nations for purposes of immigration and border security, commonly referred to as the "Five Country Conference" or "M-5."

- The number of times there are matches against USCIS fingerprints that are already known to be associated with derogatory information (expressed both as a number and percentage of all USCIS data shared with Greece and Italy).

Migration Crises

In 2015 Europe was first confronted with a large number of refugees primarily escaping conflicts in Syria, Iraq, and Afghanistan. A total of 1.2 million refugees arrived in Europe between 2015 and early 2016,[30] overwhelming many European countries, particularly Greece and Italy, which sit on the Mediterranean Sea. This migration crisis is the largest Europe has faced since World War II.[31]

In an effort to manage the migration crisis, the European Commission issued the *European Agenda on Migration* (Agenda) in May 2015,[32] which set out a comprehensive approach toward saving lives at sea, targeting criminal smuggling networks, and helping frontline European Union Member States (i.e., Greece and Italy). The European Commission demonstrated the urgency of this crisis when it proposed, for the first time, to activate the migrant emergency response system in Article 78(3) of the Treaty on the Functioning of the European Union (TFEU), which states:

> "In the event of one or more Member States being confronted with an *emergency situation* characterised by a sudden inflow of nationals of third countries, the Council, on a proposal from the Commission, may adopt provisional measures for the benefit of the Member State(s) concerned. It shall act after consulting the European Parliament (emphasis added)."[33]

The European Commission's recommendation was adopted by The Council of the European Union, Council Decision (September 22, 2015). The criteria for triggering Article 78(3) requires:

> "[E]xceptional circumstances when, based on clear and measurable indications, the functioning of the asylum system of a Member State(s) can be endangered by a consistently high [number] of refugees arriving on its territory, and in particular of those

---

[30] *See* The Office of the United Nations High Commissioner for Refugees (UNHCR), *available at* http://www.unhcr.org/en-us/europe-emergency.html.
[31] *Europe Faces Worst Refugees Crises Since Second World War, available at* http://www.telegraph.co.uk/news/worldnews/europe/11804195/Europe-faces-worst-refugee-crisis-since-Second-World-War.html.
[32] *See Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, A European Agenda on Migration*, COM(2015) 240 final, Brussels 13.5.2015 (Agenda), *available at* https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/background-information/docs/communication_on_the_european_agenda_on_migration_en.pdf.
[33] *Agenda* at 4.

> in clear need of international protection. A high threshold of urgency and severity of the problem are therefore preconditions for the triggering of the mechanism."[34]

One of the key components of the Agenda was the creation of "hotspots."[35] Hotspots are European Commission-designated areas that require operational support in handling the surge in migrations. Certain exterior borders of Greece and Italy receiving a high volume of migrants were identified as hotspots. Specifically, the European Commission directed that:

> "[T]he European Asylum Support Office, Frontex and Europol will work on the ground with frontline Member States [Greece and Italy] to swiftly identify, register and fingerprint incoming migrants. The work of the agencies will be complementary to one another. Those claiming asylum will be immediately channelled into an asylum procedure where [the European Asylum Support Office (EASO)] support teams will help to process asylum cases as quickly as possible. For those not in need of protection, Frontex will help Member States by coordinating the return of irregular migrants. Europol [law enforcement support] and Eurojust will assist the host Member State with investigations to dismantle the smuggling and trafficking networks."[36]

An unofficial *Explanatory Note* sent by a commissioner on the European Commission describes the hotspot approach as follows:

> "The aim of the Hotspot approach is to provide a platform for the agencies to intervene, rapidly and in an integrated manner, in frontline Member States when there is a crisis due to specific and disproportionate migratory pressure at their external borders, consisting of mixed migratory flows and the Member State concerned might request support and assistance to better cope with that pressure. The support offered and the duration of assistance to the Member State concerned would depend on its needs and the development of the situation. This is intended to be a flexible tool that can be applied in a tailored manner."[37]

Greece in particular has faced challenges in identifying, registering, and fingerprinting migrants. According to a 2016 European Commission report, "Greece is seriously neglecting its

---

[34] *See* European Commission Fact Sheet, Brussels (September 22, 2015), *available at* http://europa.eu/rapid/press-release_MEMO-15-5698_en.htm.
[35] *Agenda* at 6.
[36] Id; *See* Eurojust assists Member States in dealing with serious cross-border and organized crime, *available at* http://www.eurojust.europa.eu/about/background/Pages/eurojust-core-business.aspx.
[37] *See Explanatory Note* sent by Commissioner Avromopoulos to Justice and Home Affairs Ministers on July 15, 2015, Statewatch at 3, *available at* http://www.statewatch.org/news/2015/jul/eu-com-hotsposts.pdf; See *European Parliament, Directorate-General for Internal Policies, Policy Department, Citizens' Rights and Constitutional Affairs* (2016).
http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556942/IPOL_STU%282016%29556942_EN.pdf.

obligations and there are serious deficiencies in the carrying out of external border controls that must be overcome and dealt with by the Greek authorities."[38]

According to the U.S. State Department's *Greece 2016 Human Rights Report*, more than 60,000 migrants and refugees were stranded in Greece at the end of 2016. The most significant human rights problems were the overcrowding and poor humanitarian conditions facing migrants and asylum seekers at migrant reception and registration sites.[39] Compounding the problem, in early 2016, Croatia, Serbia, and the Former Yugoslav Republic of Macedonia closed their borders, leaving a large number of migrants in Greece.[40]

Most migrants traveling to Italy are coming from North Africa, primarily Libya.[41] According to the International Organization for Migration, between January 1, 2017 through October 8, 2017, 107,028 migrants arrived in Italy representing 75% of all arrivals in Europe, while 2,570 died *en route* to Italy.[42]

Analysis of Facts Considered in Determining the Existence of Exceptional Circumstances

The following facts were considered in determining that sharing USCIS non-criminal justice data for criminal justice purposes was warranted.

1. United Nations Security Council Resolutions 1373 (2001),[43] 2178 (2014),[44] and 2396 (2017)[45] that call upon Member States to "prevent the movement of terrorists by effective border controls."
2. The European Commission's declaration that the Greece and Italy migration situations are emergencies requiring immediate action;
3. The sharing of certain non-criminal justice USCIS data sets is limited to those permissible under U.S. law and the routine uses in place for the USCIS data;

---

[38] *See* European Commission - Press release: Commission discusses draft Schengen Evaluation Report on Greece (January 27, 2016), *available at* http://europa.eu/rapid/press-release_IP-16-174_en.htm.
[39] *See Greece 2016 Human Rights Report*, U.S. Department of State, *available at* https://www.state.gov/documents/organization/265638.pdf.
[40] *See Report to the Greek Government on the Visits to Greece Carried Out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 13-18 April and 19 to 25 July 2016*, *available at* https://rm.coe.int/pdf/168074f85d.
[41] *See Central Mediterranean Route: Commission Proposes Action Plan to Support Italy, Reduce Pressure and Increase Solidarity* (July 4, 2017), *available at* http://europa.eu/rapid/press-release_IP-17-1882_en.htm.
[42] *See Mediterranean Migrant Arrivals Reach 140,538 in 2017; Deaths Reach 2,754*, International Organization for Migration, *available at* https://www.iom.int/news/mediterranean-migrant-arrivals-reach-140538-2017-deaths-reach-2754.
[43] United Nations Security Council Resolution 1373 (2001), *available at* https://undocs.org/S/RES/1373(2001).
[44] United Nations Security Council Resolution 2178 (2014), *available at* https://undocs.org/S/RES/2178(2014).
[45] United Nations Security Council Resolution 2396 (2017), *available at* https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf.

4. Greece and Italy protect privacy in a manner similar to the United States; and
5. Sharing certain USCIS non-criminal justice data during these crises will assist Greece and Italy in denying entry to those who may pose a threat to Europe and the United States.

Analysis of Facts Considered in Determining the Existence of Exceptional Circumstances

1. ***United Nations Security Council Resolutions 1373 (2001), 2178 (2014), and 2396 (2017) that call upon Member States to "prevent the movement of terrorists or terrorist groups by effective border controls."***

Terrorist attacks in Brussels, Paris, Nice, Berlin, Istanbul, London, Stockholm, Manchester, and elsewhere reveal the way in which the global terrorist threat has evolved, to include attacks by foreign terrorist fighters returning home.

More than 30,000 foreign terrorist fighters from more than 100 nations have traveled to conflict zones, such as Syria, Afghanistan, the Horn of Africa, Yemen, Libya, and Iraq.[46] Many foreign terrorist fighters have joined the massive flow of refugees and asylum seekers from these conflict zones.

Because the challenges posed by the return of foreign terrorist fighters are by nature international, the U.N. Security Council has repeatedly called on Member States to enhance their international cooperation to prevent their travel. On December 21, 2017, the United Nations Security Council unanimously adopted a new resolution intended to help Members States to detect and counter the growing threat posed by foreign terrorist fighters returning from conflict zones. Like prior Resolutions, Resolution 2396 "[c]alls upon Member States to prevent the movement of terrorists by effective national border controls." Resolution 2396 differs from other Resolutions in that it also requires Member States to "develop and implement systems to collect biometric data … [to] include fingerprints … in order to responsibly and properly identify terrorists, including foreign terrorist fighters…." And Resolution 2396 encourages Member States to share such data responsibly with relevant Member States.[47]

2. ***The European Commission's declaration that the Greece and Italy migration situations are emergencies that requires immediate action.***

The sharing of certain USCIS non-criminal justice data will assist Greece and Italy in denying entry or refugee status to those who may pose a threat to Greece, Italy, the United States, and other U.S. allies. Most notably, in October 2015, four terrorists posing as Syrians escaping the

---

[46] Foreign Terrorist Fighters, United Nations Security Council, Counter-Terrorism Committee, *available at* https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters.
[47] United Nations Security Council Resolution 2396 (2017), *available at* https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf.

war arrived on a Greek island with fraudulent passports and identities according to subsequent press reporting.[48] Consistent with an exception to the Schengen Agreement, several EU member countries continue to carrying out temporary border checks on anti-terror grounds.[49]

As previously discussed, the volume of migrants flowing into Europe has created a humanitarian crisis, which further impedes the ability to properly identify those seeking to do harm. In September 2017, the Office of the United Nations High Commissioner for Refugees (UNHCR) expressed concern over the deteriorating situation in Greece:

> "Arrivals on [certain hotspot Greek islands] have now outpaced the rate at which people are being authorized by the authorities to transfer to the mainland, further worsening already very challenging living conditions. Estimated departures for the mainland last month were 2,561 against 3,695 arrivals, based on data from the authorities. Many of the people have been staying on the islands for months and the conditions have affected their physical and mental health. The threat of violence, self-harm and sexual assault is extremely worrying and more security is needed."[50]

In its September 2017 report on its visits to Greece, the Council of Europe's Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment found:

> "over crowding, combined with high levels of inter-detainee violence, insufficient basic health-care provision, inadequate assistance to vulnerable groups and deficient legal safeguards, created a "highly explosive situation" on certain hotspot Greek islands."[51]

In July 2017, with regards to the Italian crisis, UNHCR declared:

> "What is happening in front of our eyes in Italy is an unfolding tragedy. In the course of last weekend, 12,600 migrants and refugees arrived on its shores, and an estimated 2,030 have lost their lives in the Mediterranean since the beginning of the year."[52]

---

[48] Raziye Akkoc and Melanie Hall, "Germany Investigates Suspected Terrorists Posing as Migrants," The Telegraph, October 29, 2015, http://www.telegraph.co.uk/news/worldnews/europe/germany/11963672/Germanyinvestigates-suspected-terrorists-posing-as-migrants.html.

[49] *Temporary Reintroduction of Border Control* https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen/reintroduction-border-control_en.

[50] *UNHCR urges action to ease conditions on Greek islands.* http://www.unhcr.org/news/briefing/2017/9/59b24a377/unhcr-urges-action-ease-conditions-greek-islands.html?query=Greece.

[51] *Greece: Anti-Torture Committee Criticises Treatment of Irregular Migrants - and Continued Detention of Migrant-Children.* https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168074f9a7.

[52] *High Commissioner Grandi urges more solidarity with Italy.* http://www.unhcr.org/en-us/news/press/2017/7/5957c2304/high-commissioner-grandi-urges-solidarity-italy.html?query=italy.

3. The sharing of non-criminal justice USCIS data sets is temporary and limited.

DHS's temporary sharing of non-criminal USCIS data sets will last only as long as such sharing is deemed necessary or beneficial to the DHS mission.

4. Greece and Italy protect privacy in a manner similar to the United States.

For instance, both Greece and Italy have endorsed the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)*.[53] The OECD Guidelines are based on the globally recognized privacy Fair Information Practice Principles (FIPPs), which are reflected in their national laws, and found in the European Union's *General Data Protection Regulation,*[54] and the Directive *on the Protection of Natural Persons With Regard To The Processing Of Personal Data By Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties.*[55]

5. Sharing certain USCIS non-criminal justice data during this crisis will assist Greece and Italy in denying entry to those who may pose a threat to Europe and the United States.

The exceptional circumstances in Greece and Italy warrant this temporary and limited sharing of certain USCIS data sets, which furthers not only the national security interests of the United States, but that of Greece, Italy, and other European and non-European U.S. allies. This sharing helps to ensure bad actors are not permitted entry to Europe or elsewhere.

Specifically, the Homeland Security Committee in the U.S. House of Representatives issued a preliminary review, which in part, found "America's security is put at risk when partner countries fail to conduct adequate counterterrorism checks on refugees and are unable to cope with the radicalization challenges created by mass migration." In particular, the Committee found "[w]hen our allies overseas are unable to effectively weed out suspects with terrorist ties from refugee flows, those individuals represent a long-term danger to U.S. security."[56]

---

[53] *OECD's Guidelines on the Protection of Privacy and Transborder Flows of PII.* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[54] Regulation (EU) 2016/679 *of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of PII and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation, *available at* http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[55] *Directive (EU) 2016/680* of *the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of PII by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at* https://db.eurocrim.org/db/en/doc/2479.pdf.

[56] U.S. House Homeland Security Committee, *Syrian Refugee Flows, Security Risks and Counterterrorism Challenges*, Preliminary Findings of a House Homeland Security Committee Review (Nov. 2015), p.9, *available at*

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. Although PCSC Agreements share many similar provisions, each agreement is individually negotiated, so there are differences among the agreements, including between the Greece and Italy agreements. This PIA examines the privacy impact of the Greece and Italy PCSC agreements as they relate to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

This PIA provides the public with transparency about the details of the Greece and Italy PCSC Agreements, and the reasons for sharing USCIS non-criminal justice data for criminal justice purposes. The following SORNs from the IDENT source system owners - ICE, CBP, and USCIS - cover the data shared with Greece and eventually Italy under the PCSC Agreements:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, which covers records documenting ICE's criminal arrests, and also those documenting most of ICE's immigration enforcement actions;[57]

https://homeland.house.gov/wp-content/uploads/2015/11/Homeland-Security-Committee-Syrian-Refugee-Report.pdf.

[57] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016).

- DHS/CBP-006 Automated Targeting System; which supports CBP in identifying individuals and cargo that need additional review traveling to and from the United States;[58]
- DHS/USCIS-002 Background Check Service; which consolidates all background check requests and results on immigration benefit applicants / petitioners;[59]
- DHS/USCIS-003 Biometric Storage System, serves as the central repository for all biometric data captured by USCIS from applicants filing immigration applications;[60] and
- Forthcoming DHS-wide External Biometric Records SORN.[61]

In response to a query match on fingerprints, certain additional PII (e.g., biographics, encounter-related information) may be provided automatically by the receiving country to the querying country. If the queried fingerprint does not match the holdings in the receiving country's automated biometric system, then the fingerprint is not retained by the receiving country, unless the fingerprints are provided on a country's own initiative to alert the other PCSC signatory country of an impending terrorist or serious crime threat.

In the Greece and Italy PCSC Agreements, biographic information is automatically shared on a person of interest following a biometric match, which may include: first and last names, former names, other names, aliases, alternative spelling of names, gender, date and place of birth, photographs, current and former nationalities, passport data, numbers from other identity documents[62] and applicable encounter data. *See Appendix A* for a full list of data

---

[58] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[59] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[60] DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 3, 2007). As stated earlier, The USCIS Office of Privacy is in the process of consolidating DHS/USCIS-002 Background Check Service and DHS/USCIS-003 Biometric Storage System SORNs into a new SORN, titled the *Immigration Biometric and Background Check SORN* to holistically cover biometric and biographic screening and background checks for USCIS customers and international partners. Once this consolidated SORN is published in the Federal Register, it will be *available at* www.dhs.gov/privacy.
[61] The DHS Privacy Office is in the process of developing a new SORN, titled the External Biometric Records SORN, to allow DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic, for the following purposes pursuant to formal or informal information sharing agreements or arrangements ("external information"), or with the express approval of the entity from which the Department received biometric and associated biographic information: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. Once this SORN is published in the Federal Register, it will also be available at www.dhs.gov/privacy.
[62] The terms of the *Implementing Arrangement* for the Italy PCSC also specifies that "numbers from other identity documents and criminal, police and alien records" may be shared. *The Implementing Arrangement under the Agreement between the Government of the United States of America and the Government of the Italian Republic on Enhancing Cooperation in Preventing and Combating Serious Crime, Italian PCSC signed at Rome on May 28,*

elements that may be shared with Greece and Italy. Currently, DHS is only able to receive fingerprints from Greece, and not able to query the fingerprint holdings of Greece in an automated fashion. DHS is expected to begin receiving fingerprints from Italy in 2018.

The Greece and Italy PCSC Agreements also permit each country, in compliance with their respective national laws, to share PII - without being requested to do so – to supply information to the other country when there is a reason to believe a person may be a threat. Such instances are defined as when an individual:

- will commit (or may be planning to commit), or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association; or
- is undergoing or has undergone training to commit terrorist or terrorism related offenses, or offenses related to a terrorist group or association; or
- will commit (or may be planning to), or has committed a serious criminal offense or participates in an organized criminal group or association.

In both agreements, the country providing this information may impose conditions on the use of such data.[63]

Privacy Risk: A privacy risk remains that data will be shared more broadly than permitted by the relevant SORNs and the terms of the PCSC Agreement.

Mitigation: This risk is partially mitigated. The countries are obligated under the PCSC Agreements to maintain a log of all data transmitted and received. OBIM continually monitors quality assurance and generates monthly, quarterly, and annual reports for each PCSC partner country. If data are found to have been inappropriately shared, DHS will take appropriate remedial action. Also, the Chief Privacy Officer may direct an internal Privacy Compliance Review to ensure USCIS and other data sets are appropriately shared with Greece and Italy. In so doing, the DHS Privacy Office will work with the relevant component privacy officer and the program to identify and remedy any problems to sustain compliance. Nevertheless, DHS's ability to deploy its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, investigations, onsite inspections) is greatly limited when a partner is located overseas. Therefore, it is important for DHS and its partner countries to establish strong working relationships, with regular communications, to ensure compliance with the PCSC agreements are faithfully adhered to by all countries.

2009 (signed *October 20, 2017), available at* https://www.dhs.gov/news/2017/10/20/acting-secretary-homeland-security-elaine-duke-meets-italian-minister-interior-marco.

[63] *Greece Agreement*, Article 11; *Italy Agreement*, Article 10.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Individual participation provides the Government with the most accurate information about the public, while the public is given greater access to the information maintained by the Government. However, a traditional approach to individual participation is not always practical or possible when sharing information with law enforcement agencies, such as in the context of PCSC Agreements. It would be counterproductive to provide persons of interest with access to information about themselves during a pending law enforcement investigation, as this would alert them to, or otherwise compromise the investigation. Although individuals cannot participate in the initial collection or access their records during a pending law enforcement investigation, these individuals may contest or seek redress through any resulting proceedings brought against them.

The right of individuals to request amendments to their records under the Privacy Act of 1974 (5 U.S.C. §552a) (Privacy Act) is limited to United States citizens and lawful permanent residents. Executive Order No. 13,768, *Enhancing Public Safety in the Interior of the United States (EO 13,768)* (January 25, 2017) reiterates that agencies, to the extent consistent with applicable law, will ensure that only PII relating to United States citizens and lawful permanent residents are covered by the protections of the Privacy Act. However, the Judicial Redress Act of 2015 (Judicial Redress Act) (5 U.S.C. §552a note), which amended the Privacy Act, provides citizens of covered countries with access and amendment rights under the Privacy Act in certain limited situations, as well as the right to sue for civil damages for willful and intentional disclosures of covered records made in violation of the Privacy Act.[64]

The DHS Privacy Policy that implements EO 13,768[65] makes clear that DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate,

---

[64] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website https://www.justice.gov/opcl/judicial-redress-act-2015.

[65] DHS Memorandum 2017-01: *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 25, 2017) (DHS Privacy Policy), *available at* https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf. As the DHS Privacy Policy notes, Executive Order 13768, does not affect statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. §1367. These laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and aliens, regardless of a person's immigration status.

relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes.

Individuals not covered by the Privacy Act or the Judicial Redress Act may access their records by filing a Freedom of Information Act (FOIA) with the respective Component or DHS FOIA office. Additional information about FOIA is available at http://www.dhs.gov/foia. Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The legal authority for PCSC Agreements is found in the *Secure Travel and Counterterrorism Partnership Act of 2007,*[66] which imposes requirements on current Visa Waiver Program (VWP) countries. The VWP uses a risk-based, multi-layered approach to detect and prevent terrorists, serious criminals, and other bad actors from traveling to the United States. Greece and Italy, both VWP countries, have entered into PCSC Agreements and Implementing Arrangements with the United States.[67]

The stated purpose of the agreement with Greece is to enhance the cooperation between the United States and Greece in "*preventing and combating* serious crimes."[68] The purpose of the Italian agreement is not substantively different, though it is stated "to enhance the cooperation between the United States and [Italy] in the *prevention and investigation* of serious crimes (emphasis added).[69]

The Greece Implementing Arrangement more specifically describes its purpose as:

---

[66] *Secure Travel and Counterterrorism Partnership Act of 2007(*incorporated into *the Implementing Recommendations of the 9/11 Commission Act of 2007),* codified as amended in 8 U.S.C. 1187.
[67] Greece PCSC Agreement and Implementing Arrangement: *Agreement Between the Government of the United States of America and the Government of the Hellenic Republic on Enhancing Cooperation in Preventing and Combating Serious Crime (Greece Agreement) (June 28, 2009);* and the *Implementing Arrangement under the Hellenic Republic on Enhancing Cooperation in Preventing and Combating Serious Crime* (Greece Implementing Arrangement) (November 7, 2016) *(*collectively both are referred to as the Greece Agreement*)*; Italy PCSC Agreement and Implementing Arrangement: *Agreement Between the Government of the United States of America and the Government of the Italian Republic on Enhancing Cooperation in Preventing and Combating Serious Crime (Italy Agreement) (May 28, 2009);* and the *Implementing Arrangement under the Agreement Between the Government of the United States of America and the Government of the Italian Republic (October 20, 2017) (Italy Implementing Arrangement) (*collectively both are referred to as the Italy Agreement*).*
[68] *Greece Agreement,* Article 2.
[69] *Italy Agreement,* Article 2.

> "identify[ing] criminals, including potential terrorists or other threats to national security, attempting to exploit the international movement of migrants, refugees and asylum seekers for mala fide purposes, including obtaining documents valid for VWP travel."[70]
>
> The Italy Implementing Arrangement similarly describes the purpose of its sharing as:
>
> "identify[ing] individuals who attempt to exploit the international movement of migrants, refugees and asylum seekers to commit the crimes of terrorism, offenses linked to illegal immigration or other serious crimes, including fraudulent acquisition of or misrepresentation on documents, including those valid for Visa Waiver Program (VWP) travel."[71]

In addition to preventing and combating serious crimes and terrorist activities, the information sharing under the PCSC Agreements helps to also preserve the integrity of the VWP by identifying fraudulent documents presented by those who seek to exploit the VWP process. For instance, if a VWP country notices a discrepancy between the biographic information (e.g., name nationality, date of birth) on a passport with the biographic information provided by DHS as a result of fingerprint match, this may indicate a potentially fraudulent or stolen passport. VWP countries are required to report lost or stolen passports to the United States, through Interpol.[72]

Privacy Risk: There is a risk that sharing will be predicated on crimes not deemed to be "serious crimes" in the United States.

Mitigation: This risk cannot be mitigated. The Greece Agreement permits each country to provide a list of serious crimes for which a query should *not* be made by either party.[73] On the other hand, Italy and the United States agreed on a comprehensive list of offenses that *will* serve as the basis for cooperation under their respective national laws.[74] Although OBIM monitors the transmissions for quality assurance, data may still be shared inappropriately. If this occurs, both the Greece and Italy Agreements require the receiving country, for instance, to correct, block, or delete data when the collection or further processing of the data contravenes the Agreement or the supplying country's information sharing rules. DHS will take appropriate remedial action to ensure the receiving country purges any information about crimes associated with an individual that are not deemed "serious crimes" (i.e., felonies) in the United States. These remedial actions, however, may not always fully remedy or mitigate the actions already taken by the receiving country. The Chief Privacy Officer may also direct an internal Privacy Compliance Review or other action to help avoid future reoccurrences.

---

[70] *Greece Implementing Arrangement*, Section 1.
[71] *Italy PCSC Implementing Arrangement*, Section 1.
[72] 8 USC §1187(c)(2)(D).
[73] *Greece Agreement*, Article 2.
[74] *Italy Agreement*, Article 5(2); *Italy Implementing Arrangement, Technical Annex.*

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The signatory countries to the Greece and Italy PCSC Agreements commit to processing PII fairly, in accordance with their laws, to:

- ensure that the personal data provided are adequate and relevant in relation to the specific purpose of the transfer;
- retain personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Agreement; and
- ensure that possibly inaccurate personal data are timely brought to the attention of the receiving Party in order that appropriate corrective action is taken.[75]

If there is no match to the initial query, transmitted biometric data will be deleted, consistent with applicable law. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared, in accordance with applicable national laws and established information retention policies. PII is retained for as long as necessary for the specific purpose for which the data were provided, as determined by each country's national law.

As discussed earlier, all information pertaining to individuals protected by 8 U.S.C. § 1367 are generally protected from disclosure to third parties, except in limited circumstances. This statutory prohibition applies to *all* IDENT encounters pertaining to a protected individual, not only the encounters specific to the protected benefit type. In addition, encounters related to individuals having Temporary Protected Status are filtered out in an automated manner. Individuals who fall into any other special protected class are manually filtered out of any PCSC sharing, pending the development of an automatic filtering process.

Asylum and refugee-related information, as previously mentioned, will not be shared with Greece or Italy without signature of a Secretarial waiver, pursuant to 8 C.F.R. 208.6, permitting such disclosure.

---

[75] *Greece PCSC Agreement*, Article 12; *Italy PCSC Agreement*, Article 11.

The Secure Real-Time Platform (SRTP), as described earlier, uses CBP's Unified Passenger System (UPAX), a module of CBP's Automated Targeting System (ATS),[76] which acts as a proxy between IDENT and a foreign partner's automated biometric identification system. Since UPAX is only a proxy to the IDENT system, CBP does not retain a copy of data passing through UPAX or for additional queries. UPAX records transaction details used only for auditing purposes.

Privacy Risk: There is a risk that information about individuals in special protected classes will be inadvertently shared with the querying country.

Mitigation: This risk is partially mitigated. While the automatic and manual filtering processes are methodically performed, data concerning an individual in a special protected class may be inadvertently shared with a partner country. For instance, an individual's special protected class status may not have been known at the time of the sharing. In order to ensure such sharing is performed appropriately, DHS is obligated under the PCSC Agreements to maintain a log of all data transmitted and received, which will be reviewed on a regular basis. OBIM has a dedicated team that continuously monitors and reports on the sharing with partner countries. Reports are generated, reviewed, and distributed to ICE, USCIS, and the DHS Office of Policy. If information is found to have been inappropriately shared, DHS will take remedial action, such as increased training. The DHS Chief Privacy Officer may also direct that a Privacy Compliance Review be conducted or take other action, or refer the issue to another oversight office (such as the DHS Office of Civil Rights and Civil Liberties), as appropriate.

Privacy Risk: There is a risk that PII will be retained longer than is necessary.

Mitigation: This risk is partially mitigated. OBIM has a dedicated team that continually monitors the sharing to ensure quality assurance and issues reports on its sharing with PCSC partner countries. These monthly, quarterly, and annual reports help identify and remedy any data that are retained longer than necessary. The countries agree to engage in regular consultations with each other, which may also help to identify areas of non-compliance. If data are found to have been retained by DHS longer than necessary, then DHS will take appropriate remedial actions, including notifying the data owner if its data is retained longer than necessary. The DHS Privacy Officer reserves the right to initiate an internal Privacy Compliance Review to ensure data are appropriately retained.

[76] *See* DHS/CBP/PIA-006 Automated Targeting Systems and subsequent updates, *available at* www.dhs.gov/privacy.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The Greece and Italy PCSC Agreements restrict *the use* of data to the following: a) criminal investigations; b) preventing a serious threat to its public security; c) non-criminal judicial or administrative proceedings directly related to its criminal investigations; or d) for any other purpose, only with the prior consent of the country which has supplied the data.[77]

The countries are not permitted to communicate data provided under the respective PCSC Agreement to any third State, international body, or private entity without the consent of the country that provided the data, and without the appropriate safeguards. The Greece Agreement restricts querying to only individual cases relating to detecting, combating, and investigating serious crimes,[78] while the Italy PCSC Agreement limits queries to individual cases for the prevention and investigation of serious crimes.[79]

DHS will provide certain data under extraordinary circumstances to Greece and Italy, and trusted foreign partners, to prevent criminals and terrorists from abusing migration. This is consistent with UN Security Council Resolutions, which make expediting such cooperation a priority. The USCIS data sharing will last for only as long as DHS deems it necessary or beneficial to the DHS mission.

Privacy Risk: There is a risk that information may be shared on individuals not in the course of preventing or combating serious crimes.

Mitigation: This risk is partially mitigated. The Greece and Italy PCSC Agreements include accountability and auditing mechanisms to ensure the agreements are properly implemented. As discussed in the Accountability and Auditing section below, the countries are obligated to maintain a log of all data transmitted and received, which is required to be maintained securely for two (2) years. Each country supplying data is entitled to an accounting of what has been done with the data it supplied, and the results obtained from the data it provided. Answers are to be provided in a timely manner. The countries also agree to consult one another regularly on the implementation of their agreement. OBIM continuously conducts quality assurance monitoring and generates monthly, quarterly, and annual reports on its sharing with each PCSC partner country. If data are found to have been inappropriately shared, then DHS will take appropriate remedial actions. The DHS Chief Privacy Officer also reserves the right to

[77] *Greece Agreement*, Article 13; *Italy Agreement*, Article 12.
[78] *Greece Agreement*, Article 4(1).
[79] *Italy Agreement*, Article 2(2).

initiate an internal Privacy Compliance Review to ensure data are appropriately shared with Greece and Italy.

Privacy Risk: There is a risk that a partner country may share DHS-provided data with a third party without first obtaining DHS's consent.

Mitigation: This risk is partially mitigated. The Greece and Italy PCSC Agreements include accountability and auditing mechanisms to ensure the agreements are properly implemented. The Greece and Italy PCSC agreements permit the supplying country to inquire how its data were used and the results obtained, although even this request may not always be fulfilled; and even if this request were fulfilled, any such remedial actions would be forward-looking and would not remedy or mitigate the unauthorized sharing that has already occurred.

DHS's ability to deploy its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, investigations, onsite inspections) used within the Department or with domestic third-party vendors is greatly limited when our partner is located overseas. It is for this reason that both the United States and its partner countries need to establish strong working relationships, with regular communications, to ensure compliance with the PCSC Agreements are faithfully adhered to by all countries. Otherwise, the risk of impairing a cooperative relationship by a country engaging in misconduct, such as unauthorized sharing, is too great and would betray the trust between the countries and the national security benefits derived from PCSC agreements. If DHS concludes that a country is not a responsible steward of the PII with which it is entrusted, then terminating the PCSC agreement, in accordance with its terms, may be an option for consideration by DHS.

Privacy Risk: There is a risk that DHS will continue to share information for longer than originally intended and when circumstances are no longer considered exigent.

Mitigation: This risk is partially mitigated. DHS expects to share non-criminal USCIS data sets as long as such sharing is deemed necessary or beneficial to the DHS mission. The DHS Chief Privacy Officer may periodically review the program to ensure DHS's exchange of information is appropriate and consistent with the original purpose.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

PCSC Agreements help to preserve the data integrity of the VWP by identifying fraudulent documents of those seeking to illegally exploit the program. For instance, at the request of the querying country, the receiving country is obligated to correct, block, or delete data - consistent with its national law- that are incorrect or incomplete, or if its collection or use violates the PCSC agreement, or rules applicable to the querying country.

When a country becomes aware that material data it transmitted or received are inaccurate, unreliable, or subject to significant doubt, it is responsible for notifying the other country and taking all appropriate measures to safeguard against erroneous reliance on such data, which may include supplementation, deletion, or correction of the data.[80] As discussed, VWP countries are specifically required to report lost or stolen passports to the United States.[81]

Privacy Risk: A risk exists that a partner country will not inform DHS that data it provided were inaccurate.

Mitigation: This risk is partially mitigated. The Greece and Italy PCSC Agreements include accountability and auditing mechanisms to ensure the agreements are properly implemented. Although OBIM has a dedicated team that continually monitors and reports on the sharing with our PCSC partner countries, the monitoring may or may not identify whether any inaccurate data has been provided by the partner country. DHS's ability to deploy its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, onsite inspections) is greatly limited when our partner is located overseas. It is for this reason that both the United States and its partner countries need to establish strong working relationships, with regular communications, to ensure compliance with the PCSC agreements are appropriately implemented. The DHS Chief Privacy Officer may also choose to open an internal Privacy Compliance Review to ensure that DHS and its partner country are complying with the terms of a PCSC agreement.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The PCSC Agreements with Greece and Italy ensure that the necessary technical and organizational measures are used to protect PII against accidental or unlawful destruction, accidental loss, unauthorized disclosure, alteration, access, or any unauthorized processing of the data. Each country must take reasonable measures so only authorized individuals have access to the PII exchanged.

The countries must also establish procedures for automated querying of fingerprints using appropriate technology to ensure data protection, security, confidentiality, and integrity; employ encryption and authorization procedures that are recognized by each country's respective expert authorities, as well as ensuring that only permissible queries are conducted.

---

[80] *Greece Agreement*, Article 14(2); *Italy Agreeme*nt, Article 13(2).
[81] 8 USC §1187(c)(2)(D).

Privacy Risk: There is a risk that the transmission of data between DHS and Greece and Italy, respectively, will be intercepted by a third party.

Mitigation: This risk is partially mitigated by the SRTP, which uses high security encryption protocols to provide biometric query and response capabilities. As depicted earlier, SRTP uses a server proxy – CBP's Unified Passenger System (UPAX) – so there is not a direct connection between a foreign partner's server and IDENT. The transmissions are conducted over the public Internet using a Virtual Private Network (VPN) connection to provide a secure "tunnel" between UPAX and foreign partners.

Despite the robust protocols of SRTP, DHS cannot fully mitigate any security risks associated with Greece's and Italy's technology and processes. However, under Greek law, the data controller must implement appropriate organizational and technical measures to secure data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful processing.[82] Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing.

DHS places limitations on third-party sharing, by limiting the amount of data shared based on specific circumstances described in information sharing access agreements, and by conducting periodic reviews, as appropriate, of the use of the data with end users.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The PCSC Agreements require each country to maintain a log of the transmission and receipt of data communicated to the other country. This log serves to: a) ensure effective monitoring of data protection in accordance with the national law of the respective country; b) enable the countries to effectively make corrections, block, or delete certain data; c) inform the querying country of the result obtained from the supplied data; and d) ensure data security.

The log must include: a) information on the data supplied (Italy Agreement also requires the purpose for supplying the data); b) the date on which the data was supplied; and c) the recipient of the data in case the data are supplied to other entities.

The countries must protect the log with suitable measures against inappropriate use and other forms of improper use, and shall be kept for two (2) years. In particular, the Greece

[82] *Ten points of importance for Controllers* by the Hellenic Data Protection Authority: http://www.dpa.gr/portal/page?_pageid=33,43376&_dad=portal&_schema=PORTAL.

Agreement specifies that the log may be kept longer than two (2) years (and not deleted) if it is necessary for the specific purpose for which the data were provided, or for further use in accordance with the PCSC agreement. The Italy Agreement, however, requires the log be immediately deleted after two (2) years, unless that would be inconsistent with national law, including applicable data protection and retention rules.

The Implementing Arrangements for both Greece and Italy require the countries to regularly engage in consultations to, in part, review the number of automated queries made and percentage of automated matches, and share, to the extent practical, additional statistics and case studies demonstrating how the exchange of information under the agreement has assisted in encountering serious crime and terrorism (the Italy Implementing Arrangement adds "or other threats to national security").[83] As discussed, in order to ensure continued value in sharing USCIS data, OBIM will provide the DHS Privacy Office with metrics on a regular basis to confirm that this sharing remains relevant and beneficial to DHS.

The Greece and Italy Implementing Arrangements further require the countries to consult one another on any privacy incidents (including unauthorized access or disclosure) involving PII shared under the agreement, and remedial actions taken in response to any such incidents.[84]

Privacy Risk: There remains a risk that a partner country may not report a privacy incident to DHS, including unauthorized access or disclosure of PII.

Mitigation: This risk is partially mitigated. As discussed, countries are required to keep a log of data sent and received. As discussed, the country supplying the data is entitled to inquire with the receiving country about what was done with the data and results generated. This response may be useful in revealing privacy incidents or unauthorized disclosures by a partner country. However, it is dependent on the partner country's willingness to comply with the request and to be transparent about prior privacy incidents involving DHS-supplied data. In the event DHS concludes that the country is not a responsible steward of the PII with which it is entrusted, then terminating the PCSC agreement, in accordance with its terms, may be an option for consideration by the U.S. Government.

Conclusion

PCSC Agreements provide appropriate privacy and security protections to ensure the risks inherent with international sharing are properly mitigated, while also respecting each country's laws.

---

[83] *Greece Implementing Arrangement*, Section 9; *Italy Implementing Arrangement*, Section 8.
[84] *Id.*

In its efforts to cooperate with other countries in preventing and combating serious crimes, the United States considers a country or region's unique circumstances in determining the types of data to share. This was the case when DHS deemed the situations in Greece and Italy to be exceptional. The sharing of USCIS non-criminal justice data is designed to ensure our allies have enough information at their borders to make informed decisions in the midst of their migration crises.

The privacy risks in sharing USCIS data with Greece and Italy are mitigated, to the extent possible, in part by limiting the duration and circumstances for when the data are shared. Moreover, Greece and Italy are subject to the European Union's privacy regulations, and the 2015 *Data Protection and Privacy Agreement* between the European Union and the United States, which establishes privacy protections when sharing PII for the prevention, detection, investigation, or prosecution of crimes. This sharing with Greece and Italy is a reasonable privacy-protective approach that furthers the security interests of the United States.

Responsible Officials

Michael Scardaville
Office of Policy
Department of Homeland Security

Approval Signature Page

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A

***Data Elements Shared with Greece and Italy, if Available*:**

- Providing Participant subject specific reference number;
- Providing Participant event specific reference number;
- Date fingerprinted;
- Reason fingerprinted;
- Location fingerprinted;
- Last name;
- First name;
- Date of birth;
- Passport nationality;
- Country of birth;
- Gender;
- Current immigration status;
- Other names;
- Alias last name(s);
- Alias first name(s);
- Travel document number;
- Travel document type;
- Travel document issuing authority/country;
- Travel document expiry date;
- Reason for alert;
- Visa Refusal code;
- Watchlist Indicator;
- Scan of travel document biodata page;
- Scan of other marked travel document pages;
- Facial image;

- Previous immigration status;
- Date removed;
- Date of arrival;
- Location of arrival;
- Date of departure;
- Location of departure;
- Date of immigration application or non-biometric encounter;
- Type of immigration application or non-biometric encounter;
- Date of outcome of immigration application;
- Outcome of immigration application;
- Reason for outcome of immigration application; and
- Expiry date of current leave/stay or visa.

DHS will also share the following Derogatory (DI) alert indicators:

- Deported Felon;
- Gang Member;
- Absconder;
- Identity Fraud;
- BioVisa Denial;
- Benefit Denial;
- Overstay;
- US-VISIT Program Management Office (US-V PMO);
- Recidivist;
- Alien Smuggler;
- Suspected-system;
- Final Order;
- Expedited Removal (ER)-Aggravated;
- ER-Routine;

- Pending Removal;
- Adverse Action; and
- Terrorist Screening Center (TSC)/Known or Suspected Terrorist (KST) (when tied to a matched record in the DOJ/TSC OUS).