April 12, 2011

Mr. Marc Rapp
Acting Assistant Director
Secure Communities Program Management Office
Immigration & Customs Enforcement
5th Floor, 500 12th Street, SW
Washington, DC 20036

Marc,

It has taken me several days to regain my equilibrium after the abrupt termination of my contract with Secure Communities (SC) in the late afternoon of Friday, March 25 and the subsequent New York Times article on the following Sunday.

When the contract project leader and his deputy called to give me the news at about 330 pm on that Friday, they told me [redacted] wanted them to relay the message that it was "nothing personal, we still love you; it's just business."

I appreciate the sentiment, but what happened *was* personal and it was intended to be so -- DHS and ICE chose to play hardball with my job and my reputation because they felt politically exposed and embarrassed by the questions that arose about Rahm Emmanuel's involvement (or lack thereof) in attempting to persuade Chicago and Cook County to participate in interoperability. They wanted to distance themselves from me. The clear implication made by Brian Hale on behalf of the government in the article was that I was some kind of rogue contractor. That is far from the truth, as you well know.

I've given some thought to all that has happened, and am unwilling to leave that impression uncorrected. For much of the time that I was employed under subcontract, I was not in fact a regional coordinator; I will speak to my accomplishments as a regional coordinator later. But regarding my role as the contract employee who drafted certain documents which later became controversial as the result of release in response to a Freedom of Information Act (FOIA) suit, here are the facts.

1. <u>Pre-Coordinator Contract Work, Secure Communities.</u>

My contract work with Secure Communities began in late December 2008, as a subject matter expert providing advice to contract staff on ICE matters as they related to Secure Communities. During the preliminary months, I assisted them with generally becoming knowledgeable on removals, detention, the interface of immigration enforcement with the criminal justice system, etc., so that they could better serve you, their client. In addition, I drafted a number of white papers on matters that I believed would have an impact on the long-term success of SC: at-large criminal aliens; illegal aliens who would be no-matches in the IDENT system, etc.

Opting Out. In August of 2009, I was asked by [redacted] (Deployment Team contract manager) and [redacted] (then a regional coordinator but also my subcontract boss) to look into the issue of whether a jurisdiction could opt out. Pursuant to their request, I drafted and submitted a white paper indicating my belief that, as a legal proposition, they could not. That paper was provided to other members of SC, both government and contract, as the issue had become volatile in light of events in San Francisco and in Chicago / Cook County ***[Exhibit "A"].*** I was later advised that the recommendations and views it contained would not be adopted, because ICE had already provided a formal response to a Congressional Question for the Record (QFR) prepared by then-SC Chief of Staff Rachel Canty, indicating that participation was voluntary ***[Exhibit"B"].***[1]

As an outcome of that meeting , however, I was asked to prepare for you alternative recommendations as to how to address the question of opting out in politically sensitive locations. In September 2009, I prepared a generic document to that effect, suggesting that a possible reconciliation existed between the QFR and the need to preclude a jurisdiction from opting out: that reconciliation was to adopt the stance that "opting out" did not mean refusing to participate in interoperability; it meant only that an LEA could choose not to receive the IDENT "second message" via the SIB ***[Exhibit "C"].***[2] That same month I traveled to ICE HQ and met with you and the contract project manager. During the meeting I again stated my belief that the law was on the federal government's side, and that jurisdictions could be prevented from opting out. You indicated that view was not on the table. I then presented my alternative

[1] It seems clear, at least to me, that the primary reason ICE was unwilling to "walk back" this response was political in nature (like so much that has afflicted this program): it had been made to David Price, then-Chairman of a powerful Congressional committee with DHS oversight responsibilities. Of course, with the change of majority parties in the House and Mr. Price's replacement as chairman, at least some of those political considerations have changed, as is evident by what followed. See the next paragraph in the body of this paper.

[2] I have provided only a few exhibits as attachments (which nonetheless have made it lengthy). However everything I assert is documented as a part of the comprehensive response I provided to the FOIA Office search request of some months ago. They can be found on the SC Sharepoint site / FOIA subsection. Parenthetically, although my knowledge is imperfect, I will admit to being puzzled as to which items of mine the FOIA Office elected to provide versus those they withheld; and, additionally, to the fact that some were provided in a redacted fashion that makes the author unclear, whereas in other instances, ICE has chosen to identify me as the author. In some articles, journalists quote redacted emails and documents of mine in which I am not identified, against documents in which I am identified, as if to illustrate how in error I was. This would be downright amusing, if the subject matter were not so serious. The difference of course is between positions I took internally when providing my views, and those I put forward for the program consistent with its public posture. But a cynic might conclude that the intent was to deliberately obfuscate what positions I took, when, and for what purpose. For instance, nowhere do I find myself credited for suggesting that "opting out" might be construed only to mean not receiving a second message. The only things ICE is apparently willing to credit to me at this point are those which they wish to use to imply I was a rogue without adequate supervision.

suggestion that ICE adopt a narrow definition of opting out. That too was rejected.[3] I left the meeting with a request to prepare site-specific mitigation strategies for the following specific locations:

- San Francisco
- Chicago
- New York City

Faced with rejection of my initial two suggestions – first, to exercise the prerogatives of the law; or, second, to narrowly construe the meaning of "opting out," I was left with only one possibility that I could see, to offer political solutions to what were fundamentally political problems posed by the elected leaders in the jurisdictions mentioned above. In the end, though, I took two tacks in the documents which I submitted to the government: on the strategic level, I suggested that ICE and DHS acknowledge the fundamental problem as being political in nature, and ask select members of the Administration or Congress to meet with local political leaders who appeared to be spearheading the impediments to activation in order to arrive at resolution; on the tactical level, I suggested that SC move forward aggressively with activation in the states where these jurisdictions existed so that the effects of their non-participation could be mitigated and perhaps overcome.

In the following months, I prepared several draft versions which went back-and-forth among contract and government staff for review and consideration. I provided my final-drafts through the SC contract project managers in December 2009. When it appeared that these products had not reached the client, I retransmitted them directly to government staff in late January / early February 2010.

The final drafts were clearly endorsed by me as both "Draft" and "Pre-Decisional-Deliberative / FOIA Exempt." I did this because, contrary to the depiction of me as a rogue or out-of-control, I recognized the sensitivity of the materials, and the fact that the final decisions were not mine or any contractor's to make – they were solely and entirely in the purview of the government to make, and that because the documents were not final, they needed to be debated and deliberated with the freedom of expression they deserved.

Once they reached your good offices, I cannot say what happened, or whether they in fact ever received consideration, dialogue or debate as to the strategic political suggestions. I know that the tactical recommendations were adopted, because as a regional coordinator, I participated in putting them into play.

I still cannot for the life of me determine why – somewhere between a year and fifteen months after they had been prepared and submitted as draft documents – the ICE FOIA Office decided

[3] It is ironic that this alternative has since become the public stance of ICE and DHS, both having realized that no other proposition would further their interest in ensuring implementation of interoperability, but recognizing too late that they were boxed in by the previously-submitted QFR.

that they did not merit protection from disclosure, given the chilling effect that such a disclosure would (and did) have. If government officers do not feel the freedom to explore all options in an atmosphere of open dialogue, then their decisions will inevitably be made not on the basis of what is best, but only what is expedient or safe for their careers. But we are clearly well past that point to the detriment, I think, of your program.

Now I wish to speak for a moment to my work as a contract regional coordinator.

2. <u>Regional Coordinator, Secure Communities.</u>

When in late March / early April of 2010 [redacted], one of the four regional coordinators, provided notice that he intended to take another position, I was approached by [redacted] on behalf of the contractor and the government, and asked if I would step into his role. I agreed. A few weeks later [redacted], another coordinator, served notice of his departure and I was asked to additionally take on [redacted]'s area of control. I expressed concern over the geographic span but was assured that if I found it burdensome, the work would be redistributed.

At that point I found myself responsible for 30 of the 50 states, plus Puerto Rico and the U.S. Virgin Islands – *more than double the area of control of the remaining two coordinators combined*. What is more, I assumed responsibility for many troubling (not to say troublesome) states, including Illinois, Massachusetts, Pennsylvania and New York.

In late September I received modest relief from the burden of my load: at that point, [redacted] agreed to take responsibility for the New Orleans Field Office AOR, thus reducing my responsibility from 30 states, down to 25 plus P.R. and U.S.V.I., still double that of the other two regional coordinators. It was only in mid-January of 2011, after 10 months of extraordinary work and efforts, when [redacted] was hired as a fourth contract regional coordinator, that my workload was reduced to normal.

During the many months I carried a double workload I did not complain, but stepped into the task determined to try and make a difference on behalf of the program, and over the course of time I believe that I did. Here are some of my accomplishments:

<u>State Signatures on Memoranda of Agreement</u>. By way of example, I personally negotiated with the state identification bureaus of three states which had previously steadfastly declined to sign the Memorandum of Agreement -- Indiana, Kansas and Wisconsin[4] -- and did ultimately obtain their signatures on the MOA. I was successful through perseverance, a substantial investment of time, and a willingness to listen to and work through their questions, difficulties and objections. All during these discussions and negotiations, I don't recall anyone from the government or the contract team expressing concern that I was overstepping my bounds. But those weren't my only achievements.

[4] The MOA with Rhode Island was also signed during my tenure as regional coordinator, but I cannot in good conscience, and do not, claim credit for that success as it belongs to Mr. Archibeque and others.

Statewide Activations. During my tenure as a regional coordinator *carrying a double load*, I also accomplished several statewide activations: West Virginia, Wisconsin, and Rhode Island. What is more, I was the individual who wrote the plans which Secure Communities adopted, and the other regional (and field) coordinators used, to achieve statewide activations in Texas and North Carolina.

Politically Sensitive States. All while I was undertaking the above tasks, I was also working as best I could on behalf of the government and the contractor to try to keep forward momentum in difficult states, primarily but not exclusively Illinois and New York.

New York: In New York, as you will recall, after signing of the MOA in May 2010, the state came under pressure from special interest groups to withdraw. By July, former Governor Patterson was giving this serious consideration. I know this because one afternoon (ironically, while I was on travel in Illinois doing law enforcement outreaches) I received a panic call from Joe Morrissey, Deputy Commissioner of New York DCJS. Joe told me he had made several unreturned telephone calls to you, to Vince Archibeque, to Randi Greenberg and others at SC. He had wanted to impart the news that there was to be a meeting between his boss, the Governor, and other senior officials to discuss the MOA – they (he and Sean Byrne, his boss the Commissioner) were concerned that, absent something in writing they could carry to the governor documenting previous verbal assurances SC leaders had made to them that no jurisdiction in New York would be activated absent the approval of the involved LEAs, the Governor would in fact terminate the MOA.

It was that circumstance which led me to send Joe the email which Byrne later provided in un-redacted form to NGOs and the media that got quoted in the New York Times months later. Unfortunately, by the time the email was made public, SC, ICE and the Department had started to shift their stance on what participation in SC meant, and so I drew heat then because of the release, even though what I articulated to the state in the email was perfectly accurate and reflective of the status quo. I am convinced that the email saved for SC New York State's participation in interoperability; that is why the only thing that the state ultimately demanded was a minor, face-saving rewrite of the MOA. And that is why the road was paved to activate so many New York jurisdictions – painstakingly, one LEA at a time, and at the expense of hundreds of hours of effort, as I and the field coordinators can attest – during my tenure as regional coordinator.

Illinois: When I inherited this state from [redacted], Chicago and Cook County had already gone on record that they did not wish to participate. Repeated efforts by the Field Office Director, SC leaders, and even Mr. Morton, did not result in any change of that stance. In fact, it ultimately resulted (in late August / early September 2010) in a decision by the Illinois State Police, acting as the SIB, to take a stance similar to that which New York DCJS had taken and to require each sheriff to affirm his/her willingness to participate in interoperability before any county would be activated. (A short time later, even this stance was reversed to preclude any further activations in the state at all.) Fortunately for SC,

because of my perseverance and that of the field coordinator, by the time the program was halted, nearly every one of the 102 counties in the state had received outreach, and 26 had been activated. In fact, due to my efforts a number of the sheriffs in still-unactivated counties have gone on the record and indicated their willingness to see interoperability activated; it is only the "stop order" of the ISP that impedes going forward, something that cannot be laid at my doorstep.

My Activations This Fiscal Year. The number of activations set as a 2011 FY goal for SC was extremely high – over 900, if my memory serves me correctly. In the six months of this FY during which I was employed as a regional coordinator (October 2010 – March 2011), I was personally responsible for 316 activations – over 1/3 of the program's total yearly goal, done in half of a year by one person – and that is a conservative tally, because many of the jurisdictions activated in states which AI took over had been taken care of and already put onto the master dashboard by me prior to the turnover . (I do, however, lay claim to all 53 of the Indiana counties which continue to be activated whose schedules were established during my time as a regional coordinator.)

State	Number of Jurisdictions Activated During My Tenure, FY 2011
GA	7
IL	11
IN	53
KS	10
KY	1
MD	3
MO	26
NC	37
NY	14
OH	9
RI	5
SC	14
WI	72
WV	54
Total	**316**

In conclusion, Marc, I want to say that despite the public assertions and innuendos made by the agency and the department to the contrary, I worked tirelessly and am proud of my accomplishments on behalf of Secure Communities and the federal government. I took on much more than I had to, and perhaps more than I should have, believing it was the right thing to do.

And, contrary to the notion that I was somehow "off the reservation," the evidence of my commitment is that notwithstanding my firmly held view that interoperability cannot be lawfully considered optional, I recognized that as a contract employee, I did not have the last word. For

that reason, I faithfully put forward the government's often-shifting positions, as best I understood them, even when I did not personally agree with them and believed (as I still do) that in the end, the only rational position which the government can take is that it has both the right and the obligation to implement interoperability nationwide.

That I have been made a scapegoat for reasons of political expediency is more a reflection of the shifting sands of Secure Communities' ever changing opt-in / opt-out policies than any failings I brought to the job.

I wish you and the rest of the SC staff, both government and contractors, well and every success for the initiative itself.

Regards,
Dan Cadman

Attachments:

- Exhibit A – "NCIC GO-NO GO PAPER.doc" date / time created: 8/31/2009 10:14 AM (includes its own Appendices, 1 – 6)

- Exhibit B – "090325 WF826447 Price Q27 If a locality does not wish to participate in the Secure Communities.doc" date / time created: unknown

- Exhibit C – "ISSUE--OPT OUT.doc" date / time created: 9/1/2009 7:39 AM

EXHIBIT A

“NCIC GO-NO GO PAPER.doc”
(includes its own Appendices 1 – 6)

date / time created: 8/31/2009 10:14 AM

Monday, August 10, 2009

Re: Local Law Enforcement Agency (LEA) Authorization ("Go – No go") for Interoperability Deployment

[redacted],

Per [redacted]'s request, I have been looking into the functions and operations of the National Crime Information Center (NCIC) generally, and IAFIS more particularly, with an eye toward the "go – no go" system presently in place for purposes of Secure Communities interoperability deployment. (Parenthetically, I prefer the phrase "interoperability activation," but that's neither here nor there.)

I have concluded that submitting law enforcement agencies (LEAs) surrender their right to dictate what happens to the prints submitted under the existing modus operandi.

The U.S. Attorney General's collection of criminal identification information, including fingerprints, is authorized by federal law. *See 28 U.S.C. 534, attached as Appendix 1 (yellow highlighting has been added for ease of reference).* That statute is the 'undergirding' principle of the NCIC. The language of the statute clearly implies that collection equates to ownership of the information, once obtained.

The Attorney General has delegated such collection to the Federal Bureau of Investigation (FBI), which in addition to its own investigative responsibilities with regard to enforcement of various federal laws, has a secondary mission to assist and support state and local police agencies in the investigation and suppression of crime.

The FBI, in turn, created the Criminal Justice Information System (CJIS) division to administer the collection and collation of such information. The NCIC is a primary tool by which such information is gathered. Because the timely and complete collection of such information inevitably involves the states and their political subdivisions, it was important that, from the start, they be given a voice in operation and policy. Thus, the NCIC is governed by the FBI Director, with substantial input from an Advisory Policy Board consisting of state / local law enforcement officials. *For a succinct explanation of the workings and importance of the APB, see attached at Appendix 2, a paper from FBI Special Agent Don Johnson which, although dated, is still accurate.*

To take advantage of NCIC, the various states and other federal agencies sign an agreement agreeing to abide by all NCIC policies and procedures. Each state is required to designate a Control Terminal Agency (CTA), referred to in more modern parlance as a Control Systems Agency (CSA). These CSAs were formed within each state to control access to, and ensure compliance with the rules governing, NCIC. In the Secure Communities context, we know the CSAs more familiarly as the State Identification Bureaus (SIBs).

It is significant that the federal-interstate agreement does not filter below CSAs/SIBs. They are required, in turn, to maintain their own agreements with participating state and local law enforcement organizations. That is because the federal government has not contracted, via the compact with any organization below the state level. And, in binding the states, they bind their political subdivisions. The state – local agreements are also very specific in requiring each signing political subdivision of the state to abide by the laws, regulations and policies governing the NCIC. *For an example of a State SIB agreement with subordinate local law enforcement agencies, in this case South Carolina, refer to the attached Appendix 3.*

Fundamentally, then, through a chain of compacts / agreements, states and their political subdivisions have tendered to the federal government the right to collect, maintain and disseminate criminal justice information including fingerprints for all designated lawful purposes.

What are those lawful purposes? Clearly, criminal justice is one of them. However, only a part of the work performed by ICE meets with the definition of "criminal justice."

Enforcement of the civil and administrative removal provisions of immigration law are not technically criminal justice. An arrest in removal proceedings is not for the purpose of enforcing a criminal statute, and detention in order to effect a removal is not for the purpose of punishment. This does not lessen the importance of removal proceedings in the context of the nation's public safety and security, and as a fundamental assertion of our sovereignty—after all, a nation which surrenders the right to decide which non-citizens get to stay and which do not, is no nation at all.

But is there a lawful basis for disseminating fingerprints (and the corollary data relating to prior arrests and criminal history) of an individual to ICE for its administrative removal purposes? There is.

Recognizing that there are many valid purposes above-and-beyond pure criminal justice proceedings, Congress enacted a statute authorizing the United States to engage in a compact for that purpose with the several states. *See 42 U.S.C. 14611, attached as Appendix 4 to this paper.*

The specific provisions of this federal-interstate compact, which once again clearly limits signatories within each state to the appropriate authorities within the CSA/SIB, can be found in a succeeding statute, which specifically lays out "immigration and naturalization matters" as an authorized non-criminal justice purpose. *See 42 U.S.C. 14616, attached as Appendix 5 to this paper (yellow highlighting has been added for ease of reference).*

Thus, it is clear that states and their political subdivisions may not opt out from dissemination of fingerprint and corollary crime information to ICE or other DHS entities. *It is also clear that Congress intended strict compliance with the provisions of*

the compact, as is evident from the provisions of 42 U.S.C. 14615, a copy of which is attached as Appendix 6 to this paper.

This statute would appear to require the FBI, through CJIS, to take appropriate disciplinary action against any state or political subdivision of a state which refused to cooperate in the dissemination of fingerprints to DHS and thereafter ICE for purposes of a comparison against alien fingerprints maintained in US-VISIT biometric data repositories.

In sum, then, it would appear that there is no obstacle to adjusting the language of electronic communications from ICE to local LEAs, away from a "go-no go" standard to one of simple notification that activation will occur on a date certain, and asking whether those LEAs wish to receive the resultant matched IAR, if any.

Having provided you with my views based on a review of relevant statutes, I will go further, however, and speculate that even if Secure Communities makes the shift away from a "go – no go" standard (and I think the program should), it is possible that some communities which are disinclined to cooperate with ICE in any fundamental way will find another mechanism to disenfranchise themselves.

If they do, it is entirely likely that the avenue this will take is through a refusal to honor detainers filed against particular criminal aliens. I have noted with interest that in at least one jurisdiction the American Civil Liberties Union has filed suit on behalf of detainees against a local police agency for honoring such a detainer, arguing that to do so was to engage in unlawful restraint of their liberties since the local agency has no authority to enforce administrative provisions of federal immigration law.

While I would like to say that the suit will be dismissed, or that the court will issue findings on behalf of the LEA, because of the existence of law and regulations embedded in the Immigration and Nationality Act authorizing the filing and honoring of such detainers, I do not know enough of the specific facts (for instance, whether ICE honored its detainer(s) in a timely fashion) to reach that conclusion. And, until the court renders its judgment, certainly the case is a chilling factor, and can be cited by local LEAs as a reason to opt out of honoring detainers filed by ICE.

Hope this helps,

Dan Cadman

APPENDIX 1

28 U.S.C. § 534. Acquisition, preservation, and exchange of identification records and information; appointment of officials[5]

(a) The Attorney General shall—
(1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records;
(2) acquire, collect, classify, and preserve any information which would assist in the identification of any deceased individual who has not been identified after the discovery of such deceased individual;
(3) acquire, collect, classify, and preserve any information which would assist in the location of any missing person (including an unemancipated person as defined by the laws of the place of residence of such person) and provide confirmation as to any entry for such a person to the parent, legal guardian, or next of kin of that person (and the Attorney General may acquire, collect, classify, and preserve such information from such parent, guardian, or next of kin); and
(4) exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States, cities, and penal and other institutions.
(b) The exchange of records and information authorized by subsection (a)(4) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.
(c) The Attorney General may appoint officials to perform the functions authorized by this section.
(d) Indian Law Enforcement Agencies.— The Attorney General shall permit Indian law enforcement agencies, in cases of domestic violence, dating violence, sexual assault, and stalking, to enter information into Federal criminal information databases and to obtain information from the databases.
(e) For purposes of this section, the term "other institutions" includes—
(1) railroad police departments which perform the administration of criminal justice and have arrest powers pursuant to a State statute, which allocate a substantial part of their annual budget to the administration of criminal justice, and which meet training requirements established by law or ordinance for law enforcement officers; and

[5] Title 42 of the US Code as currently published by the US Government reflects the laws passed by Congress as of Jan. 8, 2008, and it is this version that is published here.

(2) police departments of private colleges or universities which perform the administration of criminal justice and have arrest powers pursuant to a State statute, which allocate a substantial part of their annual budget to the administration of criminal justice, and which meet training requirements established by law or ordinance for law enforcement officers.

(f)

(1) Information from national crime information databases consisting of identification records, criminal history records, protection orders, and wanted person records may be disseminated to civil or criminal courts for use in domestic violence or stalking cases. Nothing in this subsection shall be construed to permit access to such records for any other purpose.

(2) Federal and State criminal justice agencies authorized to enter information into criminal information databases may include—

(A) arrests, convictions, and arrest warrants for stalking or domestic violence or for violations of protection orders for the protection of parties from stalking or domestic violence; and

(B) protection orders for the protection of persons from stalking or domestic violence, provided such orders are subject to periodic verification.

(3) As used in this subsection—

(A) the term “national crime information databases” means the National Crime Information Center and its incorporated criminal history databases, including the Interstate Identification Index; and

(B) the term “protection order” includes—

(i) any injunction, restraining order, or any other order issued by a civil or criminal court for the purpose of preventing violent or threatening acts or harassment against, sexual violence or contact or communication with or physical proximity to, another person, including any temporary or final orders issued by civil or criminal courts whether obtained by filing an independent action or as a pendente lite order in another proceeding so long as any civil order was issued in response to a complaint, petition, or motion filed by or on behalf of a person seeking protection; and

(ii) any support, child custody or visitation provisions, orders, remedies, or relief issued as part of a protection order, restraining order, or stay away injunction pursuant to State, tribal, territorial, or local law authorizing the issuance of protection orders, restraining orders, or injunctions for the protection of victims of domestic violence, dating violence, sexual assault, or stalking.

APPENDIX 2

January 1991

NCIC TRAINING: HIT OR MISS

By

Don M. Johnson
Special Agent
FBI Headquarters, Washington, DC

Today, the National Crime Information Center (NCIC) continues to be the best example of law enforcement cooperation. Information on wanted persons, stolen guns, stolen articles and securities, unidentified bodies, and computerized criminal history information is available to virtually every police agency in the United States. However, without proper training on the use of NCIC and State computer systems, law enforcement agencies could lose their tactical edge and may no longer be able to ensure that their employees perform their duties as efficiently and accurately as possible.

NCIC IN BRIEF

Management of NCIC is shared between the FBI and the Advisory Policy Board (APB). The APB consists of 20 elected State representatives, 6 individuals appointed by the Director of the FBI, and 4 representatives of national law enforcement organizations, including the International Association of Chiefs of Police, the National Sheriff's Association, the National District Attorneys Conference, and the National Probation and Parole Association. Together they set policy and procedure for NCIC's 59,000 users.

LAW ENFORCEMENT AND NCIC TRAINING

Law enforcement training in the 1960s saw an explosion of minimum standards for police officers nationwide. From then on, officers were required to be trained and certified prior to active duty. This training included such topics as legal issues, firearms, mechanics of arrest, report writing, first aid, and defensive driving. These minimum standards for police have greatly increased the quality of law enforcement in the United States today.

Prior to 1984, the responsibility for training NCIC and State terminal operators was left to the discretion of the various State criminal information system managers. These managers decided the amount and type of training given to terminal operators. As a result, the APB noted marked differences in the types and quality of NCIC/State system training that terminal operators were receiving.

The APB also recognized that many States limited their training to terminal operators, and as a result, the training was very technical in nature. However, by limiting training to terminal operators, many states neglected the training needs of

officers, investigators, and administrators, especially in the areas of data quality and user compliance with policy issues. For these reasons, the APB mandated that by December 31, 1986, all 50 states were to have NCIC training programs in place for the following four separate personnel levels: (1)

* Terminal Operators--Must be trained and tested within 6 months of employment or assignment. Their proficiency must also be retested biennially.

* Criminal Justice Practitioners--The daily users of the NCIC/State systems are required to receive entry level and inservice training. They must be taught what signifies a "hit," the levels of probable cause needed for arrest, the need for hit confirmation, the idiosyncrasies of soundexing, and the availability and searchability of various fields within a record.

* Criminal Justice Agency Records Personnel--Individuals who control the records management systems in every law enforcement agency are required to be completely familiar with all NCIC/State systems policy and procedure matters.

* Criminal Justice Administrators and Upper-level Managers--Must have a thorough knowledge of NCIC regulations, including training, audits, sanctions, and the related civil liability issues to guide them in protecting their agencies from law suits.

Since NCIC's beginning in 1967, one law enforcement agency in every State has assumed the responsibility for managing that State's computer system and its relationship with NCIC. This agency is known as the Control Terminal Agency (CTA). Each CTA has also designated one individual within that agency to assume the responsibility for complying with NCIC policy and procedure issues. This individual is known as the Control Terminal Officer (CTO). The CTO in each CTA has training programs available for all law enforcement agencies within that State.

The NCIC training policy was made intentionally broad to allow the CTAs to employ a wide variety of methods. Under this policy, each CTA has the flexibility to create its own training program using available resources. Since the policy and procedures mandated by NCIC and the APB apply to all 50 States, as well as Federal users, each State has incorporated national policy issues into its training programs. As a result, the quality of the data in computerized systems and compliance with national and State policy issues has become a priority in State training programs.

Even though training in one State may be handled regionally, another State may centralize its training program. Yet, no matter how a State trains its personnel, all must teach nationwide policy and procedural issues mandated by the APB. This provides assurance to the criminal justice community that terminal operators, police officers, record managers, and

administrators across the country receive adequate and uniform training on such important issues as hit confirmation, validation, and the necessity for entering information into NCIC and the State systems in a timely and accurate manner.

IMPORTANCE OF ADEQUATE TRAINING

Complete and proper use of NCIC/State computer systems can save the lives of police officers, fugitives, and innocent citizens. Tragically, in one recent case, a terminal operator failed to enter a stolen vehicle into NCIC in a timely fashion. Instead, the operator waited for additional information before making the vehicle entry. A police officer on routine patrol stopped a car that fit the description of a stolen vehicle, queried NCIC, and received a negative response. When the officer approached the vehicle, the car thief killed the officer. This tragedy could have been prevented if the operator were trained as to the minimum criteria for entering stolen vehicle records into NCIC. Unfortunately, many similar examples exist as a result of improper use or inadequate training of NCIC and State computer systems.

Use of available NCIC and State systems will also generate investigative leads for law enforcement agencies. Through training, officers have become more aware of the Interstate Identification Index, State data bases, public domain data bases, and the National Law Enforcement Telecommunications System (NLETS). For example, when an officer obtains an arrest warrant, the Interstate Identification Index is queried. When positive identification is made, the Index will produce aliases, fingerprint classifications, places of birth, Social Security numbers, and a multitude of other descriptive information that will aid the department in its search for the fugitive.

CONCLUSION

Just as terminal opeators' adrenaline rises when an NCIC "hit" appears on the monitor, police administrators' adrenaline should also rise if they have not provided their employees with the best available training in NCIC and State computerized system use. But, by using the State NCIC training programs available through each State's Control Terminal Agency, police administrators can be assured that their employees enter accurate and complete information into NCIC, know how to interpret the information accurately in the system, validate active records, and promptly remove old records from the system. While doctors can change a prescription and lawyers can cross-examine witnesses, the law enforcement employee must often make swift decisions based on the instantaneous results of NCIC and State system inquiries. All law enforcement agencies must, therefore, ensure that law enforcement employees are able to use the NCIC and State systems. For someone, there may not be a second chance.

FOOTNOTE

(1) U.S. Department of Justice, Federal Bureau of Investigation, "Minutes National Crime Information Center Advisory Board," October 17-18, 1984, pp 311-312.

APPENDIX 3

South Carolina Law Enforcement Division
Criminal Justice Information System

(CJIS)

USER AGREEMENT AND SYSTEM RESPONSIBILITIES

Introduction

The South Carolina Criminal Justice Information and Communications System (CJIS) operates under a shared management concept between the South Carolina Law Enforcement Division (SLED), as the service provider, and criminal justice agencies or non-governmental agencies contracting to support certain functions for criminal justice agencies, as the service users, herein after known as "user agencies".

Criminal Justice Information and Communications System (CJIS) User Agreement

The responsibility of the SLED CJIS Division is to provide up-to-date, reliable and quality identification and information services to user agencies.

The out-of-state data (originating outside of South Carolina) provided by the SLED CJIS Division are managed and exchanged in cooperation with the FBI CJIS Division, each state CJIS Systems Agency (CSA) and Federal Service Coordinator (FSC). This information includes, but is not limited to, the Interstate Identification Index (III), the National Crime Information Center (NCIC), National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs. In addition, information is routed from all the states, Canada, and certain federal agencies via the National Law Enforcement Telecommunications System (NLETS)

The in-state data (originating within South Carolina) provided by the SLED CJIS Division are routed from and exchanged with source agencies in South Carolina. This information includes, but is not limited to, the South Carolina Central Repository for Computerized Criminal History (CCH) Record Information, the South Carolina Hot File(s), the South Carolina Incident-Based Reporting System (SCIBRS), the South Carolina Sex Offender Registry (SOR), the South Carolina Automated Fingerprint Identification System (SC AFIS), and the Violent Gang Terrorist Organization File programs. Motor vehicle and motor vehicle operator data managed by the SC Department of Public Safety are routed via interface with that agency.

In order to fulfill this responsibility, the SLED CJIS Division provides the following services to its users:

- State CJIS Systems Agency and interface services for NCIC;
- State CJIS Systems Agency and interface services for NLETS;
- National Weather Service and sex offender registry;

- Operational, technical, and investigative assistance;

- Policy review of matters pertaining to III, NCIC, NIBRS, IAFIS and CCH, SCIBRS, SC SOR, SC AFIS;
- Training assistance to each terminal agency coordinator;
- Ongoing assistance to System users; and
- System and data integrity auditing.

.

The following documents are incorporated by reference and made part of this agreement:

- *Interstate Identification Index Operational and Technical Manual*, *NCIC 2000 Operating Manua and related updates (TOUS)*; and National Incident-Based Reporting System Volumes 1-4;
- Minutes of the FBI CJIS Advisory Policy Board meetings;
- *Bylaws for the CJIS Advisory Policy Board and Working Groups;*
- *Title 28, United States Code, Section 534;*
- *Title 28,Code of Federal Regulations, Sections 16.30 – 16.34, Part 20, Part 25;*
- *Title 42, United States Code, Section 14611;*
- [FBI] CJIS Security Policy to include all elements of the NCIC Computerized Criminal History Program Background, Concept and Policy;
- *A Policy and Reference Manual*;
- Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information, and NCIC Standards, as recommended by the [FBI] CJIS Advisory Policy Board;
- Other relevant documents to include NCIC Technical and Operational Update, CJIS Information Letter, etc.;
- *SLED Personnel Security Policy 7.6*, SLED Technical Security Policies 7.6 et seq., *Section 23-3-40 of the SC Code of Laws, Section 23-3-110 et seq. of the SC Code of Laws, Section 23-4-430 et seq. of the SC Code of Laws, SC Appropriations Act Proviso 56DD.8. et seq., Chapter 73 of the SC Regulations, SLED CJIS Operations Manual*;
- South Carolina Incident-Based Reporting System (SCIBRS) Guide/Training Manual;
- SLED CJIS NCIC Entry Quality Check Form (CJ-016);
- SLED CJIS Missing Person Validation Form (CJ-017); Amber Alert Information; and
- Other applicable federal and state laws, regulations, guides and forms.

The following NCIC or state files are available when direct access is authorized:

Identity Theft

Unidentified Person

Stolen Vehicle

Stolen Article
Stolen or Recovered Gun
Stolen License Plate
Wanted Person
Stolen Securities
Stolen Boat

Missing Person
US Secret Service Protective
Dept. Motor Vehicles
Foreign Fugitive
Violent Gang / Terrorist Org.
Deported Felon
Protective Order File
Interstate Identification Index
SC Sex Offender Registry

SC Criminal Histories SC Alcohol Local Option
SC Concealed Weapons

The following limitations or conditions, if any, for specified state and/or NLETS files are made:

By accepting access as set forth above, the user agency agrees to adhere to the following NCIC and SLED CJIS policies in order to ensure continuation of that access:

1. TIMELINESS: (Availability, including priority of service): Agency records must be entered, modified, cleared, and canceled promptly in NCIC to ensure maximum system effectiveness. Agencies that provide NCIC access to other agencies, such as through an interface or other process for non-terminal agencies, must ensure priority service for those agencies.
   Fingerprints of custodial arrest subjects taken by a law enforcement agency or detention facility for state offenses must be submitted to SLED within three workdays; and wanted persons records meeting entry criteria must be entered into NCIC immediately upon receipt of the arrest warrants by the law enforcement agency (i.e., not more than three days after).

2. QUALITY ASSURANCE: Appropriate and reasonable quality assurance procedures must be in place to ensure that the most complete, accurate, and valid entries are in NCIC. Pursuant to § 23-3-120 of the SC Code of Laws, a person subjected to a custodial arrest for a state offense must be fingerprinted for identification and to establish records.

3. VALIDATION: NCIC requires that all records except Article File records be validated 60-90 days after entry and annually thereafter. The NCIC Validation Policy is defined as:

   Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized, and copies of these procedures must be on file for review during an NCIC audit.

   SLED CJIS requirements include, but are not necessarily limited to, conducting quarterly Missing Person Validations, completing the Missing Person Validation Form and the NCIC Entry Quality Check Form.

4. HIT CONFIRMATION: Each agency entering records must, within ten minutes or one-hour depending on priority, furnish to an agency requesting a record confirmation a response indicating a positive or negative confirmation or notice of the specific amount of time necessary to provide a response to the request for record confirmation.
5. SECURITY: See Technical Security Policies 7.6 (Available through SLED ISO).
6. DISSEMINATION: See Dissemination Policy 7.13 (Located in FBI/CJIS Security Policy & S.C Code of Laws.

7. AUDIT: See FBI/CJIS Security Policy. (Located on LEMS.WEB & LEO
8. NCIC & SCIBRS TRAINING: Each agency will be responsible for complying with mandated training requirements.

9. PERSONNEL BACKGROUND SCREENING: According to the FBI CJIS Security Policy, all personnel who have authorized access to FBI CJIS systems must be fingerprinted within 30 days of initial employment or assignment to include personnel directly responsible to configure and maintain computer systems and networks with direct access to FBI CJIS systems (4.5.1, (a)). Agencies should send to SLED Records on (1) completed blue applicant fingerprint card with "Criminal Justice Applicant" as the reason.
10. LOGGING: See Technical Security Policies.
11. USE OF THE SYSTEM: According to any NCIC/state policies not specifically listed above:
    A. The user agency will provide fingerprints for all custodial arrests made or brought by that agency, or ensure that they are provided, in turn, by another agency on behalf of the arresting or charging agency either via electronic submission or fingerprint card that meet submission criteria.
    B. Each user agency with an interface to SLED CJIS must establish and maintain an information security structure that is satisfactory to the SLED Information Security Officer (ISO).
    C. The user agency is responsible for the system access by that agency and any other agency that is, in turn, served by their agency.
    D. Each user agency is to have a Terminal Agency Coordinator (TAC) to ensure adherence to NCIC and SLED CJIS procedures and policies within each user agency.

Acknowledgment and Certification

We hereby acknowledge the duties and responsibilities as set out in this agreement. We acknowledge that these duties and responsibilities have been developed and approved by NCIC System users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the FBI / SLED CJIS Systems. We further acknowledge that a failure to comply with these duties and responsibilities will subject our access to various sanctions as approved by the [FBI] Criminal Justice Information Services Advisory Policy Board. These sanctions may include the termination of NCIC services to the agency. We may appeal these sanctions through our CJIS Systems Agency.

_____
Name of User Agency

_____
Address for User Agency

_____

_____
ORI for User Agency

E-mail Address

_____
Signature of User Agency Head

SLED:

Reginald I. Lloyd, Director

BY:

_____
Signature of CSO

_____

Title/Date

_____
Title/Date

Agencies Serviced By User Agency

Agency Name	ORI Number
Agency Name	ORI Number
Agency Name	ORI Number
Agency Name	ORI Number

Non-terminal User Agreement(s) with the above agencies must be on file with the user agency.

Revised 03/05/08

APPENDIX 4

42 U.S.C. § 14611. Findings[6]

Congress finds that—
(1) both the Federal Bureau of Investigation and State criminal history record repositories maintain fingerprint-based criminal history records;
(2) these criminal history records are shared and exchanged for criminal justice purposes through a Federal-State program known as the Interstate Identification Index System;
(3) although these records are also exchanged for legally authorized, noncriminal justice uses, such as governmental licensing and employment background checks, the purposes for and procedures by which they are exchanged vary widely from State to State;
(4) an interstate and Federal-State compact is necessary to facilitate authorized interstate criminal history record exchanges for noncriminal justice purposes on a uniform basis, while permitting each State to effectuate its own dissemination policy within its own borders; and
(5) such a compact will allow Federal and State records to be provided expeditiously to governmental and nongovernmental agencies that use such records in accordance with pertinent Federal and State law, while simultaneously enhancing the accuracy of the records and safeguarding the information contained therein from unauthorized disclosure or use.

[6] Title 42 of the US Code as currently published by the US Government reflects the laws passed by Congress as of Jan. 8, 2008, and it is this version that is published here.

APPENDIX 5

42 U.S.C. § 14616. National Crime Prevention and Privacy Compact[7]

The Contracting Parties agree to the following:
Overview
(a) In general
This Compact organizes 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, such as background checks for governmental licensing and employment.
(b) Obligations of parties
Under this Compact, the FBI and the Party 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 Party States for authorized purposes. The FBI shall also manage the Federal data facilities that provide a significant part of the infrastructure for the system.
ARTICLE I—DEFINITIONS
In this Compact:
(1) Attorney General
The term "Attorney General" means the Attorney General of the United States.
(2) Compact officer
The term "Compact officer" means—
(A) with respect to the Federal Government, an official so designated by the Director of the FBI; and
(B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
(3) Council
The term "Council" means the Compact Council established under Article VI.
(4) Criminal history records
The term "criminal history records"—
(A) means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; and

[7] Title 42 of the US Code as currently published by the US Government reflects the laws passed by Congress as of Jan. 8, 2008, and it is this version that is published here.

(B) does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

(5) Criminal history record repository

The term "criminal history record repository" means the State agency designated by the Governor or other appropriate executive official or the legislature of a State to perform centralized recordkeeping functions for criminal history records and services in the State.

(6) Criminal justice

The term "criminal justice" includes activities relating to the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage, and dissemination of criminal history records.

(7) Criminal justice agency

The term "criminal justice agency"—

(A) means—

(i) courts; and

(ii) a governmental agency or any subunit thereof that—

(I) performs the administration of criminal justice pursuant to a statute or Executive order; and

(II) allocates a substantial part of its annual budget to the administration of criminal justice; and

(B) includes Federal and State inspectors general offices.

(8) Criminal justice services

The term "criminal justice services" means services provided by the FBI to criminal justice agencies in response to a request for information about a particular individual or as an update to information previously provided for criminal justice purposes.

(9) Criterion offense

The term "criterion offense" means any felony or misdemeanor offense not included on the list of nonserious offenses published periodically by the FBI.

(10) Direct access

The term "direct access" means access to the National Identification Index by computer terminal or other automated means not requiring the assistance of or intervention by any other party or agency.

(11) Executive order

The term "Executive order" means an order of the President of the United States or the chief executive officer of a State that has the force of law and that is promulgated in accordance with applicable law.

(12) FBI

The term "FBI" means the Federal Bureau of Investigation.

(13) Interstate Identification System

The term “Interstate Identification Index System” or “III System”—
(A) means the cooperative Federal-State system for the exchange of criminal history records; and
(B) includes the National Identification Index, the National Fingerprint File and, to the extent of their participation in such system, the criminal history record repositories of the States and the FBI.

(14) National Fingerprint File

The term “National Fingerprint File” means a database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

(15) National Identification Index

The term “National Identification Index” means an index maintained by the FBI consisting of names, identifying numbers, and other descriptive information relating to record subjects about whom there are criminal history records in the III System.

(16) National indices

The term “National indices” means the National Identification Index and the National Fingerprint File.

(17) Nonparty State

The term “Nonparty State” means a State that has not ratified this Compact.

(18) Noncriminal justice purposes

The term “noncriminal justice purposes” means uses of criminal history records for purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

(19) Party State

The term “Party State” means a State that has ratified this Compact.

(20) Positive identification

The term “positive identification” means a determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects’ names or other nonunique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

(21) Sealed record information

The term “sealed record information” means—
(A) with respect to adults, that portion of a record that is—
(i) not available for criminal justice uses;
(ii) not supported by fingerprints or other accepted means of positive identification; or

(iii) subject to restrictions on dissemination for noncriminal justice purposes pursuant to a court order related to a particular subject or pursuant to a Federal or State statute that requires action on a sealing petition filed by a particular record subject; and

(B) with respect to juveniles, whatever each State determines is a sealed record under its own law and procedure.

(22) State

The term "State" means any State, territory, or possession of the United States, the District of Columbia, and the Commonwealth of Puerto Rico.

ARTICLE II—PURPOSES

The purposes of this Compact are to—

(1) provide a legal framework for the establishment of a cooperative Federal-State system for the interstate and Federal-State exchange of criminal history records for noncriminal justice uses;

(2) require the FBI to permit use of the National Identification Index and the National Fingerprint File by each Party State, and to provide, in a timely fashion, Federal and State criminal history records to requesting States, in accordance with the terms of this Compact and with rules, procedures, and standards established by the Council under Article VI;

(3) require Party States to provide information and records for the National Identification Index and the National Fingerprint File and to provide criminal history records, in a timely fashion, to criminal history record repositories of other States and the Federal Government for noncriminal justice purposes, in accordance with the terms of this Compact and with rules, procedures, and standards established by the Council under Article VI;

(4) provide for the establishment of a Council to monitor III System operations and to prescribe system rules and procedures for the effective and proper operation of the III System for noncriminal justice purposes; and

(5) require the FBI and each Party State to adhere to III System standards concerning record dissemination and use, response times, system security, data quality, and other duly established standards, including those that enhance the accuracy and privacy of such records. ARTICLE III—RESPONSIBILITIES OF COMPACT PARTIES

(a) FBI responsibilities

The Director of the FBI shall—

(1) appoint an FBI Compact officer who shall—

(A) administer this Compact within the Department of Justice and among Federal agencies and other agencies and organizations that submit search requests to the FBI pursuant to Article V(c);

(B) ensure that Compact provisions and rules, procedures, and standards prescribed by the Council under Article VI are complied with by the Department of Justice and the Federal agencies and other agencies and organizations referred to in Article III(1)(A); and

(C) regulate the use of records received by means of the III System from Party States when such records are supplied by the FBI directly to other Federal agencies;
(2) provide to Federal agencies and to State criminal history record repositories, criminal history records maintained in its database for the noncriminal justice purposes described in Article IV, including—
(A) information from Nonparty States; and
(B) information from Party States that is available from the FBI through the III System, but is not available from the Party State through the III System;
(3) provide a telecommunications network and maintain centralized facilities for the exchange of criminal history records for both criminal justice purposes and the noncriminal justice purposes described in Article IV, and ensure that the exchange of such records for criminal justice purposes has priority over exchange for noncriminal justice purposes; and
(4) modify or enter into user agreements with Nonparty State criminal history record repositories to require them to establish record request procedures conforming to those prescribed in Article V.

(b) State responsibilities

Each Party State shall—
(1) appoint a Compact officer who shall—
(A) administer this Compact within that State;
(B) ensure that Compact provisions and rules, procedures, and standards established by the Council under Article VI are complied with in the State; and
(C) regulate the in-State use of records received by means of the III System from the FBI or from other Party States;
(2) establish and maintain a criminal history record repository, which shall provide—
(A) information and records for the National Identification Index and the National Fingerprint File; and
(B) the State's III System-indexed criminal history records for noncriminal justice purposes described in Article IV;
(3) participate in the National Fingerprint File; and
(4) provide and maintain telecommunications links and related equipment necessary to support the services set forth in this Compact.

(c) Compliance with III System standards

In carrying out their responsibilities under this Compact, the FBI and each Party State shall comply with III System rules, procedures, and standards duly established by the Council concerning record dissemination and use, response times, data quality, system security, accuracy, privacy protection, and other aspects of III System operation.

(d) Maintenance of record services

(1) Use of the III System for noncriminal justice purposes authorized in this Compact shall be managed so as not to diminish the level of services provided in support of criminal justice purposes.
(2) Administration of Compact provisions shall not reduce the level of service available to authorized noncriminal justice users on the effective date of this Compact. ARTICLE IV—AUTHORIZED RECORD DISCLOSURES
(a) State criminal history record repositories
To the extent authorized by section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974"), the FBI shall provide on request criminal history records (excluding sealed records) to State criminal history record repositories for noncriminal justice purposes allowed by Federal statute, Federal Executive order, or a State statute that has been approved by the Attorney General and that authorizes national indices checks.
(b) Criminal justice agencies and other governmental or nongovernmental agencies
The FBI, to the extent authorized by section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974"), and State criminal history record repositories shall provide criminal history records (excluding sealed records) to criminal justice agencies and other governmental or nongovernmental agencies for noncriminal justice purposes allowed by Federal statute, Federal Executive order, or a State statute that has been approved by the Attorney General, that authorizes national indices checks.
(c) Procedures
Any record obtained under this Compact may be used only for the official purposes for which the record was requested. Each Compact officer shall establish procedures, consistent with this Compact, and with rules, procedures, and standards established by the Council under Article VI, which procedures shall protect the accuracy and privacy of the records, and shall—
(1) ensure that records obtained under this Compact are used only by authorized officials for authorized purposes;
(2) require that subsequent record checks are requested to obtain current information whenever a new need arises; and
(3) ensure that record entries that may not legally be used for a particular noncriminal justice purpose are deleted from the response and, if no information authorized for release remains, an appropriate "no record" response is communicated to the requesting official. ARTICLE V—RECORD REQUEST PROCEDURES
(a) Positive identification
Subject fingerprints or other approved forms of positive identification shall be submitted with all requests for criminal history record checks for noncriminal justice purposes.
(b) Submission of State requests

Each request for a criminal history record check utilizing the national indices made under any approved State statute shall be submitted through that State's criminal history record repository. A State criminal history record repository shall process an interstate request for noncriminal justice purposes through the national indices only if such request is transmitted through another State criminal history record repository or the FBI.

(c) Submission of Federal requests

Each request for criminal history record checks utilizing the national indices made under Federal authority shall be submitted through the FBI or, if the State criminal history record repository consents to process fingerprint submissions, through the criminal history record repository in the State in which such request originated. Direct access to the National Identification Index by entities other than the FBI and State criminal history records repositories shall not be permitted for noncriminal justice purposes.

(d) Fees

A State criminal history record repository or the FBI—

(1) may charge a fee, in accordance with applicable law, for handling a request involving fingerprint processing for noncriminal justice purposes; and

(2) may not charge a fee for providing criminal history records in response to an electronic request for a record that does not involve a request to process fingerprints.

(e) Additional search

(1) If a State criminal history record repository cannot positively identify the subject of a record request made for noncriminal justice purposes, the request, together with fingerprints or other approved identifying information, shall be forwarded to the FBI for a search of the national indices.

(2) If, with respect to a request forwarded by a State criminal history record repository under paragraph (1), the FBI positively identifies the subject as having a III System-indexed record or records—

(A) the FBI shall so advise the State criminal history record repository; and

(B) the State criminal history record repository shall be entitled to obtain the additional criminal history record information from the FBI or other State criminal history record repositories. ARTICLE VI—ESTABLISHMENT OF COMPACT COUNCIL

(a) Establishment

(1) In general

There is established a council to be known as the "Compact Council", which shall have the authority to promulgate rules and procedures governing the use of the III System for noncriminal justice purposes, not to conflict with FBI administration of the III System for criminal justice purposes.

(2) Organization

The Council shall—

(A) continue in existence as long as this Compact remains in effect;

(B) be located, for administrative purposes, within the FBI; and
(C) be organized and hold its first meeting as soon as practicable after the effective date of this Compact.

(b) Membership

The Council shall be composed of 15 members, each of whom shall be appointed by the Attorney General, as follows:
(1) Nine members, each of whom shall serve a 2-year term, who shall be selected from among the Compact officers of Party States based on the recommendation of the Compact officers of all Party States, except that, in the absence of the requisite number of Compact officers available to serve, the chief administrators of the criminal history record repositories of Nonparty States shall be eligible to serve on an interim basis.
(2) Two at-large members, nominated by the Director of the FBI, each of whom shall serve a 3-year term, of whom—
(A) 1 shall be a representative of the criminal justice agencies of the Federal Government and may not be an employee of the FBI; and
(B) 1 shall be a representative of the noncriminal justice agencies of the Federal Government.
(3) Two at-large members, nominated by the Chairman of the Council, once the Chairman is elected pursuant to Article VI(c), each of whom shall serve a 3-year term, of whom—
(A) 1 shall be a representative of State or local criminal justice agencies; and
(B) 1 shall be a representative of State or local noncriminal justice agencies.
(4) One member, who shall serve a 3-year term, and who shall simultaneously be a member of the FBI's advisory policy board on criminal justice information services, nominated by the membership of that policy board.
(5) One member, nominated by the Director of the FBI, who shall serve a 3-year term, and who shall be an employee of the FBI.

(c) Chairman and Vice Chairman

(1) In general

From its membership, the Council shall elect a Chairman and a Vice Chairman of the Council, respectively. Both the Chairman and Vice Chairman of the Council—
(A) shall be a Compact officer, unless there is no Compact officer on the Council who is willing to serve, in which case the Chairman may be an at-large member; and
(B) shall serve a 2-year term and may be reelected to only 1 additional 2-year term.

(2) Duties of Vice Chairman

The Vice Chairman of the Council shall serve as the Chairman of the Council in the absence of the Chairman.

(d) Meetings

(1) In general
The Council shall meet at least once each year at the call of the Chairman. Each meeting of the Council shall be open to the public. The Council shall provide prior public notice in the Federal Register of each meeting of the Council, including the matters to be addressed at such meeting.
(2) Quorum
A majority of the Council or any committee of the Council shall constitute a quorum of the Council or of such committee, respectively, for the conduct of business. A lesser number may meet to hold hearings, take testimony, or conduct any business not requiring a vote.
(e) Rules, procedures, and standards
The Council shall make available for public inspection and copying at the Council office within the FBI, and shall publish in the Federal Register, any rules, procedures, or standards established by the Council.
(f) Assistance from FBI
The Council may request from the FBI such reports, studies, statistics, or other information or materials as the Council determines to be necessary to enable the Council to perform its duties under this Compact. The FBI, to the extent authorized by law, may provide such assistance or information upon such a request.
(g) Committees
The Chairman may establish committees as necessary to carry out this Compact and may prescribe their membership, responsibilities, and duration.
ARTICLE VII—RATIFICATION OF COMPACT
This Compact shall take effect upon being entered into by 2 or more States as between those States and the Federal Government. Upon subsequent entering into this Compact by additional States, it shall become effective among those States and the Federal Government and each Party State that has previously ratified it. When ratified, this Compact shall have the full force and effect of law within the ratifying jurisdictions. The form of ratification shall be in accordance with the laws of the executing State.
ARTICLE VIII—MISCELLANEOUS PROVISIONS
(a) Relation of Compact to certain FBI activities
Administration of this Compact shall not interfere with the management and control of the Director of the FBI over the FBI's collection and dissemination of criminal history records and the advisory function of the FBI's advisory policy board chartered under the Federal Advisory Committee Act (5 U.S.C. App.) for all purposes other than noncriminal justice.
(b) No authority for nonappropriated expenditures
Nothing in this Compact shall require the FBI to obligate or expend funds beyond those appropriated to the FBI.
(c) Relating to Public Law 92–544
Nothing in this Compact shall diminish or lessen the obligations, responsibilities, and authorities of any State, whether a Party State or a

Nonparty State, or of any criminal history record repository or other subdivision or component thereof, under the Departments of State, Justice, and Commerce, the Judiciary, and Related Agencies Appropriation Act, 1973 (Public Law 92–544), or regulations and guidelines promulgated thereunder, including the rules and procedures promulgated by the Council under Article VI(a), regarding the use and dissemination of criminal history records and information.

ARTICLE IX—RENUNCIATION

(a) In general

This Compact shall bind each Party State until renounced by the Party State.

(b) Effect

Any renunciation of this Compact by a Party State shall—

(1) be effected in the same manner by which the Party State ratified this Compact; and

(2) become effective 180 days after written notice of renunciation is provided by the Party State to each other Party State and to the Federal Government. ARTICLE X—SEVERABILITY

The provisions of this Compact shall be severable, and if any phrase, clause, sentence, or provision of this Compact is declared to be contrary to the constitution of any participating State, or to the Constitution of the United States, or the applicability thereof to any government, agency, person, or circumstance is held invalid, the validity of the remainder of this Compact and the applicability thereof to any government, agency, person, or circumstance shall not be affected thereby. If a portion of this Compact is held contrary to the constitution of any Party State, all other portions of this Compact shall remain in full force and effect as to the remaining Party States and in full force and effect as to the Party State affected, as to all other provisions.

ARTICLE XI—ADJUDICATION OF DISPUTES

(a) In general

The Council shall—

(1) have initial authority to make determinations with respect to any dispute regarding—

(A) interpretation of this Compact;

(B) any rule or standard established by the Council pursuant to Article V; and

(C) any dispute or controversy between any parties to this Compact; and

(2) hold a hearing concerning any dispute described in paragraph (1) at a regularly scheduled meeting of the Council and only render a decision based upon a majority vote of the members of the Council. Such decision shall be published pursuant to the requirements of Article VI(e).

(b) Duties of FBI

The FBI shall exercise immediate and necessary action to preserve the integrity of the III System, maintain system policy and standards, protect

the accuracy and privacy of records, and to prevent abuses, until the Council holds a hearing on such matters.

(c) Right of appeal

The FBI or a Party State may appeal any decision of the Council to the Attorney General, and thereafter may file suit in the appropriate district court of the United States, which shall have original jurisdiction of all cases or controversies arising under this Compact. Any suit arising under this Compact and initiated in a State court shall be removed to the appropriate district court of the United States in the manner provided by section 1446 of title 28, United States Code, or other statutory authority.

APPENDIX 6

42 U.S.C. § 14615. Enforcement and implementation[8]

All departments, agencies, officers, and employees of the United States shall enforce the Compact and cooperate with one another and with all Party States in enforcing the Compact and effectuating its purposes. For the Federal Government, the Attorney General shall make such rules, prescribe such instructions, and take such other actions as may be necessary to carry out the Compact and this subchapter.

[8] Title 42 of the US Code as currently published by the US Government reflects the laws passed by Congress as of Jan. 8, 2008, and it is this version that is published here.

EXHIBIT B

“090325 WF826447 Price Q27 If a locality does not wish to participate in the Secure Communities.doc”

date / time created: unknown

QUESTIONS FOR THE RECORD SUBMITTED BY

CHAIRMAN DAVID PRICE

Michael Aytes, Acting Deputy Director,
United States Citizenship and Immigration Services
Marcy Forman, Director, Office of Investigations,
U.S. Immigration and Customs Enforcement
David Venturella, Executive Director, Secure Communities,
U.S. Immigration and Customs Enforcement
Priorities Enforcing Immigration Law

Criminal Aliens/Secure Communities

Question #27: If a locality does not wish to participate in the Secure Communities program, is it allowed to opt out?

ANSWER:

Yes. ICE does not require any entity to participate in the information sharing technology at the state or local level. ICE is entering into agreements with each state identification bureau to oversee the sharing of information between ICE and the state. Each of these agreements contains a clause allowing either side to suspend or terminate the use of the information sharing technology with 30 days written notice.

Rachel Canty (202) 732-9504
<insert OCR reviewer name and telephone number>
<insert CFO reviewer name and telephone number>
<insert OAS final clearance>

EXHIBIT C

“ISSUE--OPT OUT.doc”

date / time created: 9/1/2009 7:39 AM