Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable...."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

---

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5)

[redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]...[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

---

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.*, 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[4] (b) (5) [redacted]

(b) (5) [redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-157 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)
Chief, Enforcement Law Section

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – Manda

Executive Summary

We present the arguments supporting a position that Secure Communities will be mandatory in 2013. Based on applicable , and case-law, we conclude that participation in the S l be mandatory in 2013 without violating the Tenth Amendment.

Background

Secure Communities' Use of ID

In Fiscal Year 200 to "improve and modernize efforts to identify a sonment, and who may be deportable, and re re judged deportable…."[2] In response, ICE laun sform the way ICE identifies and s. In this initiative, Secure Communities utili NT and IAFIS to share information, not only to a s, but also to share immigration status info gencies (LEAs). The Secure Communities "Pro provides the planning and outreach support for ongoing efforts to a perability in jurisdictions nationwide. *See generally* Secure Co , Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20.

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).
4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an I[illegible]e (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to [illegible] to send to the originating LEA. The LESC also sends the IA[illegible]fice, which prioritizes enforcement actions ba[illegible]

There are two types of participation in Secure C[illegible] Interoperability is deployed. First, participation [illegible]-sharing in which the SIB and LEA receive the return me[illegible]erability process informing about the subject's immigrati[illegible]rst sentence). Second, a state or LEA may choose to participa[illegible]urn message or the state may not have the technological ability t[illegible]m CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability i[illegible]

According to Secu[illegible]turella and the CJIS Director reached an agreem[illegible]013, all fingerprint requests from any LEAs tha[illegible] This future information sharing will not in[illegible]ent IDENT/IAFIS Interoperability process whe[illegible]sible) the automatic return message from ICE[illegible]ccording to Secure Communities, this proc[illegible] for policy reasons and to ensure adequate reso[illegible]ies have currently chosen to wait until 2013, whe[illegible]hould be completed, until instituting this process.

[illegible]Tasks In Order to Physically Deploy IDENT/IAFIS [illegible]EA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

(b) (5) [redacted]

Discussion

The FBI's Authority To Share Fingerprint Submissi[on] [redacted] Via IDENT/IAFIS Interoperability

It is unquestioned that the FBI may share finger[print] [redacted] C. § 534 provides that the Attorney General shall "acqui[re] [redacted] fication, criminal identification, crime, and other records [redacted] o provides for the sharing of the information, by r[egulation] [redacted] change such records and information with, and for the [official use] [redacted] d officials of the Federal Government. . . ." 28 U.S.C. § 534(a)([4]) [redacted] FBI must provide ICE access to criminal history record inform[ation] [redacted] Crime Information Center files). Further, the applicable S[ystem] [notice] [redacted] FBI's Fingerprint Identification Records System (FIRS), [redacted] FIS, provides that identification and criminal history reco[rds] [redacted] prints and rap sheets) may be disclosed, in releva[nt] [redacted] irectly engaged in criminal justice activity "wh[ere] [redacted] the performance of a law enforcement functi[on] [redacted] vil law enforcement function; or where such disc[losure] [redacted] the mutual law enforcement efforts of the law e[nforcement] [redacted] e of Modified Systems of Records, 64 Fed. Reg [redacted]

The [redacted] int information with DHS via IDENT/IAFIS Inte[roperability] [redacted] he establishment of an interoperable elec[tronic] [redacted] e current and immediate access to information in databases of Fed[eral] [redacted] es and the intelligence community that is relevant to determine the [redacted] y of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

(b) [redacted]

[5] 8 U.S.C. § 1722 provides, in relevant part:

(2) Requirement for interoperable data system

Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive

Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate [illegible] erated by the Department of Homeland Security (DHS) with t[illegible]stigation (FBI). The IDENT/IAFIS project was designed to su[illegible]d prosecution of criminal aliens and to pro[illegible]personnel with direct access to DHS data through [illegible]een the two systems, DHS would have the capab[illegible]nded person is subject to a currently posted W[illegible]'s Criminal Master File. Collaterally, the i[illegible] enable cognizant law enforcement agencies to [illegible]gration information as part of a criminal history respon[illegible]

H.R. Rep. No. 109-118 (2005). Congre[illegible]s not only crucial that DHS and the Department of Justice ens[illegible]ve, in real time, the

---

intelligence communit[illegible]formation with the Department of State[illegible]t to the admissibility and deportability of aliens, cons[illegible]ction.
(b) R[illegible]rmation
(1) I[illegible]
Not [illegible]ll submit to the appropriate committees of Congress a rep[illegible]plement and the intelligence community information needed by the Depa[illegible]plicants, or by the Immigration and Naturalization Service to screen appli[illegible] States, and to identify those aliens inadmissible or deportable under the Imm[illegible].S.C.A. § 1101 *et seq.*]
(2) C[illegible]
(c) C[illegible]
(1) R[illegible]
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a Compact for the organization of an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. Under this Compact, the FBI and the ratifying states agree to maintain their respective criminal history records, including arrests and dispositions, and to make them available to the Federal Government and to other participating States for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, there are twenty-nine states that have ratified the Compact as of July 1, 2010.[9] For these twenty-nine states, participation in Secure Communities mandatory since they are already obligated by Federal law to make their criminal history records available for immigration purposes.

Case Law Supports a Position that Compelling Participation in Secure Communities in 2013 Does Not Violate the 10th Amendment

Although LEAs may argue that the Tenth Amendment prohibits DHS from compelling participation in Secure Communities, a review of relevant case law supports a position that Tenth Amendment protections are not implicated. In New York v. United States, 505 U.S. 144 (1992), the Supreme Court held that the Tenth Amendment, "[t]he Federal Government may not compel the States to enact or administer a federal regulatory program." *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may not commandeer the States to address particular problems, or require the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court struck down Brady Violence Prevention Act provisions requiring the chief law enforcement officer to conduct background checks on prospective handgun purchasers and certain related ministerial tasks. *See* i*d.* at 933-

[7] Similarly, "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information from the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information from IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate explanations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935.

The *Printz* court, however, also held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. Under this rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D [redacted] e District Court explained that "because the individuals subject to the [redacted] o register pursuant to state registration laws, and because the Act only [redacted] information rather than administer or enforce a federal prog[redacted] ate the Tenth Amendment." *Id.* at * 6. Similarly, the U[redacted] Fourth Circuit upheld a District Court's conclusion tha[redacted] not violate the Tenth Amendment because the feder[redacted] d information and "does not require the state to d[redacted] lready required, authorized, or provided by its own leg[redacted] *Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th [redacted] *ich v. Board of Directors of Upper Chesapeake Health[redacted]* D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-0[redacted], at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendme[redacted] the same federal law as in *Brown* that required a state to accept [redacted] sex offender, holding that, unlike the state officers in *Printz* [redacted] equire states, or their state officials, to do any[redacted] aws.") (citing *United States v. Pitts*, No. 07-157-A[redacted]; *cf. Reno v. Condon*, 528 U.S. 141, 150-51 ([redacted] nonconsensual sale or release by a state of a driv[redacted] Tenth Amendment, as the Act doe[redacted] ity to regulate their own citizens, but regu[redacted]

A c[redacted] larly recognize that an LEA's participation in S[redacted] of IDENT/IAFIS Interoperability) does not viol[redacted] Specifically, participation in Secure Communities does not alte[redacted] s and only requires the same provision of information to the FBI[redacted] vide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal[redacted] ring LEAs to provide fingerprint submissions along with arrest data[redacted] e for each arrest made). Therefore, unlike in *Printz* where the federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in

[11] *See* FN 6, *supra.*

Printz held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, as discussed *supra,* Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation re[redacted] 2013, if not sooner. Second, state and local officials already validat[redacted]h the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this vali[redacted]tate and local officials "to do anything they do not already do." Las[redacted]pite this ministerial task, participation in Secure Commu[redacted]fficials to enact a legislative program, administer regulati[redacted]g immigration law, but rather only involves the sa[redacted]ral Government as currently practiced. *See New Yo*[redacted]-76 (1992) (holding a federal law violated the Tenth [redacted]r to enact legislation providing for the disposal of radioac[redacted]hin their borders or to implement an administrative solution f[redacted]of, the waste).

A challenger to Secure Communities m[redacted]*ntz*, that 2013 participation in Secure Communities vi[redacted]cause it may require the State to expend significant funds in ord[redacted]am. The *Printz* Court held that Congress cann[redacted]cial burden of implementing a federal regulatory [redacted]ly, according to Secure Communities, an S[redacted]upgrades in order to have the capability to receiv[redacted]ENT/IAFIS Interoperability proc[redacted]

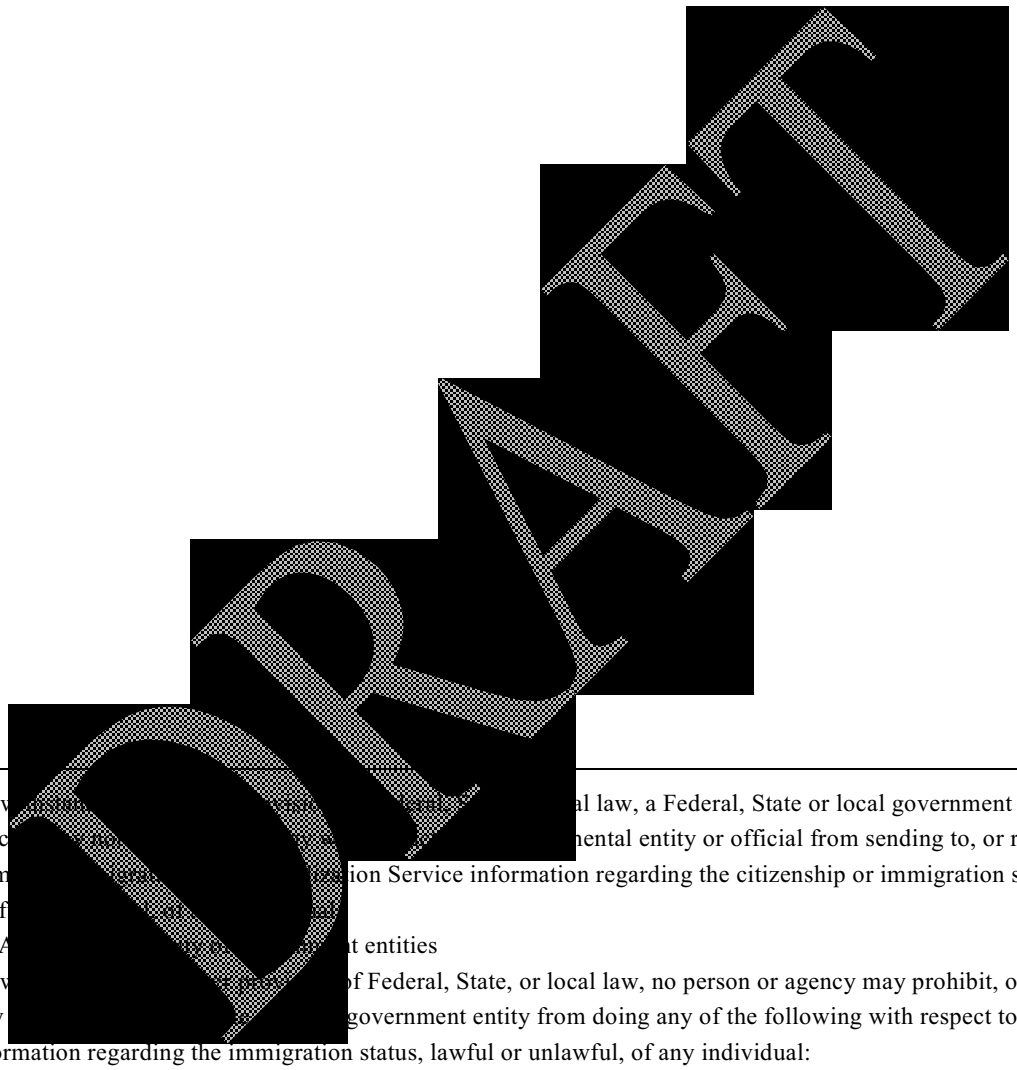
The [redacted]d fail both in 2010 and in 2013. First, part[redacted]ire the states or LEAs to receive the return IAR[redacted]nsistently informed LEAs that they may "op[redacted] IAR message if they so choose or if the SIB does not have the tech[redacted]ve that message or relay that message to the LEA. Second, as per [redacted]nt between Mr. Venturella and the CJIS Director for 2013, the [redacted] will send ICE all fingerprint requests from any non-part[redacted]de the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Last, please note that 8 U.S.C. §§ 1373[12] and 1644[13] do not support mandatory participation in Secure Communities. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.



Notw l law, a Federal, State or local government entity or offic nental entity or official from sending to, or receiving from ion Service information regarding the citizenship or immigration status, lawf

(b) A t entities

Notw f Federal, State, or local law, no person or agency may prohibit, or in any way government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)
Chief, Enforcement Law Section

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – Manda

Executive Summary

We present the arguments supporting a position [redacted] ties will be mandatory in 2013. Based on applicable sta [redacted] l case law, we conclude that participation in Secure C [redacted] datory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 inform [redacted] forms the factual basis for the legal analysis, we have included [redacted] familiar with the technology and the 2013 deployment m [redacted] Discussion section.

In the Discussion s [redacted] h the mandatory nature of the 2013 Secure Comm [redacted] relating to Attorney General sharing of criminal [redacted] S.C. § 1722, which mandates a data-sharing syst [redacted] agencies to determine the inad [redacted] U.S.C. §14616, which establishes an info [redacted] government and ratifying states. Con [redacted] ment that the 2013 Secure Communities dep [redacted]

Our [redacted] trates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the sem [redacted] l state participation in mandatory government programs. Sig [redacted] hat "federal laws which require only the provision of info [redacted] rnment" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more [redacted] receive that information from DOJ. Consequently, choices availab[redacted]ncies who have thus far decided to decline or limit their participation i[redacted]ing processes will be streamlined and aspects eliminated. In tha[redacted]nce, becomes "mandatory" in 2013, when the more [redacted]ar 2013 was chosen by ICE and DOJ for policy and resc[redacted]

Secure Communities' Use of IDENT/IA[redacted]

In Fiscal Year 2008, Congress appropriated $20[redacted]nprove and modernize efforts to identify aliens convicted of a [redacted]nt, and who may be deportable, and remove them from the [redacted]ed deportable…."[2] In response, ICE launched the Secure Co[redacted] the way ICE identifies and removes criminal aliens from the U[redacted]ecure Communities utilizes existing technology, *i.e.* the abi[redacted]to share information, not only to accomplish its g[redacted]hare immigration status information with s[redacted]s). The Secure Communities "Program Manager[redacted]ch support for ongoing efforts to activate IDENT/[redacted]vide. *See generally* Secure Communities: Qua[redacted]terly Report to Congress Third Quarter, at iv, 20.

The [redacted]AFIS Interoperability process:

[redacted]ed and booked into custody, the arresting LEA sends the [redacted]d associated biographical information to IAFIS via the [redacted]fication Bureau (SIB).
[redacted]es the subject's biometric and biographic information to US-[redacted]ine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the [redacted] us (See Step 5, first sentence). Second, a state or LEA may choose [redacted] to receive the return message or the state may not have the tec[redacted]e the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant D[redacted] CJIS Director reached an agreement by which CJIS will send [redacted] quests from any LEAs that are not participating in Sec[redacted] future information sharing will not include the component [redacted] eroperability process where the SIB and LEA receive (if tech[redacted] eturn message from ICE regarding the subject's immigratio[redacted] ommunities, this process is technologically available no[redacted] d to ensure adequate resources are in place, CJIS and Secure[redacted] ntly chosen to wait until 2013, when all planned d[redacted] ing this process.

Current CJ[redacted] loy IDENT/IAFIS Interoperal[redacted]

Acc[redacted] ministerial-related IT tasks that, pursuant to curr[redacted] physically deploy IDENT/IAFIS Inte[redacted] e" its "unique identifier" (called an "ORI") that [redacted] official contacts CJIS to inform CJIS that the ORI [redacted] inal). Once this validation occurs, CJIS must note within IAFIS the [redacted] ill be informed to relay fingerprints to IDENT that originate fro[redacted]

(b) (5) [redacted]

[4] (b) (5) [redacted]

(b) (5)

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerp S, and, therefore, ICE. This authority derives from three distinct s lating to Attorney General sharing of criminal records with other gov . § 1722, which mandates a data-sharing system to enable intelligen ncies to determine the inadmissibility or deportability of h establishes an information-sharing compact bet ving states. Federal register notices and the legislati ain that a system such as the 2013 Secure Communities d

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides A acquire, collect, classify, and preserve identification, cri other records." 28 U.S.C. § 534(a)(1). That law also prov information, by requiring that the Attorney Gene th, and for the official use of, authorized officials 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must pr ormation contained within National Crime Inf e System of Records Notice for the FBI's Finge stem (FIRS), which are maintained within IAF story record information (*i.e.*, fingerprints and to a federal law enforcement agency directly eng sclosure may assist the recipient in the perf a federal agency for "a compatible civil law enf such disclosure may promote, assist, or otherwise serve the mut of the law enforcement community." Notice of Modified Sys g. 52343, 52348 (September 28, 1999).

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate [redacted] erated by the Department of Homeland Security (DHS) with t[redacted]tigation (FBI). The IDENT/IAFIS project was designed to su[redacted]d prosecution of criminal aliens and to pro[redacted]personnel with direct access to DHS data through [redacted]een the two systems, DHS would have the capab[redacted]nded person is subject to a currently posted W[redacted]'s Criminal Master File. Collaterally, the i[redacted] enable cognizant law enforcement agencies to c[redacted]gration information as part of a criminal history respon[redacted]

---

develop and implement an interoperable electro[redacted] immediate access to information in databases of Federal law enforc[redacted]mmunity that is relevant to determine whether to issue a visa or to determi[redacted]ility of an alien (also known as the "Chimera system").

8 U.S.C. 1721, refer[redacted]

(a) Interim directive
Until the plan required[redacted]al law enforcement agencies and the intelligence communit[redacted]formation with the Department of State[redacted]t to the admissibility and deportability of aliens, cons[redacted]ction.
(b) R[redacted]rmation
(1) I[redacted]
Not [redacted]all submit to the appropriate committees of Congress a rep[redacted]plement and the intelligence community information needed by the Depa[redacted]plicants, or by the Immigration and Naturalization Service to screen appli[redacted] States, and to identify those aliens inadmissible or deportable under the Imm[redacted].S.C.A. § 1101 *et seq.*]
(2) C[redacted]
(c) C[redacted]
(1) R[redacted]
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Se for twenty-nine states. This statute establishes a co ronic information sharing system among the federal g criminal history records for noncriminal justice purposes cluding immigration and naturalization matters. *See* 42 the FBI and the ratifying states agree to maintain detaile l history records, including arrests and dispositions, and to the federal government and to other ratifying state 2 U.S.C. 14616(b). According to the FBI website, twenty-n act as of July 1, 2010.[9] For these twenty-nine states, a court ma ommunities mandatory since they are already required by the a al history records available for immigration matters.

Compelling Does Not Raise Constitutio

Although LEAs ma . Constitution prohibits ICE fro ties, applicable case law supports a position that . Under the Tenth Amendment, "[t]he Fed implement, by legislation or executive acti *nited States*, 521 U.S. 898, 925 (1997). Sim ment may neither issue directives requiring the States to

[7] Sim it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biom IAFIS database, and that the IAFIS database can retrieve, in real time, biom ENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] Th ations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphas

Applying this holding, the United States District Court for t w York found no Tenth Amendment issue in a federal act that requi de information regarding sexual offenders-informa y already have through their own state registries-t *wn*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D urt explained that "because the individuals subject ter pursuant to state registration laws, and because information rather than administer or enforce a does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of A eld a District Court's conclusion that a federal reporting requ th Amendment because the federal law only requires the state t "does not require the state to do anything that th ed, or provided by its own legislative comma , 313 F.3d 205, 214 (4th Cir. 2002) (citing *Friel e Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2 r-00332-OWW, 2008 WL 505 ng a Tenth Amendment challenge to the pro t required a state to accept registration info ke the state officers in *Printz*, the federal law "do o anything they do not already do under thei 07-157-A, 2007 WL 3353423 (M.D.La. Nov *don*, 528 U.S. 141, 150-51 (2000) (holding a federal act which rest or release by a state of a driver's personal information does not viol s the Act does not require the states in their sovereign capacity to re ut regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11]*See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking t[illegible]heness and for its defects." *Id.* at 930. A court following this *Pri*[illegible]ize that certain jurisdictions do not want to be blamed for the immig[illegible] constituents resulting from its participation in Secure Comm[illegible]

ICE has several defenses to the above claim. Fi[illegible]S-VISIT are currently discussing the necessity of this mi[illegible]ossible that this additional pre-activation requirement n[illegible]inated sooner. Second, state and local officials already [illegible]e FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, th[illegible]ot force state and local officials "to do anything they do not al[illegible]that, despite this ministerial task, participation in Secure [illegible]tate or local officials to enact a legislative program, administer [illegible]tions enforcing immigration law, but rather only involv[illegible]on to the federal government as currently practiced. *See* [illegible]*s*, 505 U.S. 144, 175-76 (1992) (holding a f[illegible]requiring states either to enact legislation providi[illegible]ted within their borders or to implement an adm[illegible]ession of, the waste).

A c[illegible]ue, in reliance on *Printz*, that 2013 part[illegible]enth Amendment because it may require the Stat[illegible]ment the program. The *Printz* Court held that[illegible]sorb the financial burden of implementing a fede[illegible]930. Currently, according to Secure Con[illegible] to pay for its own technological upgrades in order to have the capa[illegible]AR message from CJIS in the IDENT/IAFIS Interoperability proc[illegible] the LEA.

The[illegible]isleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City is [redacted] ing city employees from voluntarily sending immigration status inf[redacted] al to the immigration authorities. Following passage of IIRIRA and [redacted] y brought suit against the federal government, claiming, in re[redacted] 1373 and 8 U.S.C. § 1644 violated the Tenth Amendm[redacted] nact and enforce a federal regulatory program. The Sec[redacted] and 1644 "do not directly compel states or localities [redacted], they prohibit state and local government entities or o[redacted] e voluntary exchange of immigration information [redacted] F. 3d at 35.

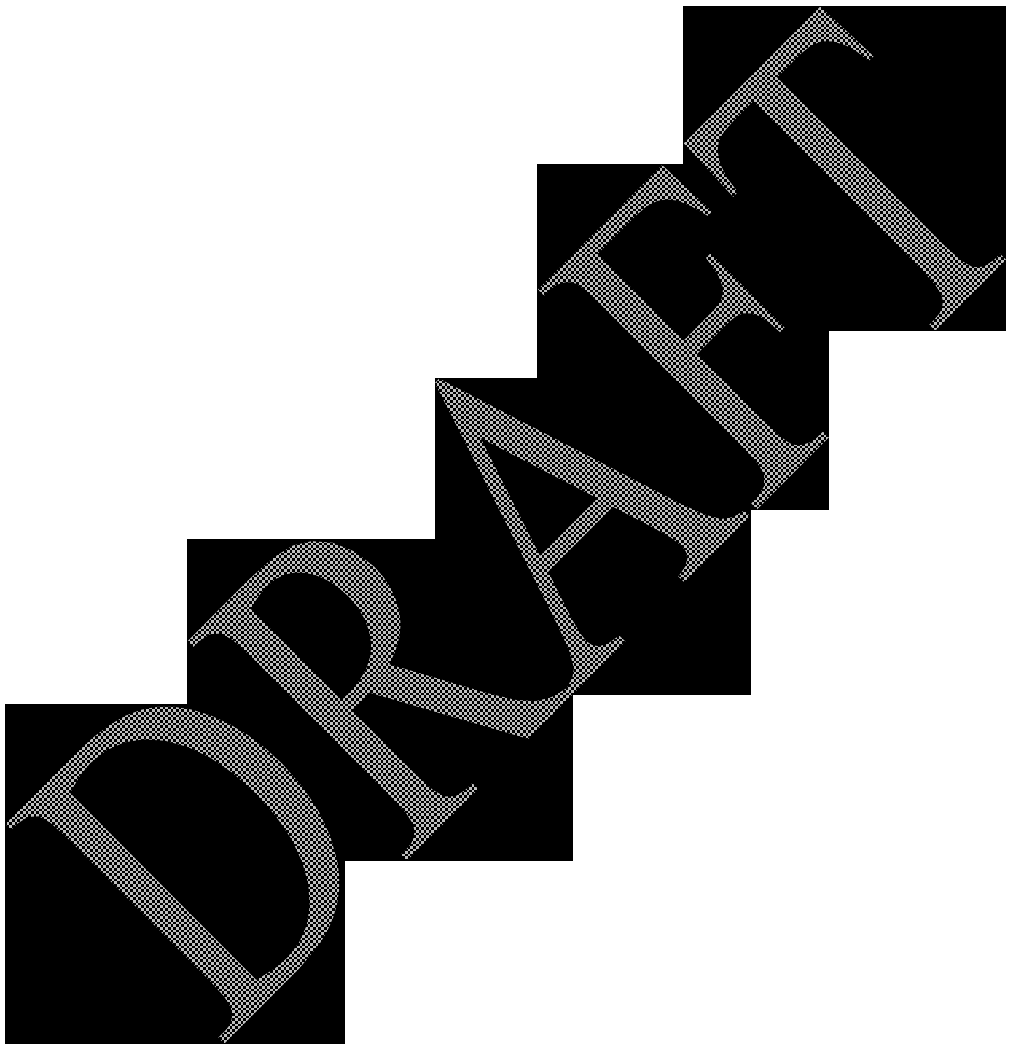
Conclusion

Based on applicable statutory authority [redacted], we conclude that there is ample support for the argument [redacted] Communities will be mandatory in 2013 [redacted] cal information will be shared with ICE at that tim[redacted] nt concerns of unconstitutional compulsion by stat[redacted]

[12] 8 [redacted]
(a) I[redacted]
Notw[redacted] al law, a Federal, State or local government entity or offic[redacted] mental entity or official from sending to, or receiving from[redacted] ion Service information regarding the citizenship or immigration status, lawf[redacted]
(b) A[redacted] t entities
Notw[redacted] f Federal, State, or local law, no person or agency may prohibit, or in any way [redacted] government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.
(2) Maintaining such information.
(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."


DRAFT

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[4] (b) (5) [redacted]

(b) (5) [redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Microsoft Outlook

From: Vincent, Peter S
Sent: Monday, October 04, 2010 8:02 AM
To: Perry, Carl E; Ramlogan, Riah
Subject: RE: SC Memo

Carl:

Remind me: Did this memorandum (or a similar one) ever go to Beth last week?

Best regards,

Peter

Peter S. Vincent
Principal Legal Advisor
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
(b)(6), (b)

From: Perry, Carl E
Sent: Friday, October 01, 2010 1:31 PM
To: Vincent, Peter S; Ramlogan, Riah
Subject: SC Memo
Importance: High

Peter- (suggested that I paste this into the B'berry so you can read. I have read it once and think its good. I would like to furnish to Beth – along with the simple draft changes to SCAAP she aske (b)(6), to provide—along with the caveat that this is a draft neither you nor Riah have reviewed. Please let me know.

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)
Chief, Enforcement Law Section

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enforcement Law Section

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in the Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case-law, we conclude that participation in the Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Background

Secure Communities' Use of IDENT/IAFIS Interoperability [1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…." [2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS [3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).
4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an

agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5)

[redacted]

Discussion

The FBI's Authority To Share Fingerprint Submission Information with DHS Via IDENT/IAFIS Interoperability

It is unquestioned that the FBI may share fingerprint information with DHS. 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement

agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7] …[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a Compact for the organization of an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this Compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the Federal Government and to other ratifying States for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the Compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Case Law Supports a Position that Compelling Participation in Secure Communities in 2013 Does Not Violate the 10th Amendment

Although LEAs may argue that the Tenth Amendment prohibits ICE from compelling participation in Secure Communities, applicable case-law supports a position that Tenth Amendment protections are not

at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935.

The *Printz* court, however, also held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. Under this rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6. Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state

or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, as discussed *supra,* Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, if not sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the Federal Government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring States either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Last, please note that 8 U.S.C. §§ 1373[12] and 1644[13] do not support mandatory participation in Secure Communities. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Carl E. Perry
Director of Enforcement and Litigation
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
(b)(6), (b)(7)

---

[1]
"Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2]
Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3]
"CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

[4]
According to Secure Communities, the agencies discussed this issue at a September 21, 2010 meeting, but did not come to a resolution.

[5]
8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").
8 U.S.C. 1721, referred to above, provides, in relevant part:
(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6]
The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

[7]
Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8]
The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9]
See Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10]
Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

[11]
See FN 6, *supra.*

[12]
8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13]
8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[4] (b) (5) [redacted]

(b) (5) [redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-157 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)
Chief, Enforcement Law Section

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – Manda

Executive Summary

We present the arguments supporting a position that Secure Communities will be mandatory in 2013.

Background

Secure Communities' Use of ID

In Fiscal Year 2008, Congress appropri to "improve and modernize efforts to identify a sonment, and who may be deportable, and re re judged deportable…."[2] In response, ICE laun sform the way ICE identifies and removes crimi tive, Secure Communities utilizes existing te to share information, not only to a s, but also to share immigration status info gencies (LEAs). The Secure Communities "Pr ing and outreach support for ongoing efforts to a ictions nationwide. *See generally* Secure Co , Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20.

The f the full IDENT/IAFIS Interoperability process:

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE LESC.
4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to [redacted] to send to the originating LEA. The LESC also sends the IA[redacted]fice, which prioritizes enforcement actions based on leve[redacted]

There are two types of participation in Secure C[redacted] Interoperability is deployed. First, participation[redacted]-sharing in which the SIB and LEA receive the return m[redacted]erability process informing about the subject's immigrati[redacted] Second, a state or LEA may choose to participate but ele[redacted] the state may not have the technological ability to receiv[redacted]m CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability i[redacted]

According to Secure Communities, Ass[redacted]turella and the CJIS Director reached an agreem[redacted]013, all fingerprint requests from any LEAs tha[redacted] This future information sharing will not in[redacted]FIS Interoperability process where the SIB and [redacted]matic return message from ICE regarding the [redacted] status. According to Secure Communities, this proc[redacted] for policy reasons and to ensure adequate reso[redacted]ies have currently chosen to wait until 2013, whe[redacted]d, until instituting this process.

[redacted] Tasks In Order to Physically Deploy IDENT/IAFIS [redacted] LEA

Acc[redacted]ies, there are two ministerial-related IT tasks that, pursuant to curr[redacted]rformed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[redacted]CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

(b) (5)

Discussion

The FBI's Authority To Share Fingerprint Submissi Via IDENT/IAFIS Interoperability

It is unquestioned that the FBI may share fingerprint inform C. § 534 provides that the Attorney General shall "acquir fication, criminal identification, crime, and other records o provides for the sharing of the information, by change such records and information with, and for the e ne Federal Government. . . ." 28 U.S.C. § 534(a)(ide ICE access to criminal history record information co Crime Information Center files). Further, the applicable the Syste the FBI's Fingerprint Identification Records System (FIRS), FIS, provides that identification and criminal history reco and rap sheets) may be disclosed, in relevant part, to a federal engaged in criminal justice activity "where such disclosure the performance of a law enforcement functi vil law enforcement function; or where such disc the mutual law enforcement efforts of the law e Systems of Records, 64 Fed. Reg. 52343, 52348

The int information with DHS via IDENT/IAFIS Inte the establishment of an interoperable elec ediate access to information in databases of Fed nce community that is relevant to determine the of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[4] (b) (5)

[5] 8 U t part:
(2) R system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate [redacted] erated by the Department of Homeland Security (DHS) with t[redacted]tigation (FBI). The IDENT/IAFIS project was designed to su[redacted]d prosecution of criminal aliens and to pro[redacted]personnel with direct access to DHS data through [redacted]een the two systems, DHS would have the capa[redacted]nded person is subject to a currently posted W[redacted]'s Criminal Master File. Collaterally, the i[redacted] enable cognizant law enforcement agencies to [redacted]gration information as part of a criminal history respon[redacted]

H.R. Rep. No. 109-118 (2005). Congre[redacted]s not only crucial that DHS and the Department of Justice ens[redacted]ve, in real time, the existing biometric information contain[redacted]..[but] it is equally essential for the FBI, and St[redacted]ty to retrieve the proper level

---

(b) Report identifying [redacted]
(1) I[redacted]
Not [redacted]all submit to the appropriate committees of Congress a rep[redacted]ence community information needed by the Dep[redacted]igration and Naturalization Service to screen appl[redacted] those aliens inadmissible or deportable under the Imm[redacted]S.C.A. § 1101 *et seq.*]
(2) C[redacted]
(c) C[redacted]
(1) R[redacted]
Not [redacted]26, 2001, the President shall develop and implement a plan based on the findi[redacted]n (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a Compact for the organization of an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. See 42 U.S.C. § 14616. Under this Compact, the FBI and the ratifying states agree to maintain their respective criminal history records, including arrests and dispositions, and make them available to the Federal Government and to other ratifying States for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the Compact as of July 1, 2010.[9] For these twenty-nine states, participation in Secure Communities mandatory since they are already required to make their criminal history records available for immigration purposes.

Case Law Supports a Position that Compelling States to Participate in Secure Communities in 2013 Does Not Violate the 10th Amendment

Although LEAs may argue that the Tenth Amendment prohibits DHS from compelling participation in Secure Communities, a review of case law supports the position that Tenth Amendment protections are not at issue in Secure Communities. Courts have held that "[t]he Federal Government may not compel the States to enact or administer a federal regulatory program" through legislation or executive action, federal regulatory program. *New York v. United States*, 505 U.S. 144, 898, 925 (1997). Similarly, "[t]he Federal Government cannot circumvent this prohibition by conscripting the States to address particular problems, or by directing the States or their political subdivisions, to administer or enforce a federal regulatory program." *Id.* at 925. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of local jurisdictions to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Court held that these provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935.

The Supreme Court has also held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program."

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] For a complete listing of Compact states, please see http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

Id. at 918. Under this rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6. Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only [redacted] information and "does not require the state to do anything [redacted] already required, authorized, or provided by its own legislative com[redacted] *Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) [redacted] *Directors of Upper Chesapeake Health, Inc.*, 14[redacted] *see United States v. Keleher*, No. 1:07-cr-00332-O[redacted] Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challe[redacted] al law as in *Brown* that required a state to accept registrat[redacted] olding that, unlike the state officers in *Printz*, the feder[redacted] state officials, to do anything they do not already do [redacted] (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 335342[redacted] *eno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a fed[redacted] nsensual sale or release by a state of a driver's personal informa[redacted] Amendment, as the Act does not require the states in their sove[redacted] wn citizens, but regulates the states as the owners of da[redacted]

A court following [redacted] that an LEA's participation in Secure Commun[redacted] FIS Interoperability) does not violate the Tenth A[redacted] re Communities does not alte[redacted] the same provision of information to the FBI[redacted] ctice[11] or as required by state law. *See*, *e.g.*, Cal[redacted] de fingerprint submissions along with arrest data[redacted] ade). Therefore, unlike in *Printz* where the fede[redacted] ded duties, participation in Secure Com[redacted] ocal officials "to do anything they do not already do."

Des[redacted] challenger to Secure Communities may argue that the current task[redacted] prior to activating IDENT/IAFIS Interoperability extends part[redacted] nities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that

[11] *See* FN 6, *supra.*

certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, as discussed *supra,* Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, if not sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perfo g immigration law, but rather only involves the same sharing ral Government as currently practiced. *See New York v. Unite* -76 (1992) (holding a federal law violated the Tenth Amendme r to enact legislation providing for the disposal of radioac rs or to implement an administrative solution for taking

A challenger to Secure Communities may also a participation in Secure Communities violates th quire the State to expend significant funds in order to imp he *Printz* Court held that Congress cannot force state govern rden of implementing a federal regulatory program. *See Printz*, cording to Secure Communities, an SIB may need to pay es in order to have the capability to receive the return IAR me AFIS Interoperability process or relay that message to the LE

The above fiscal ar 010 and in 2013. First, participation in Sec r LEAs to receive the return IAR message. In f rmed LEAs that they may "opt-out" of receiv ey so choose or if the SIB does not have the tech relay that message to the LEA. Second, as per enturella and the CJIS Director for 2013, the fingerprint requests from any non-part of the current IDENT/IAFIS Interoperability proc receive the automatic return IAR message. Therefore, the 201 the state to expend any funds in order for IDENT/IAFIS Inte Last § 1373[12] and 1644[13] do not support mandatory participation in Sec *f New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Notw[illegible]f Federal, State, or local law, no person or agency may prohibit, or in any way [illegible]government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Atty work product

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable...."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following *is* a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

---

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With real time connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See, e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]...[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-157 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

---

[7] Similarly, Congress later reiterated "it is essential that... IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.*, Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See id.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program.**" *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.*, 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See, e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[redacted]

(b) (5) [redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-157 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)(C)
Chief, Enforcement and Removal Operations Law Division

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – "Opt

Executive Summary

We address the question of whether a law enfor f the Secure Communities Initiative. Although the ex in different contexts by Secure Communities, this the relevant interpretation whereby an LEA requests not to n the Secure Communities initiative.[1]

Background

Secure Con ty[2]

In Fiscal Year 200 to "improve and modernize efforts to identify a sonment, and who may be deportable, and rem e judged deportable…."[3] In resp nitiative to transform the way ICE identifies and s. In this initiative, Secure Communities utili NT and IAFIS to share information, not only to a s, but also to share immigration status info Secure Communities "Program Management Office" provides the ort for ongoing efforts to activate IDENT/IAFIS

[1] Sec y informed LEAs that they may "opt out" of receiving the return message from y process informing about the subject's immigration status if they so choose or if s not have the technological capability to receive that message or relay that message to the LEA.

[2] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[3] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The FBI's Authority to Share Fingerprint Submission Information with DHS and IDENT/IAFIS Interoperability Process

It is unquestioned that the FBI may share fingerprint information with DHS. 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use o[illegible]e Federal Government. . . ." 28 U.S.C. § 534(a)(4).

"IDENT/IAFIS Interoperability" is the technological mecha[illegible]tomates the sharing of the fingerprint submissions from [illegible]s from subjects booked into custody,[4] with DHS. The [illegible]T/IAFIS Interoperability process:

1. When a subject is arrested and booked i[illegible]e subject's fingerprints and associated bio[illegible] IAFIS via the appropriate State Identification [illegible]
2. CJIS[5] electronically routes the s[illegible]ic information to US-VISIT/IDENT to determine if th[illegible]ecords in its system.
3. As a result of a fingerprint matc[illegible]erates an Immigration Alien Query (IAQ) to the ICE L[illegible]
4. The LESC [illegible]bases to make an initial immigratio[illegible]ration Alien Response (IAR) to prioritize [illegible]
5. The LESC [illegible]ppropriate State SIB to send to the origi[illegible]ds the IAR to the local ICE field office, [illegible]d on level of offense.

[illegible]s Deploys IDENT/IAFIS Interoperability to

Bec[illegible]ty that is responsible for transmitting LEA's fingerprint sub[illegible]ommunities first enters into a voluntary Memorandum of Agr[illegible]ject SIB that either party may terminate at any time,[6] wherein

[4] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website).

[5] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

[6] *See* Section XIII of Template Secure Communities MOA with SIBs.

the SIB elects to participate in the Secure Communities initiative. Once the MOA is signed and any required technological enhancements are made to the SIB's computer-system to facilitate the SIB and LEA in receiving the return IAR message, Secure Communities engages in outreach at the local level before requesting the LEA to participate in the deployment of IDENT/IAFIS Interoperability to its jurisdiction.

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" that is attached to its fingerprint machine (*i.e*, a state or local official contacts CJIS to inform CJIS that the unique identifier pertains to the LEA's terminal). Once this validation occurs [redacted] FIS the LEA's "unique identifier" so that IAFIS will be informed to [redacted] NT that originate from the LEA.

(b) (5)

[redacted]

(b) (5)

(b) (5)

[redacted]

Further, according to Secure Communities, Assistant Director David Venturella and the CJIS Director met last week and reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that do not participate in Secure Communities.

This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until sharing information without state/local participation.

Discussion

[redacted]

(*Printz v. United* [redacted] milarly, "[t]he Federal Government may neither issue di[redacted] particular problems, nor command the States' o[redacted] visions, to administer or enforce a federal regulatory pro[redacted]

(b) (5)

[redacted] The *Printz* court explained "eve[redacted] costs[8] of implementing a federal program, they [redacted] for its burdensomeness and for its defects." *Id.* a[redacted] he *Printz* reasoning would recognize that certain jurisdictions do n[redacted] e immigration consequences of its constituents resulting from its p[redacted] munities. Moreover, although the currently-required LEA task to v[redacted] " may be very minor, and involve no local costs, the Supreme

[7] (b) (5) [redacted]

Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Id.* at 929-30.

Please note that 8 U.S.C. §§ 1373[9] and 1644[10] do not support mandatory participation in Secure Communities. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 a[redacted]ompel states or localities to require or prohibit anything. Rather, th[redacted] government entities or officials only from directly restrictin[redacted]of immigration information with the INS." *City of New York*, [redacted]added).

(b) (5)

[redacted]

[9] 8 U[redacted]

(a) I[redacted]

Notw[redacted]al law, a Federal, State or local government entity or offic[redacted]mental entity or official from sending to, or receiving from[redacted]ion Service information regarding the citizenship or immigration status, lawf[redacted]

(b) A[redacted]t entities

Notw[redacted]f Federal, State, or local law, no person or agency may prohibit, or in any way [redacted]government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[10] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

(b) (5) [redacted] The *Printz* court held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Printz*, 521 U.S. at 918.[11] Under the same rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federa[redacted]*wn*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. [redacted]urt explained that "because the individuals subject to the Act ar[redacted]ter pursuant to state registration laws, and because the Act only re[redacted] information than administer or enforce a federal [redacted] Tenth Amendment." *Id.* at * 6; *see Frielich v. Board [redacted]lth, Inc.*, 142 F.Supp.2d 679, 696-97 (D.Md. 2001) (upho[redacted]that "merely requires the state to forward informatio[redacted]already collects on its own under its own state laws," an[redacted]as never been held to violate the Tenth Amendment"); *aj*[redacted]*hesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002)(in aff[redacted]ederal law only requires the states to forward information).

(b) (5) [redacted]

[11] *See also Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)
Chief, Enforcement Law Section

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – Manda

Executive Summary

We present the arguments supporting a position that Secure Communities will be mandatory in 2013.

Background

Secure Communities' Use of ID

In Fiscal Year 2008, Congress appropri to "improve and modernize efforts to identify a sonment, and who may be deportable, and ren re judged deportable…."[2] In response, ICE laun sform the way ICE identifies and removes crimi tive, Secure Communities utilizes existing tec to share information, not only to a s, but also to share immigration status info gencies (LEAs). The Secure Communities "Pro ing and outreach support for ongoing efforts to a ictions nationwide. *See generally* Secure Cor Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20.

The f the full IDENT/IAFIS Interoperability process:

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE LESC.
4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to [redacted] to send to the originating LEA. The LESC also sends the IA[redacted]fice, which prioritizes enforcement actions based on leve[redacted]

There are two types of participation in Secure C[redacted] Interoperability is deployed. First, participation[redacted]-sharing in which the SIB and LEA receive the return m[redacted]erability process informing about the subject's immigrati[redacted] Second, a state or LEA may choose to participate but ele[redacted] the state may not have the technological ability to receiv[redacted]m CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability i[redacted]

According to Secure Communities, Ass[redacted]turella and the CJIS Director reached an agreem[redacted]013, all fingerprint requests from any LEAs tha[redacted] This future information sharing will not in[redacted]FIS Interoperability process where the SIB and [redacted]matic return message from ICE regarding the [redacted] status. According to Secure Communities, this proc[redacted] for policy reasons and to ensure adequate reso[redacted]ies have currently chosen to wait until 2013, whe[redacted]d, until instituting this process.

[redacted] Tasks In Order to Physically Deploy IDENT/IAFIS [redacted] LEA

Acc[redacted]ies, there are two ministerial-related IT tasks that, pursuant to curr[redacted]rformed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

(b) (5) [redacted]

Discussion

The FBI's Authority To Share Fingerprint Submissi[redacted]Via IDENT/IAFIS Interoperability

It is unquestioned that the FBI may share fingerprint inform[redacted]C. § 534 provides that the Attorney General shall "acquir[redacted]fication, criminal identification, crime, and other records[redacted]o provides for the sharing of the information, by r[redacted]change such records and information with, and for the [redacted]e Federal Government. . . ." 28 U.S.C. § 534(a)([redacted]ide ICE access to criminal history record information co[redacted]Crime Information Center files). Further, the applicable the Syste[redacted]the FBI's Fingerprint Identification Records System (FIRS), [redacted]FIS, provides that identification and criminal history reco[redacted]and rap sheets) may be disclosed, in relevant part, to a federal [redacted]engaged in criminal justice activity "where such disclosure [redacted]the performance of a law enforcement functi[redacted]vil law enforcement function; or where such disc[redacted]the mutual law enforcement efforts of the law e[redacted]Systems of Records, 64 Fed. Reg. 52343, 52348[redacted]

The [redacted]int information with DHS via IDENT/IAFIS Inte[redacted]he establishment of an interoperable elec[redacted]ediate access to information in databases of Fed[redacted]nce community that is relevant to determine the [redacted]y of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

---

[4] (b) (5) [redacted]

[5] 8 U[redacted]t part:

(2) R[redacted]system

Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive

Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate [illegible] erated by the Department of Homeland Security (DHS) with t[illegible]tigation (FBI). The IDENT/IAFIS project was designed to su[illegible]d prosecution of criminal aliens and to pro[illegible]personnel with direct access to DHS data through [illegible]een the two systems, DHS would have the capa[illegible]nded person is subject to a currently posted W[illegible]'s Criminal Master File. Collaterally, the i[illegible] enable cognizant law enforcement agencies to [illegible]gration information as part of a criminal history respon[illegible]

H.R. Rep. No. 109-118 (2005). Congre[illegible]s not only crucial that DHS and the Department of Justice ens[illegible]ve, in real time, the existing biometric information contain[illegible]..[but] it is equally essential for the FBI, and St[illegible]ty to retrieve the proper level

---

(b) Report identifying [illegible]
(1) I[illegible]
Not [illegible]all submit to the appropriate committees of Congress a rep[illegible]ence community information needed by the Dep[illegible]igration and Naturalization Service to screen appl[illegible] those aliens inadmissible or deportable under the Imm[illegible]S.C.A. § 1101 *et seq.*]
(2) C[illegible]
(c) C[illegible]
(1) R[illegible]
Not [illegible]26, 2001, the President shall develop and implement a plan based on the findi[illegible]n (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a Compact for the organization of an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. See 42 U.S.C. § 14616. Under this Compact, the FBI and the ratifying states agree to maintain their respective criminal history records, including arrests and dispositions, available to the Federal Government and to other ratifying States for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the Compact as of July 1, 2010.[9] For these twenty-nine states, participation in Secure Communities mandatory since they are already required to make their criminal history records available for immigration purposes.

Case Law Supports a Position that Compelling States to Participate in Secure Communities in 2013 Does Not Violate the 10th Amendment

Although LEAs may argue that the Tenth Amendment prohibits DHS from compelling participation in Secure Communities, as DHS has taken the position that Tenth Amendment protections are not at issue in Secure Communities because "[t]he Federal Government may not compel the States to enact legislation or executive action, federal regulatory programs." *New York*, 505 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may not commandeer the States to address particular problems or to govern their political subdivisions, to administer or enforce a federal regulatory program." *Id.* at 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of local jurisdictions to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Court held that these provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935.

The Court further held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program."

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] For a complete listing of Compact states, please see http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

Id. at 918. Under this rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6. Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only [redacted] information and "does not require the state to do anything [redacted] already required, authorized, or provided by its own legislative com[redacted] *Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) [redacted] *Directors of Upper Chesapeake Health, Inc.*, 14[redacted] *see United States v. Keleher*, No. 1:07-cr-00332-O[redacted] Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challe[redacted] al law as in *Brown* that required a state to accept registrat[redacted] olding that, unlike the state officers in *Printz*, the feder[redacted] state officials, to do anything they do not already do [redacted] (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 335342[redacted] *eno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a fed[redacted] nsensual sale or release by a state of a driver's personal informa[redacted] Amendment, as the Act does not require the states in their sove[redacted] wn citizens, but regulates the states as the owners of da[redacted]

A court following [redacted] that an LEA's participation in Secure Commun[redacted] FIS Interoperability) does not violate the Tenth A[redacted] re Communities does not alte[redacted] the same provision of information to the FBI[redacted] ctice[11] or as required by state law. *See*, *e.g.*, Cal[redacted] de fingerprint submissions along with arrest data[redacted] ade). Therefore, unlike in *Printz* where the fede[redacted] ded duties, participation in Secure Con[redacted] ocal officials "to do anything they do not already do."

Des[redacted] challenger to Secure Communities may argue that the current task[redacted] prior to activating IDENT/IAFIS Interoperability extends part[redacted] nities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that

[11] *See* FN 6, *supra.*

certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, as discussed *supra,* Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, if not sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perfo g immigration law, but rather only involves the same sharing ral Government as currently practiced. *See New York v. Unite* -76 (1992) (holding a federal law violated the Tenth Amendme r to enact legislation providing for the disposal of radioac rs or to implement an administrative solution for taking

A challenger to Secure Communities may also a participation in Secure Communities violates th quire the State to expend significant funds in order to imp he *Printz* Court held that Congress cannot force state govern rden of implementing a federal regulatory program. *See Printz*, cording to Secure Communities, an SIB may need to pay es in order to have the capability to receive the return IAR me AFIS Interoperability process or relay that message to the LE

The above fiscal ar 010 and in 2013. First, participation in Sec r LEAs to receive the return IAR message. In f rmed LEAs that they may "opt-out" of receiv ey so choose or if the SIB does not have the tech relay that message to the LEA. Second, as per enturella and the CJIS Director for 2013, the fingerprint requests from any non-part of the current IDENT/IAFIS Interoperability proc receive the automatic return IAR message. Therefore, the 201 the state to expend any funds in order for IDENT/IAFIS Inte

Last § 1373[12] and 1644[13] do not support mandatory participation in Sec *f New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Notw[illegible]f Federal, State, or local law, no person or agency may prohibit, or in any way [illegible] government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)(C)
Chief, Enforcement and Removal Operations Law Division

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – "Opt

Purpose

To provide the background by which a law enfo of the Secure Communities Initiative. Although the ex in different contexts by Secure Communities, this the relevant interpretation whereby an LEA requests not to h the Secure Communities initiative.[1]

Background

A. Sec perability[2]

In Fiscal Year 200 to "improve and modernize efforts to identify a sonment, and who may be deportable, and ren re judged deportable…."[3] In resp nitiative to transform the way ICE identifies and s. In this initiative, Secure Communities utili NT and IAFIS to share information, not only to a s, but also to share immigration status info Secure Communities "Program Management Office" provides the ort for ongoing efforts to activate IDENT/IAFIS

[1] Sec informed LEAs that they may "opt out" of receiving the return message from y process informing about the subject's immigration status if they so choose or if s not have the technological capability to receive that message or relay that message to the LEA.

[2] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[3] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

B. The FBI's Authority to Share Fingerprint Submission Information with DHS

It is unquestioned that the FBI may share fingerprint information with DHS. 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4). "IDENT [redacted] as described *infra*, is the technological mechanism by which th[redacted]ng of the fingerprint submissions from LEAs to IAFIS, including sub[redacted]ooked into custody,[4] with DHS.

C. IDENT/IAFIS Interoperability P[redacted]

The following is a description of the IDENT/IA[redacted]

1. When a subject is arrested and booked i[redacted]g LEA sends the subject's fingerprints and assoc[redacted] IAFIS via the appropriate State Identification [redacted]
2. CJIS[5] electronically routes the s[redacted]ic information to US-VISIT/IDENT to determine if th[redacted]ecords in its system.
3. As a result of a fingerprint matc[redacted]IS generates an Immigration Alien Quer[redacted]
4. The LESC [redacted]bases to make an initial immigratio[redacted]ration Alien Response (IAR) to prioritize[redacted]
5. The LESC [redacted]utes it to the appropriate State SIB to send [redacted]ds the IAR to the local ICE field office, [redacted]d on level of offense.

[redacted]munities Deploys IDENT/IAFIS [redacted]o an LEA

Bec[redacted]ty that is responsible for transmitting LEA's fingerprint sub[redacted]ommunities first enters into a voluntary Memorandum of Agr[redacted]ject SIB that either party may terminate at any time,[6] wherein

[4] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website).

[5] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

[6] *See* Section XIII of Template Secure Communities MOA with SIBs.

the SIB elects to participate in the Secure Communities' initiative. Once the MOA is signed and any required technological enhancements are made to the SIB's computer-system to facilitate the SIB and LEA in receiving the return IAR message, Secure Communities engages in outreach at the local level before requesting the LEA to participate in the deployment of IDENT/IAFIS Interoperability to its jurisdiction.

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to an LEA. The LEA must "validate" its "unique identifier" that is attached to its fingerprint machine (*i.e*, a state or local official contacts CJIS to inform CJIS that the unique identifier pertains to the LEA's terminal). Once this validation occurs [redacted] IAFIS the LEA's "unique identifier" so that IAFIS will be informed to [redacted] NT that originate from the LEA.

(b) (5)

[redacted]

(b) (5)

[redacted]

Further, according to Secure Communities, Assistant Director David Venturella and the CJIS Director met last week and reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that do not participate in Secure Communities.

This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until sharing information without state/local participation.

Discussion

(b) (5) [redacted]

The *Printz* court explained "eve[redacted] costs[8] of implementing a federal program, they [redacted] of taking the blame for its burdensomeness and for its defects." *Id.* a[redacted] oning, a court could cite *Printz* and recognize that certain juris[redacted] lamed for the immigration consequences of its constituents resu[redacted] n Secure Communities. Moreover, although the currently-requ[redacted] s "unique identifier" may be very minor, and involve no local

[7] (b) (5) [redacted]

costs, the Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Id.* at 929-30.

Please note that 8 U.S.C. §§ 1373[9] and 1644[10] do not support mandatory participation in Secure Communities. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 a[redacted]ompel states or localities to require or prohibit anything. Rather, th[redacted] government entities or officials only from directly restrictin[redacted]of immigration information with the INS." *City of New York*, [redacted]added).

(b)(5)

[redacted]

[9] 8 U[redacted]

(a) I[redacted]

Notw[redacted]al law, a Federal, State or local government entity or offic[redacted]mental entity or official from sending to, or receiving from[redacted]ion Service information regarding the citizenship or immigration status, lawf[redacted]

(b) A[redacted]t entities

Notw[redacted]f Federal, State, or local law, no person or agency may prohibit, or in any way [redacted]government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[10] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

(b) (5) [redacted] The *Printz* court held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Printz*, 521 U.S. at 918.[11] Under the same rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federa[redacted]*wn*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. [redacted]urt explained that "because the individuals subject to the Act ar[redacted]ter pursuant to state registration laws, and because the Act only re[redacted] information than administer or enforce a federal [redacted] Tenth Amendment." *Id.* at * 6; *see Frielich v. Board [redacted]lth, Inc.*, 142 F.Supp.2d 679, 696-97 (D.Md. 2001) (upho[redacted]that "merely requires the state to forward informatio[redacted]already collects on its own under its own state laws," an[redacted]as never been held to violate the Tenth Amendment"); *aff[redacted]hesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002)(in aff[redacted]ederal law only requires the states to forward information).

.

(b) (5) [redacted]

[11] *See also Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable...."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

---

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5)

[redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See, e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]...[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

---

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.*, Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See id.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.*, 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See, e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable...."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

---

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5)

[redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]...[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

---

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6); (b)(7)(C)
Chief, Enforcement Law Section

FROM: (b)(6); (b)(7)(C)
Associate Legal Advisor, Enforcement Law Section

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in the Secure Communities will be mandatory in 2013.

Background

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable...."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

---

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE LESC.
4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

(b) (5)

[redacted]

Discussion

The FBI's Authority To Share Fingerprint Submission Information with DHS Via IDENT/IAFIS Interoperability

It is unquestioned that the FBI may share fingerprint information with DHS. 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable the System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

(b) (5)

[redacted]

[5] 8 U.S.C. § 1722 provides, in relevant part:

(2) Requirement for interoperable data system

Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive

Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level

---

(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See, e.g.*, Cal. Penal Code § 13150.

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-57 (2009).

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a Compact for the organization of an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this Compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the Federal Government and to other ratifying States for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the Compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Case Law Supports a Position that Compelling Participation in Secure Communities in 2013 Does Not Violate the 10th Amendment

Although LEAs may argue that the Tenth Amendment prohibits ICE from compelling participation in Secure Communities, applicable case-law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* id. at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935.

The *Printz* court, however, also held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program."

---

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] For a complete listing of Compact states, please see http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

Id. at 918. Under this rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6. Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.*, 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See, e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that

[11] *See* FN 6, *supra.*

certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, as discussed *supra,* Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, if not sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the Federal Government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring States either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Last, please note that 8 U.S.C. §§ 1373[12] and 1644[13] do not support mandatory participation in Secure Communities. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)(C)
Chief, Enforcement and Removal Operations Law Division

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – "Opt

Purpose

To provide the background by which a law enfo of the Secure Communities Initiative. Although the ex in different contexts by Secure Communities, this the relevant interpretation whereby an LEA requests not to h the Secure Communities initiative.[1]

Background

A. Sec perability[2]

In Fiscal Year 200 to "improve and modernize efforts to identify a sonment, and who may be deportable, and rem re judged deportable…."[3] In resp nitiative to transform the way ICE identifies and s. In this initiative, Secure Communities utili NT and IAFIS to share information, not only to a s, but also to share immigration status info Secure Communities "Program Management Office" provides the ort for ongoing efforts to activate IDENT/IAFIS

[1] Sec y informed LEAs that they may "opt out" of receiving the return message from y process informing about the subject's immigration status if they so choose or if s not have the technological capability to receive that message or relay that message to the LEA.

[2] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[3] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

B. The FBI's Authority to Share Fingerprint Submission Information with DHS

It is unquestioned that the FBI may share fingerprint information with DHS. 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4). "IDENT [redacted] as described *infra*, is the technological mechanism by which th[redacted]ng of the fingerprint submissions from LEAs to IAFIS, including sub[redacted]ooked into custody,[4] with DHS.

C. IDENT/IAFIS Interoperability P[redacted]

The following is a description of the IDENT/IA[redacted]

1. When a subject is arrested and booked i[redacted]g LEA sends the subject's fingerprints and assoc[redacted] IAFIS via the appropriate State Identification [redacted]
2. CJIS[5] electronically routes the s[redacted]ic information to US-VISIT/IDENT to determine if th[redacted]ecords in its system.
3. As a result of a fingerprint matc[redacted]IS generates an Immigration Alien Quer[redacted]
4. The LESC [redacted]bases to make an initial immigratio[redacted]ration Alien Response (IAR) to prioritize[redacted]
5. The LESC [redacted]utes it to the appropriate State SIB to send [redacted]ds the IAR to the local ICE field office, [redacted]d on level of offense.

[redacted]munities Deploys IDENT/IAFIS [redacted]o an LEA

Bec[redacted]ty that is responsible for transmitting LEA's fingerprint sub[redacted]ommunities first enters into a voluntary Memorandum of Agr[redacted]ject SIB that either party may terminate at any time,[6] wherein

[4] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website).

[5] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

[6] *See* Section XIII of Template Secure Communities MOA with SIBs.

the SIB elects to participate in the Secure Communities' initiative. Once the MOA is signed and any required technological enhancements are made to the SIB's computer-system to facilitate the SIB and LEA in receiving the return IAR message, Secure Communities engages in outreach at the local level before requesting the LEA to participate in the deployment of IDENT/IAFIS Interoperability to its jurisdiction.

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to an LEA. The LEA must "validate" its "unique identifier" that is attached to its fingerprint machine (*i.e*, a state or local official contacts CJIS to inform CJIS that the unique identifier pertains to the LEA's terminal). Once this validation occurs [redacted] IAFIS the LEA's "unique identifier" so that IAFIS will be informed to [redacted] NT that originate from the LEA.

(b)(5)

[redacted]

(b)(5)

[redacted]

Further, according to Secure Communities, Assistant Director David Venturella and the CJIS Director met last week and reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that do not participate in Secure Communities.

This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until sharing information without state/local participation.

Discussion

(b) (5) [redacted]

Printz v. United [redacted] milarly, "[t]he Federal Government may neither issue di[redacted] particular problems, nor command the States' of[redacted] visions, to administer or enforce a federal regulatory pro[redacted]

(b) (5) [redacted]

The *Printz* court explained "eve[redacted] costs[8] of implementing a federal program, they [redacted] of taking the blame for its burdensomeness and for its defects." *Id.* a[redacted] oning, a court could cite *Printz* and recognize that certain juris[redacted] lamed for the immigration consequences of its constituents resu[redacted] n Secure Communities. Moreover, although the currently-requ[redacted] s "unique identifier" may be very minor, and involve no local

[7] (b) (5) [redacted]

costs, the Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Id.* at 929-30.

Please note that 8 U.S.C. §§ 1373[9] and 1644[10] do not support mandatory participation in Secure Communities. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 a[redacted]ompel states or localities to require or prohibit anything. Rather, th[redacted] government entities or officials only from directly restrictin[redacted]of immigration information with the INS." *City of New York*, [redacted]added).

(b)(5)

[redacted]

[9] 8 U[redacted]

(a) I[redacted]

Notw[redacted]al law, a Federal, State or local government entity or offic[redacted]mental entity or official from sending to, or receiving from[redacted]ion Service information regarding the citizenship or immigration status, lawf[redacted]

(b) A[redacted]t entities

Notw[redacted]f Federal, State, or local law, no person or agency may prohibit, or in any way [redacted]government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[10] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

(b) (5) [redacted] The *Printz* court held that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Printz*, 521 U.S. at 918.[11] Under the same rationale, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federa[redacted]*wn*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. [redacted]urt explained that "because the individuals subject to the Act ar[redacted]ter pursuant to state registration laws, and because the Act only re[redacted] information than administer or enforce a federa[redacted] Tenth Amendment." *Id.* at * 6; *see Frielich v. Board [redacted]lth, Inc.*, 142 F.Supp.2d 679, 696-97 (D.Md. 2001) (upho[redacted]that "merely requires the state to forward informatio[redacted]already collects on its own under its own state laws," ar[redacted]as never been held to violate the Tenth Amendment"); *aj*[redacted]*hesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002)(in aff[redacted]ederal law only requires the states to forward information).

.

(b) (5) [redacted]

[11] *See also Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

October 2, 2010

MEMORANDUM FOR: Beth N. Gibson
Assistant Deputy Director

FROM: Riah Ramlogan
Deputy Principal Legal Advisor

SUBJECT: Secure Communities – Mandatory in 2013

Executive Summary

We present the arguments supporting a position that participation in Secure Communities will be mandatory in 2013. Based on applicable statutory authority, legislative history, and case law, we conclude that participation in Secure Communities will be mandatory in 2013 without violating the Tenth Amendment.

Because the contemplated 2013 information-sharing technology change forms the factual basis for the legal analysis, we have included that background here. Readers familiar with the technology and the 2013 deployment may proceed directly to the Discussion section.

In the Discussion section, we review the three statutes from which the mandatory nature of the 2013 Secure Communities deployment derives: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials; 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Congressional history further underscores the argument that the 2013 Secure Communities deployment fulfills a Congressional mandate.

Our analysis of case law concentrates on *Printz v. United States*, 521 U.S. 898, 925 (1997), the seminal case on unconstitutional state participation in mandatory government programs. Significantly, *Printz* holds that that "federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program." *Id.* at 918. We examine several potential legal challenges and arguments that law enforcement agencies may make to avoid the reach of Secure Communities in 2013, and conclude that each seems rather weak in the face of *Printz* and its progeny.

Finally, we note that certain statutes relating to immigration information collected by states do not provide a legal basis for characterizing participation in Secure Communities in 2013 as mandatory, but as these are essentially irrelevant given other statutory support, we address them only briefly.

Background

A review of the Secure Communities information-sharing technology, which is admittedly complicated, aids the understanding of the applicable law and the corresponding conclusion that participation will become mandatory in 2013. The process by which fingerprint and other information is relayed will change in 2013 to create a more direct method for ICE to receive that information from DOJ. Consequently, choices available to law enforcement agencies who have thus far decided to decline or limit their participation in current information-sharing processes will be streamlined and aspects eliminated. In that way, the process, in essence, becomes "mandatory" in 2013, when the more direct method will be in place. The year 2013 was chosen by ICE and DOJ for policy and resource feasibility reasons.

Secure Communities' Use of IDENT/IAFIS Interoperability[1]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…."[2] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IAFIS to share information, not only to accomplish its goal of identifying criminal aliens, but also to share immigration status information with state and local law enforcement agencies (LEAs). The Secure Communities "Program Management Office" provides the planning and outreach support for ongoing efforts to activate IDENT/IAFIS Interoperability in jurisdictions nationwide. *See generally* Secure Communities: Quarterly Report, Fiscal Year Quarterly Report to Congress Third Quarter, at iv, 20. (Aug 11, 2010).

The following is a description of the full IDENT/IAFIS Interoperability process:

1. When a subject is arrested and booked into custody, the arresting LEA sends the subject's fingerprints and associated biographical information to IAFIS via the appropriate State Identification Bureau (SIB).
2. CJIS[3] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE Law Enforcement Support Center (LESC).

[1] "Interoperability" was previously defined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[2] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[3] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

There are two types of participation in Secure Communities by which IDENT/IAFIS Interoperability is deployed. First, participation may involve "full-cycle" information-sharing in which the SIB and LEA choose to participate and receive the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status (See Step 5, first sentence). Second, a state or LEA may choose to participate but elect not to receive the return message or the state may not have the technological ability to receive the return message from CJIS or relay the message to the LEA.

IDENT/IAFIS Interoperability in 2013

According to Secure Communities, Assistant Director David Venturella and the CJIS Director reached an agreement by which CJIS will send ICE, starting in 2013, all fingerprint requests from any LEAs that are not participating in Secure Communities. This future information sharing will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive (if technically feasible) the automatic return message from ICE regarding the subject's immigration status. According to Secure Communities, this process is technologically available now; however for policy reasons and to ensure adequate resources are in place, CJIS and Secure Communities have currently chosen to wait until 2013, when all planned deployments should be completed, until instituting this process.

Current CJIS-Required Tasks In Order to Physically Deploy IDENT/IAFIS Interoperability to an LEA

According to Secure Communities, there are two ministerial-related IT tasks that, pursuant to current CJIS policy, must be performed in order to physically deploy IDENT/IAFIS Interoperability to a LEA. The LEA must "validate" its "unique identifier" (called an "ORI") that is attached to its terminal (*i.e*, a state or local official contacts CJIS to inform CJIS that the ORI pertains to the LEA's terminal). Once this validation occurs, CJIS must note within IAFIS the LEA's ORI so that IAFIS will be informed to relay fingerprints to IDENT that originate from the LEA.

(b) (5) [redacted]

[4] (b) (5) [redacted]

(b) (5) [redacted]

Discussion

The FBI has Statutory Authority To Share Fingerprint Submission Information with DHS/ICE Via IDENT/IAFIS Interoperability, and this Authority Supports the Mandatory Nature of Anticipated 2013 Secure Communities Information-Sharing Deployment

It is unquestioned that the FBI has authority to share fingerprint information with DHS, and, therefore, ICE. This authority derives from three distinct statutes: 28 U.S.C § 534, relating to Attorney General sharing of criminal records with other government officials: 8 U.S.C. § 1722, which mandates a data-sharing system to enable intelligence and law enforcement agencies to determine the inadmissibility or deportability of an alien; and 42 U.S.C. §14616, which establishes an information-sharing compact between the federal government and ratifying states. Federal register notices and the legislative history of these provisions make plain that a system such as the 2013 Secure Communities deployment is mandatory in nature.

28 U.S.C. § 534

Specifically, 28 U.S.C. § 534 provides that the Attorney General shall "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." 28 U.S.C. § 534(a)(1). That law also provides for the sharing of the information, by requiring that the Attorney General "exchange such records and information with, and for the official use of, authorized officials of the Federal Government. . . ." 28 U.S.C. § 534(a)(4); *see* 8 U.S.C. § 1105 (FBI must provide ICE access to criminal history record information contained within National Crime Information Center files). Further, the applicable System of Records Notice for the FBI's Fingerprint Identification Records System (FIRS), which are maintained within IAFIS, provides that identification and criminal history record information (*i.e.*, fingerprints and rap sheets) may be disclosed, in relevant part, to a federal law enforcement agency directly engaged in criminal justice activity "where such disclosure may assist the recipient in the performance of a law enforcement function" or to a federal agency for "a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community." Notice of Modified Systems of Records, 64 Fed. Reg. 52343, 52348 (September 28, 1999).

8 U.S.C. § 1722

The FBI has further authority to share the fingerprint information with DHS via IDENT/IAFIS Interoperability. Specifically, Congress required the establishment of an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine the admissibility or deportability of an alien. *See* 8 U.S.C. § 1722.[5] IDENT/IAFIS

[5] 8 U.S.C. § 1722 provides, in relevant part:
(2) Requirement for interoperable data system
Upon the date of commencement of implementation of the plan required by section 1721(c), the President shall

Interoperability is the technological mechanism that was developed pursuant to this information-sharing requirement by which the FBI automates the sharing of current fingerprint submissions by LEAs to IAFIS[6] with DHS so that DHS may, in part, determine the admissibility or deportability of an alien based on the alien's criminal history.

From the early stages of the IDENT/IAFIS integration efforts, Congress fully intended that IDENT/IAFIS Interoperability involve both the sharing of information between the FBI and DHS, but also the sharing of the relevant immigration information between the federal agencies and state and local law enforcement. Specifically, Congress described the early IDENT/IAFIS integration project as follows:

> This project was established to integrate the separate identification systems operated by the Department of Homeland Security (DHS) with the Federal Bureau of Investigation (FBI). The IDENT/IAFIS project was designed to support the apprehension and prosecution of criminal aliens and to provide State and local law enforcement personnel with direct access to DHS data through IAFIS. With realtime connection between the two systems, DHS would have the capability to determine whether an apprehended person is subject to a currently posted Want/Warrant or has a record in the FBI's Criminal Master File. Collaterally, the integration of IDENT and IAFIS would enable cognizant law enforcement agencies to obtain all relevant immigration information as part of a criminal history response from a single FBI search.

---

develop and implement an interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the "Chimera system").

8 U.S.C. 1721, referred to above, provides, in relevant part:

(a) Interim directive
Until the plan required by subsection (c) of this section is implemented, Federal law enforcement agencies and the intelligence community shall, to the maximum extent practicable, share any information with the Department of State and the Immigration and Naturalization Service relevant to the admissibility and deportability of aliens, consistent with the plan described in subsection (c) of this section.
(b) Report identifying law enforcement and intelligence information
(1) In general
Not later than 120 days after May 14, 2002, the President shall submit to the appropriate committees of Congress a report identifying Federal law enforcement and the intelligence community information needed by the Department of State to screen visa applicants, or by the Immigration and Naturalization Service to screen applicants for admission to the United States, and to identify those aliens inadmissible or deportable under the Immigration and Nationality Act [8 U.S.C.A. § 1101 *et seq.*]
(2) Omitted
(c) Coordination plan
(1) Requirement for plan
Not later than one year after October 26, 2001, the President shall develop and implement a plan based on the findings of the report under subsection (b) of this section that requires Federal law enforcement agencies and the intelligence community to provide to the Department of State and the Immigration and Naturalization Service all information identified in that report as expeditiously as practicable.

[6] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website). State law, however, may require LEAs to send the fingerprints to IAFIS upon each arrest. *See*, *e.g.*, Cal. Penal Code § 13150.

H.R. Rep. No. 109-118 (2005). Congress similarly explained that it was not only crucial that DHS and the Department of Justice ensure that IDENT "is able to retrieve, in real time, the existing biometric information contained in the IAFIS database[7]…[but] it is equally essential for the FBI, and State and local law enforcement to have the ability to retrieve the proper level of information out of the IDENT/USVISIT database."[8] S. Rep. No. 108-280, at 15 (2004) (emphasis added). Because IDENT/IAFIS Interoperability accomplishes the Congressionally-intended information-sharing objectives, Congress has explicitly supported expansion of Secure Communities. *See* H.R. Rep. No. 111-157 (2009).

42 U.S.C. § 14616

42 U.S.C. §14616 also supports the mandatory nature of Secure Communities, at least for twenty-nine states. This statute establishes a compact for the organization of an electronic information sharing system among the federal government and the states to exchange criminal history records for non-criminal justice purposes authorized by Federal or State law, including immigration and naturalization matters. *See* 42 U.S.C. § 14616. Under this compact, the FBI and the ratifying states agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the federal government and to other ratifying states for authorized purposes. *See* 42 U.S.C. 14616(b). According to the FBI website, twenty-nine states have ratified the compact as of July 1, 2010.[9] For these twenty-nine states, a court may find participation in Secure Communities mandatory since they are already required by the above statute to make their criminal history records available for immigration matters.

Compelling Participation in Secure Communities in 2013 Does Not Raise Constitutional Concerns

Although LEAs may argue that the Tenth Amendment of the U.S. Constitution prohibits ICE from compelling participation in Secure Communities, applicable case law supports a position that Tenth Amendment protections are not at issue. Under the Tenth Amendment, "[t]he Federal Government may not compel the States to implement, by legislation or executive action, federal regulatory programs."[10] *Printz v. United States*, 521 U.S. 898, 925 (1997). Similarly, "[t]he Federal Government may neither issue directives requiring the States to

[7] Similarly, Congress later reiterated "it is essential that. . . IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT." H.R. Rep. No. 108-792 (2004).

[8] The Senate Committee for Appropriations further stated, with respect to early IDENT/IAFIS integration efforts, that "in order for Federal, State and local law enforcement agencies to effectively fight crime, they need to be able to access fingerprint records of visitors and immigration law violators." S. Rep. No. 108-344 (2004).

[9] *See* Compact Council, National Crime Prevention and Privacy Compact (2010), http://www.fbi.gov/hq/cjisd/web%20page/pdf/compact_history_pamphlet.pdf (containing a listing of Compact states).

[10] Both DHS and ICE officials have described Secure Communities as a "program." *See e.g.,* Fiscal 2011 Appropriations: Homeland Security, Committee on House Appropriations Subcommittee on Homeland Security (2010) (statement of ICE Director Morton) (thanking Subcommittee and the Committee for "providing vital resources to establish the Secure Communities program"); DHS Office of Inspector General, The Performance of 287(g) Agreements, at 82 (2010). Moreover, Secure Communities' staff is located in the "Program Management Office." Thus, ICE would likely not prevail in any argument that Secure Communities is not a federal "program."

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program." *Id. at* 935. In *Printz*, the Supreme Court found unconstitutional Brady Handgun Violence Prevention Act provisions requiring the chief law enforcement officer of each jurisdiction to conduct background checks on prospective handgun purchasers and to perform certain related ministerial tasks. *See* i*d.* at 933-34. The Supreme Court held that such provisions constituted the forced participation of the States' executive in the actual administration of a federal program. *See id.* at 935. Significantly, however, the *Printz* court also held that that "**federal laws which require only the provision of information to the Federal Government" do not raise the Tenth Amendment prohibition of "the forced participation of the States' executive in the actual administration of a federal program**." *Id.* at 918 (emphasis added).

Applying this holding, the United States District Court for the Southern District of New York found no Tenth Amendment issue in a federal act that required "state officials to provide information regarding sexual offenders-information that the state officials will typically already have through their own state registries-to the federal government." *U.S. v. Brown*, No. 07-Cr. 485(HB), 2007 WL 4372829, at * 5 (S.D.N.Y. Dec. 12, 2007). The District Court explained that "because the individuals subject to the Act are already required to register pursuant to state registration laws, and because the Act only requires states to provide information rather than administer or enforce a federal program, the Act does not violate the Tenth Amendment." *Id.* at * 6.

Similarly, the United States Court of Appeals for the Fourth Circuit upheld a District Court's conclusion that a federal reporting requirement does not violate the Tenth Amendment because the federal law only requires the state to forward information and "does not require the state to do anything that the state itself has not already required, authorized, or provided by its own legislative command." *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002) (citing *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.,* 142 F.Supp.2d 679, 696 (D.Md. 2001)); *see United States v. Keleher*, No. 1:07-cr-00332-OWW, 2008 WL 5054116, at * 12 (E.D.Cal. Nov. 19, 2008) (rejecting a Tenth Amendment challenge to the provisions of the same federal law as in *Brown* that required a state to accept registration information from a sex offender, holding that, unlike the state officers in *Printz*, the federal law "does not require states, or their state officials, to do anything they do not already do under their own laws.") (citing *United States v. Pitts*, No. 07-157-A, 2007 WL 3353423 (M.D.La. Nov. 7, 2007)); *cf. Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

A court following the above reasoning would similarly recognize that an LEA's participation in Secure Communities (*i.e.* accepting deployment of IDENT/IAFIS Interoperability) does not violate the Tenth Amendment. Specifically, participation in Secure Communities does not alter the normal booking process and only requires the same provision of information to the FBI that the LEAs currently provide as regular practice[11] or as required by state law. *See*, *e.g.*, Cal. Penal Code § 13150 (requiring LEAs to provide fingerprint submissions along with arrest data to the Department of Justice for each arrest made). Therefore, unlike in *Printz* where the

[11] *See* FN 6, *supra.*

federal law forced the state officials to perform added duties, participation in Secure Communities does not require local officials "to do anything they do not already do."

Despite the above reasoning, a challenger to Secure Communities may argue that the current task to validate the LEA's ORI prior to activating IDENT/IAFIS Interoperability extends participation in Secure Communities beyond mere information-sharing and constitutes the same prohibited conscription of state or local officials as in *Printz*. The Supreme Court in *Printz* held that Congress cannot force state officials to even perform "discrete, ministerial tasks" to implement a federal regulatory program. *Printz*, 521 U.S. at 929-30. The *Printz* court explained "even when the States are not forced to absorb the costs of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following this *Printz* reasoning could recognize that certain jurisdictions do not want to be blamed for the immigration consequences of its constituents resulting from its participation in Secure Communities.

ICE has several defenses to the above claim. First, Secure Communities, CJIS, and US-VISIT are currently discussing the necessity of this ministerial requirement; therefore, it is possible that this additional pre-activation requirement may not exist by 2013, and may be eliminated sooner. Second, state and local officials already validate the ORIs bi-annually with the FBI; therefore, like in *Frielich*, *Keleher*, and *Pitts*, this validation task does not force state and local officials "to do anything they do not already do." Last, ICE may argue that, despite this ministerial task, participation in Secure Communities does not compel state or local officials to enact a legislative program, administer regulations, or perform any functions enforcing immigration law, but rather only involves the same sharing of information to the federal government as currently practiced. *See New York v. United States*, 505 U.S. 144, 175-76 (1992) (holding a federal law violated the Tenth Amendment by requiring states either to enact legislation providing for the disposal of radioactive waste generated within their borders or to implement an administrative solution for taking title to, and possession of, the waste).

A challenger to Secure Communities may also argue, in reliance on *Printz*, that 2013 participation in Secure Communities violates the Tenth Amendment because it may require the State to expend significant funds in order to implement the program. The *Printz* Court held that Congress cannot force state governments to absorb the financial burden of implementing a federal regulatory program. *See Printz*, 518 U.S. at 930. Currently, according to Secure Communities, an SIB may need to pay for its own technological upgrades in order to have the capability to receive the return IAR message from CJIS in the IDENT/IAFIS Interoperability process or relay that message to the LEA.

The above fiscal argument is misleading and should fail both in 2010 and in 2013. First, participation in Secure Communities does not require the states or LEAs to receive the return IAR message. In fact, Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return IAR message if they so choose or if the SIB does not have the technological capability to receive that message or relay that message to the LEA. Second, as per the aforementioned agreement between Mr. Venturella and the CJIS Director for 2013, the 2013 process by which CJIS will send ICE all fingerprint requests from any non-participating LEA will not include the component of the current IDENT/IAFIS Interoperability process where the SIB and LEA receive the automatic return IAR message. Therefore, the 2013 process would not require the state to expend any funds in order for IDENT/IAFIS Interoperability to be deployed.

Certain Statutes Relation to the Sharing of Immigration Information Do Not Lend Support to the Argument that Secure Communities Will Become Mandatory in 2013

Last, please note that 8 U.S.C. §§ 1373[12] and 1644,[13] which relate to voluntary sharing of immigration information by government employees, do not support mandatory participation in Secure Communities, but lack of support by these statutes is essentially irrelevant because statutory support exists elsewhere. We include them because the notoriety of the legal cases associated with these statutes has potential to become a "red herring" in discussions about the mandatory nature of Secure Communities participation. In *City of New York v. United States*, 179 F.3d 29 (2d Cir. 1999), the Mayor of New York City issued a 1989 order prohibiting city employees from voluntarily sending immigration status information about an individual to the immigration authorities. Following passage of IIRIRA and PRWORA in 1996, the City brought suit against the federal government, claiming, in relevant part, that 8 U.S.C. § 1373 and 8 U.S.C. § 1644 violated the Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35.

Conclusion

Based on applicable statutory authority, legislative history, and case law, we conclude that there is ample support for the argument that participation in Secure Communities will be mandatory in 2013, and that the procedures by which state and local information will be shared with ICE at that time does not create legitimate Tenth Amendment concerns of unconstitutional compulsion by states in a mandatory federal program.

---

[12] 8 U.S.C. § 1373 provides, in relevant part:

(a) In general

Notwithstanding any other provision of Federal, State or local law, a Federal, State or local government entity or official may not prohibit, or in any way restrict, any governmental entity or official from sending to, or receiving from, the Immigration and Naturalization Service information regarding the citizenship or immigration status, lawful or unlawful, of any individual.

(b) Additional authority of government entities

Notwithstanding any other provision of Federal, State, or local law, no person or agency may prohibit, or in any way restrict, a Federal, State, or local government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.

(2) Maintaining such information.

(3) Exchanging such information with any other Federal, State, or local governmental entity.

[13] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Office of the Principal Legal Advisor

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20024

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: Peter S. Vincent
Principal Legal Advisor

THROUGH: (b)(6), (b)(7)(C)
Chief, Enforcement and Removal Operations Law Division

FROM: (b)(6), (b)(7)(C)
Associate Legal Advisor, Enf

SUBJECT: Secure Communities – Manda

Executive Summary

We address the question of whether participatio will be mandatory in 2013 or whether a law enforceme ugh the expression "opt out" has been interpreted in dif e Communities, this memorandum addresses the relevant interpretat quests not to participate at any level in the Secure Communities

DRAFT

[1] Secure Communities has consistently informed LEAs that they may "opt out" of receiving the return message from the IDENT/IAFIS Interoperability process informing about the subject's immigration status if they so choose or if the State Information Bureau does not have the technological capability to receive that message or relay that message to the LEA.

Background

Secure Communities' Use of IDENT/IAFIS Interoperability[2]

In Fiscal Year 2008, Congress appropriated $200 million for ICE to "improve and modernize efforts to identify aliens convicted of a crime, sentenced to imprisonment, and who may be deportable, and remove them from the United States, once they are judged deportable…."[3] In response, ICE launched the Secure Communities initiative to transform the way ICE identifies and removes criminal aliens from the United States. In this initiative, Secure Communities utilizes existing technology, *i.e.* the ability of IDENT and IA [redacted] not only to accomplish its goal of identifying criminal aliens, but als[redacted]us information with LEAs. The Secure Communities "Progra[redacted]ovides the planning and outreach support for ongoing efforts to act[redacted] Interoperability in jurisdictions nationwide. *See* [redacted]terly Report, Fiscal Year Quarterly Report to Congre[redacted]010).

The FBI's Authority to Share Fingerpri[redacted]nd IDENT/IAFIS Interoperability Process

It is unquestioned that the FBI may sha[redacted]DHS. 28 U.S.C. § 534 provides that the Attorney General shal[redacted]preserve identification, criminal identification, crime, and othe[redacted]. That law also provides for the sharing of the informat[redacted]ey General "exchange such records and information with, and [redacted]horized officials of the Federal Governme[redacted]

"IDENT/IAFIS Int[redacted]by which the FBI automates the sharing of the f[redacted]ncluding submissions from subjects booked in[redacted]owing is a description of the IDENT/IAFIS Inte[redacted]

[redacted] custody, the arresting LEA sends the [redacted]phical information to IAFIS via the [redacted]ification Bureau (SIB).

[2] "Int[redacted]ined as the "sharing of alien immigration history, criminal history, and terrorist information based on positive identification and the interoperable capabilities of IDENT and IAFIS." DHS IDENT/IAFIS Interoperability Report, at p. 2 (May, 2005). Currently, Secure Communities officially refers to the process as "IDENT/IAFIS Interoperability."

[3] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, 121 Stat 1844, 2050 (2007).

[4] The States, whose record repositories are the primary source of criminal history records maintained at the FBI, are not required to provide fingerprint information to the FBI, but do so voluntarily in order to gain the mutual benefit of receiving access to criminal history information on individuals who have resided in other States. *See* Privacy Impact Assessment for the Federal Bureau of Investigation Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling (May 5, 2008) (available on FBI's website).

2. CJIS[5] electronically routes the subject's biometric and biographic information to US-VISIT/IDENT to determine if there is a fingerprint match with records in its system.
3. As a result of a fingerprint match with data in IDENT, CJIS generates an Immigration Alien Query (IAQ) to the ICE LESC.
4. The LESC queries law enforcement and immigration databases to make an initial immigration status determination and generates an Immigration Alien Response (IAR) to prioritize enforcement actions.
5. The LESC sends the IAR to CJIS, which routes it to the appropriate State SIB to send to the originating LEA. The LESC also sends the IAR to the local ICE field office, which prioritizes enforcement actions based on level of offense.

The Process By Which Secure Communities Deploys [redacted] bility to an LEA

Because the SIB is the state entity that is respon[redacted]nt submissions to IAFIS, Secure Communities firs[redacted] of Agreement (MOA) with the subject SIB that eit[redacted] wherein the SIB elects to participate in the Secure Comm[redacted]gned and any required technological enhancements are m[redacted]acilitate the SIB and LEA in receiving the return IAR m[redacted]nities engages in outreach at the local level before reques[redacted]e deployment of IDENT/IAFIS Interoperability to its ju[redacted]

According to Secure Communities, the[redacted] tasks that, pursuant to CJIS policy, must be performed in orde[redacted]NT/IAFIS Interoperability to a LEA. The LEA [redacted]ttached to its fingerprint machine (*i.e*, a stat[redacted] that the unique identifier pertains to the LEA[redacted] must note within IAFIS the LEA's "unique ide[redacted] fingerprints to IDENT that originate from the [redacted]

(b) (5)

[redacted]

[redacted]

[redacted]

[5] "CJIS," which stands for the FBI's Criminal Justice Information Services Division, manages IAFIS.

[6] *See* Section XIII of Template Secure Communities MOA with SIBs.

(b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]

Further, according to Secure Communities, Ass[redacted]e CJIS Director met last week and reached an agreeme[redacted]g in 2013, all fingerprint requests from any LEAs th[redacted]ecure Communities. This future information sharing will not [redacted]urrent IDENT/IAFIS Interoperability process where the SIB [redacted] feasible) the automatic return message from ICE regarding the [redacted]ccording to Secure Communities, this process is technolog[redacted]r policy reasons and to ensure adequate resources are in place, [redacted]nities have currently chosen to wait until 2013, wh[redacted]ted, until sharing information without state/local [redacted]

Discussion

(b) (5) [redacted]

Printz v. United States, 521 U.S. 898, 925 (1997).[7] Similarly, "[t][redacted] neither issue directives requiring the States to address part[redacted]nd the States' officers, or those of their political subdivisions, to a[redacted]al regulatory program." *Id. at* 935.

(b) (5) [redacted]

[7] (b) (5) [redacted]

(b) (5) [redacted]

The *Printz* court explained "even when the States are not forced to absorb the costs[8] of implementing a federal program, they are still put in the position of taking the blame for its burdensomeness and for its defects." *Id.* at 930. A court following the *Printz* reasoning would recognize that certain jurisdictions do not want to be blamed for the immigration consequences [redacted] g from its participation in Secure Communities. Moreover, althoug [redacted] EA task to validate its "unique identifier" may be very minor, and in [redacted] upreme Court in *Printz* held that Congress cannot force state officia [redacted] e, ministerial tasks" to implement a federal regula [redacted]

Please note that 8 U.S.C. §§ 1373[9] and 1644[10] [redacted] in Secure Communities. In *City of New York v. U* [redacted] 9), the Mayor of New York City issued a 1989 order p [redacted] arily sending immigration status information about a [redacted] gration authorities. Following passage of IIRIRA and PRW [redacted] suit against the federal government, claiming, in relevant part, [redacted] C. § 1644 violated the

[8] (b) (5) [redacted]

[9] 8 U [redacted]
(a) I [redacted]
Notw [redacted] al law, a Federal, State or local government entity or offic [redacted] mental entity or official from sending to, or receiving from [redacted] ion Service information regarding the citizenship or immigration status, lawf [redacted]
(b) A [redacted] t entities
Notw [redacted] f Federal, State, or local law, no person or agency may prohibit, or in any way [redacted] government entity from doing any of the following with respect to information regarding the immigration status, lawful or unlawful, of any individual:

(1) Sending such information to, or requesting or receiving such information from, the Immigration and Naturalization Service.
(2) Maintaining such information.
(3) Exchanging such information with any other Federal, State, or local governmental entity.

[10] 8 U.S.C. § 1644 provides "Notwithstanding any other provision of Federal, State, or local law, no State or local government entity may be prohibited, or in any way restricted, from sending to or receiving from the Immigration and Naturalization Service information regarding the immigration status, lawful or unlawful, of an alien in the United States."

Tenth Amendment by directly compelling states to enact and enforce a federal regulatory program. The Second Circuit held that 8 U.S.C. § § 1373 and 1644 "do not directly compel states or localities to require or prohibit anything. Rather, they prohibit state and local government entities or officials only from directly restricting the voluntary exchange of immigration information with the INS." *City of New York*, 179 F. 3d at 35 (emphasis added).

(b) (5)

[redacted]

(b) (5)

[redacted] The *Printz* court held that that "federal laws which require on[redacted]o the Federal Government" do not raise the Tenth Ar[redacted]the forced participation of the States' executive in[redacted]." *Printz*, 521 U.S. at 918.[11] Under the same rat[redacted] Southern District of New York found no Ten[redacted]red "state officials to provide information regard[redacted] officials will typically already have throu[redacted]he federal government." *U.S. v. Brown*, No. 07-[redacted].Y. Dec. 12, 2007). The District Court exp[redacted]he Act are already required to register purs[redacted] Act only requires states to provide info[redacted]ogram, the Act does not violate the Tenth Am[redacted] *Frielich v. Board of Directors of Upper Chesapeake Health, Inc.*, 142[redacted]Md. 2001) (upholding a federal reporting requirement that "me[redacted]ward information to a national data bank that the state already coll[redacted]n state laws," and observing that such a requirement "has never bee[redacted]mendment"); *aff'd*, *Frielich v Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214 (4th Cir. 2002)(in affirming, noting that the subject federal law only requires the states to forward information).

[11] *See also Reno v. Condon*, 528 U.S. 141, 150-51 (2000) (holding a federal act which restricts the nonconsensual sale or release by a state of a driver's personal information does not violate the Tenth Amendment, as the Act does not require the states in their sovereign capacity to regulate their own citizens, but regulates the states as the owners of databases).

(b) (5)

[redacted]