*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."