



INSTITUTE FOR INTERGOVERNMENTAL RESEARCH

Emory B. Williams
Founder and Chairman

D. Douglas Bodrero
President

Post Office Box 12729
Tallahassee, Florida 32317-2729
Phone: (850) 385-0600
Fax: (850) 422-3529
www.iir.com

February 19, 2008

Colonel Michael Snyders
Deputy Director, Information Sharing Command
Illinois State Police
Post Office Box 19461
Springfield, IL 62794-9461

Dear Colonel Snyders:

As requested by the Illinois State Police (ISP), on December 12, 2007, Mr. John Wilson and Ms. Patty Dobbs from the Institute for Intergovernmental Research (IIR) conducted an on-site visit to review the Illinois Statewide Terrorism Intelligence Center (STIC). The purpose of the on-site visit was to discuss the requirements in 28 CFR Part 23 and their applicability to STIC databases and begin the process of evaluating the Illinois STIC for compliance with 28 CFR Part 23.

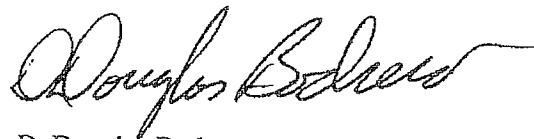
We have provided detailed information about existing operational policies and practices that appear to meet the requirements in 28 CFR Part 23 and those that do not. Details of the review and IIR's recommendations are outlined in the enclosure to this letter.

Please be advised that "official" opinions must come from the Office of General Counsel, Office of Justice Programs, U.S. Department of Justice, 810 Seventh Street, NW, Suite 5400, Washington, DC 20531. Rafael A. Madan is the General Counsel.

Colonel Michael Snyders
February 19, 2008
Page Two

A site visit survey is also enclosed for your completion. Please complete the survey and return it in the self-addressed, stamped envelope. If you have any questions or if we can be of further assistance, please do not hesitate to contact us at (850) 385-0600.

Sincerely,

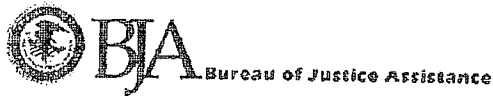
A handwritten signature in black ink, appearing to read "D. Douglas Bodrero". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

D. Douglas Bodrero

DDB:rs
ISP-STIC-SiteVisitRpt.docx

Enclosures

cc: Mr. David P. Lewis
Ms. Kathleen deGrasse



Technical Assistance Report

Evaluation of the Illinois State Police,
Statewide Terrorism Intelligence Center
in Relation to 28 CFR Part 23,
Criminal Intelligence Systems Operating Policies

February 19, 2008

Illinois State Police
Statewide Terrorism Intelligence Center

On December 12, 2007, Mr. John J. Wilson and Ms. Patricia Dobbs from the Institute for Intergovernmental Research (IIR) met with Colonel Michael Snyders, Deputy Director, Information Sharing Command; Mr. Boyd Butler; Mr. Aaron Schroeder; Mr. Kirk Lonbom; Mr. Alan Burgard; and Master Sergeant Kathleen deGrasse of the Illinois State Police (ISP), for the purpose of conducting an on-site visit to discuss the application of the provisions of 28 CFR Part 23 and to review the ISP Statewide Terrorism Intelligence Center's (STIC) criminal intelligence databases: Violent Crime Information Tracking and Linking (VITAL) and the gang criminal intelligence database. While at the fusion center, Mr. Wilson and Ms. Dobbs also met with Ms. Dora Tyrrell, STIC supervisor, and Mr. Randall Kesselring, Statewide VITAL coordinator. The STIC, Illinois's statewide fusion center, provides a 24-hour/7-day call-in center that provides immediate intelligence information to local, state, and federal law enforcement agencies on terrorism and major crimes, related suspects, and incidents.

The ISP requested the review to ensure that its major crimes and incidents database, VITAL, and its gang criminal intelligence database (which contains 96,000 records) are in compliance with 28 CFR Part 23. Colonel Snyders expressed his interest in ensuring that the ISP's criminal intelligence information system remains in compliance with the regulation, even though it is not subject to the regulation, because it is not supported with funds under the Omnibus Crime Control and Safe Streets Act of 1968, as amended (citation omitted).

While both ISP/STIC criminal intelligence information databases are used mostly for internal ISP/STIC purposes, the system allows for local agencies, FBI, and National Guard access through the STIC. The gang information database is currently stored as part of VITAL's Hot Files, which are designed for officer safety. ISP investigators or analysts make the determination of criminal predicate required of all submissions to VITAL. Each submission is approved by a supervisor.

In advance of the site visit, ISP provided IIR with copies of STIC Work Unit Directives STIC-004, Procedures for Inquiries; ISP Directive ADM-136, Crime Analysis; and STIC Standard Operating Procedures, SOP-108, Security Classifications of Information and Analytical Products. Subsequent to the site visit, the VITAL Operations Manual, updated May 16, 2003, was also provided.

Based on review of the provided documents and discussions with ISP staff, IIR is not able to determine whether or not ISP complies with 28 CFR Part 23 because the ISP has not formulated written VITAL/system operating policies and procedures that expressly address and incorporate the operating principles set forth in 28 CFR § 23.20. Given that, IIR recommends that ISP develop 28 CFR Part 23-compliant operating policies and procedures for any and all criminal intelligence information databases included in the VITAL system.

Several of the key operating principles in 28 CFR § 23.20 are addressed in the aforementioned documents. In particular, the STIC-004 Procedures for Inquiries and the VITAL Operations Manual state that criminal predicate/reasonable suspicion standard must be met for entry of a record, describe the levels of sensitivity and confidence and what combinations do or do not meet 28 CFR §23.20(g), and address what submissions may be rejected based on not meeting 28 CFR Part 23 requirements. What is missing is:

- The overlay policy statements that provide the framework for when, how, and why criminal intelligence information will be collected and stored;
- When and with whom it will be shared;
- The recipient's responsibility to safeguard the information (28 CFR § 23.20(f)((1)); and
- How often information in the system will be reviewed and validated or purged. It would be acceptable to reference the existing documents to illustrate how particular aspects of the operating principles are addressed and the policy operationalized, but the operational-level document is not adequate to express the policy principles of what can and cannot be done.

Sample operating policies can be found on the resource CD provided during the on-site visit or at the IIR Web site, www.iir.com. Also, the International Association of Chiefs of Police has a model policy available at www.iacp.org. Once a policy is developed, IIR is available to review it for compliance with 28 CFR Part 23.

Specific questions or issues raised and discussed during the site visit are outlined below.

- **Inclusion of Parolee Information in VITAL:** ISP representatives stated that the Illinois Department of Corrections provides a daily electronic transfer of information on all released parolees. This information is entered into VITAL, with a label of "parolee" attached to each name. IIR's review of this practice finds it to be acceptable. The Bureau of Justice Assistance's (BJA) 1998 policy clarification (*Federal Register*, December 22, 1998) clarifies that 28 CFR Part 23 allows non-intelligence information to be housed on the same system or network on which criminal intelligence information is housed, provided that a clear distinction can be made between what is criminal intelligence information and what is not criminal intelligence information. This distinction is made by ISP through the label of "parolee" attached to the information. Because VITAL is essentially a closed single-agency system, the users (ISP employees and trained local, state, and federal agencies) are aware that the label identifies the entry as fact-based non-intelligence information not subject to 28 CFR Part 23.
- **Retention of Link Between Records:** ISP presented a scenario in which the criminal link between two records can be maintained only if the record that links them is not purged—even when it has reached the end of its

retention period. IIR does not believe that the practice of retaining such a record to maintain the link meets 28 CFR Part 23 requirements. Each record must stand on its own merit (meeting 28 CFR Part 23 submission criteria). If the record that provided the link between two records is no longer valid and due for purge from the criminal intelligence system, purge is required even if the link will be lost. One option discussed was to maintain the linking record as a "dummy," with information identifying the subject removed from the linking record. ISP presented another scenario in which a parolee record links two criminal intelligence records together. The parolee name could be included in each criminal intelligence record as noncriminal identifying information, thus linking the two records.

- **Inclusion of Noncriminal Identifying Information:** BJA's 1998 Policy Clarification clarifies that 28 CFR Part 23 permits the inclusion of noncriminal identifying information in an existing criminal intelligence record as a searchable field. One of the caveats is that the information must be appropriately labeled to ensure that the user understands the purpose for which the noncriminal identifying information was included—identification of the criminal subject or the criminal activity. Even though VITAL is essentially a closed single-agency system, IIR suggests that ISP modify the system to clearly label noncriminal identifying information so there can be no misunderstanding or misperception about why an employer's or a relative's name is included in the criminal intelligence system.
- **Outside Audit:** ISP asked about who might be available to conduct an outside audit of its criminal intelligence system. IIR suggests that ISP contact the Law Enforcement Intelligence Unit (LEIU). LEIU has conducted this function for other agencies.

ISP should note that while the above analysis and conclusions as to the applicability of 28 CFR Part 23 to ISP's criminal intelligence information system are based on IIR's technical assistance role and experience with 28 CFR Part 23, they are not binding on ISP, BJA, or the Office of Justice Programs (OJP), and official opinions and policy interpretations of 28 CFR Part 23 must come from BJA or OJP, as appropriate.