Data Compliance Audit Report for the Minnesota Joint Analysis Center

June 1, 2010

Data Compliance Auditor:

John J. Wilson
Senior Research Associate
Institute for Intergovernmental Research

BACKGROUND

As detailed by the State Auditor and confirmed through my independent document review, the Minnesota Joint Analysis Center (MNJAC) was created by a Memorandum of Understanding (MOU) between a number of government agencies with law enforcement authority. The mission of MNJAC is "to collect, evaluate, analyze, and disseminate information regarding organized criminal, terrorist, and all-hazards activity in the state of Minnesota while complying with state and federal law to ensure the rights and privacy of all." To ensure protection of individual rights, the MNJAC Oversight Group created a committee to prepare a formal privacy policy, which was completed and approved by the MNJAC Oversight Group on July 28, 2008. The policy requires the Oversight Group to conduct audits to ensure no misuse of MNJAC's information systems.

In January of 2010, the Minnesota Bureau of Criminal Apprehension contracted on behalf of MNJAC with the Institute for Intergovernmental Research, of Tallahassee, Florida, for the services of Senior Research Associate John J. Wilson. The contract provides that Mr. Wilson audit MNJAC operations to assist the state in determining whether MNJAC operates in a manner that complies with federal laws and regulations governing the collection, use, retention, and destruction of data required to carry out its duties, to identify any deficiencies, and to make appropriate recommendations to resolve those deficiencies. The identified goals are to:

- Ensure that MNJAC complies with federal laws governing the collection, use, retention, and destruction of data;

- Review and assess MNJAC's business practices to help identify weaknesses and gaps in the protection of privacy, civil rights, and civil liberties;

- Make suggestions to improve the protection of privacy, civil rights, and civil liberties; and

- If the auditor has information about the business practices of other fusion centers, provide information about other ways to protect privacy, civil rights, and civil liberties.

The contract identifies issues to be addressed in the audit, which are addressed in the body of this report, followed by the auditor's findings. The period covered by the audit is July 28, 2008, through June 30, 2009. While this period covered records contained in the Crucible database, which was in operation until June 24, 2009, when MNJAC switched to a new case management system called ACISS, the auditor followed the submissions reviewed into the ACISS database in order to determine whether the latest entered Crucible submissions chosen for review by the auditor, many of which had not yet been reviewed or had their reviews completed by MNJAC staff, had been properly entered, labeled, and maintained in the new system.

In preparation for the audit, the auditor reviewed a variety of materials requested of and/or provided by MNJAC, including:

- MNJAC mission and vision statements and MOU creating MNJAC
- MNJAC Web site materials, including MNJAC priorities and statistics, the Intelligence Communications Enterprise for Information Sharing and Exchange (ICEFISHX) descriptions, MNJAC structure, operational descriptions, products and services, training and liaison activity, issues, funding, and goals and objectives
- MNJAC Privacy Policy Committee structure and functions and Director's Report
- MNJAC Privacy Policy (2008)
- MNJAC MOU with participating agencies
- MNJAC Operations Policy/Procedure Manual
- MNJAC Analytical Operations: Strategic Direction and Standard Operating Procedures
- MNJAC Analytical Operations: Report Management and Crucible
- MNJAC Analytical Operations: Report Management and ACISS, including Appendix A: ACISS Data Entry Procedures
- Determination of classification of data at MNJAC and authorization for the sharing of that data (January 5, 2009)
- Records Retention Schedule 09-141, May 6, 2009
- MOA between the U.S. Department of Homeland Security (DHS) and the Minnesota Department of Public Safety (DPS) (July 2008)
- Minnesota Government Data Practices Act

The auditor traveled to Minneapolis-St. Paul and conducted an initial meeting during the afternoon of March 29, 2010, with MNJAC Director Michael Bosacker, discussed the operations of MNJAC and the documents reviewed, toured the office, and met MNJAC staff members to discuss their roles and responsibilities. On March 30, 2010, the auditor conducted in-depth interviews with the training coordinator, operations management, and analytical staff; reviewed Crucible records in detail; and then reviewed these records as currently stored in the ACISS database. The auditor then discussed the results with MNJAC Analytical/Operations staff and the Director and identified tentative issues and recommendations.

IDENTIFIED ISSUES AND AUDIT FINDINGS

A. **Are the goals and scope of MNJAC clearly defined?**

Finding: The goals and scope of MNJAC are clearly defined in the MOU creating MNJAC and the vision and mission statements adopted by the Oversight Group on October 14, 2007.

B. **Is there an oversight body?**

Finding: The MOU created the Oversight Group to monitor MNJAC performance. The Oversight Group meets regularly to carry out its responsibilities.

C. **Does MNJAC management feel the oversight body provides sufficient review of the operation?**

Finding: This issue is appropriately addressed in the State Auditor's report.

D. **Does the oversight body believe it has adequate information to assess the performance of MNJAC, particularly concerning privacy, civil rights, and civil liberties?**

Finding: This issue is appropriately addressed in the State Auditor's report.

E. **Does MNJAC have a privacy policy?**

Finding: Yes (see recommendations).

F. **Was the privacy policy approved by the oversight body?**

Finding: Yes, it was approved by the Oversight Group on July 28, 2008.

G. **When was the policy last reviewed for possible revision?**

Finding: The policy was the subject of initial review and comment by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance's Privacy Policy Review Team prior to its adoption, and additional comments and suggestions were submitted to MNJAC in April 2009. However, the Global Justice Information Sharing Initiative (Global) Advisory Committee has subsequently approved a revised *Fusion Center Privacy Policy Development Template* (April 2010) to guide centers in achieving a comprehensive privacy, civil rights, and civil liberties protection policy that is eligible to be determined by DHS to be "at least as comprehensive" as the Information Sharing Environment (ISE) Privacy Guidelines. Such approval will facilitate the future flow of federal agency

terrorism-related information and intelligence to fusion centers (see recommendations).

H. **Were advocacy groups consulted in the development or most recent revision of the policy?**

Finding: This issue is appropriately addressed in the State Auditor's report. It is anticipated that privacy advocates on the Privacy Policy Committee will play a key role in reviewing and recommending revisions to the current MNJAC Privacy Policy.

I. **Is MNJAC in compliance with the following issues documented in the privacy policy?**

1. **Is the data that is collected and maintained supported by both reasonable suspicion of criminal conduct or activity and relevance?**

Finding: The auditor determined that there were 193 log entries from May 1, 2008, to June 24, 2009, in the Crucible databases—including requests for information (RFIs), inquiries for information/ photos/events, and suspicious activity reports (SARs) submitted via ICEFISHX, telephone, or other delivery mechanism. There were 788 ICEFISHX submissions between September 18, 2007, and June 24, 2009. The auditor confirmed that the Crucible and ACISS systems require that the four criteria specified in the privacy policy (Section III, 1–4, including source reliability, reasonable suspicion, lawfully collected, and accurate and current) be met. In addition, RFIs must be "in support of an ongoing criminal investigation, must have a criminal predicate, and product requests must have a defined need to know." There are currently approximately 500 case, RFI, SAR, and log files in the ACISS system.

The auditor reviewed a total of 32 of the most recent Crucible files, 29 of which were identified as suspicious activity reports or case files, and 3 of which were Terrorist Screening Center alerts. The suspicious activity reports and case files were followed into the ACISS database because many did not yet have a retention determination or were the subject of ongoing staff review when the changeover to ACISS occurred. For each file, either the completed entry in Crucible or the subsequent entry in ACISS documented that the four policy criteria were met for retention and that the retention period was in accordance with the approved MNJAC retention schedule (May 6, 2009). The schedule provides a five-year retention for case file information meeting 28 CFR § 23.20 (h) criteria, three years when an investigative subject is arrested, and one year for SAR information not meeting case file requirements (see recommendations).

Comment on Case #569, also reviewed by the State Auditor: I agree that the initial judgment that the photography at issue met the reasonable suspicion criteria was a close question due to the statement of one officer on the scene that he "did not believe that either of the men's stories or behavior was suspicious." However, another officer reported the incident as meeting SAR criteria. Consequently, I do not think the initial judgment to retain the information for one year was categorically wrong and note that the report was subsequently determined to be unfounded when considered for entry into ACISS.

2. **Is data about political, social, or religious views collected or maintained? If yes, is the data relevant to criminal conduct or activity?**

   Finding: There was no information in any of the files reflecting the political, religious, or social views of any criminal subject. Any such information received would not be maintained in MNJAC files unless it was relevant to the criminal conduct or activity (as provided by 28 CFR Part 23).

3. **Is data collected in a way that interferes with lawful political activities?**

   Finding: There was no information reviewed that pertained to political activities, hence no indication that information is gathered by source agencies or collected by MNJAC in a manner that would interfere with lawful political activities.

4. **Is data collected in a way that harasses a person or organization based on lawful political activities?**

   Finding: There was no information reviewed that had the appearance of harassment of individuals engaged in lawful political activity and no indication that information is gathered by source agencies or collected by MNJAC in a manner that harasses individuals engaged in lawful political activities.

5. **Was any data obtained in violation of law?**

   Finding: There was no indication in the files reviewed that any data was obtained in violation of law.

6. **Was any data obtained in violation of the Electronic Communications Privacy Act (ECPA) (Public Law 99-508)?**

   Finding: Compliance with the ECPA and any state law governing interception of electronic communications is a 28 CFR Part 23 requirement. Information in submissions reviewed was gathered as a

result of reports, interviews, and investigative activity that did not involve the interception of electronic communications subject to the ECPA.

7. **Are there sanctions for unauthorized access, utilization, or disclosure of data?**

Finding: The MNJAC Privacy Policy provides as follows: "The Oversight Group reserves the right to restrict the qualifications and number of personnel having access to MNJAC and to suspend or withhold service to any individual violating this *Privacy Policy*." "Use of the MNJAC's data in an unauthorized or illegal manner will subject the requestor to denial of further use of MNJAC, discipline by the requestor's employing agency, and criminal prosecution." "The MNJAC reserves the right to deny access to any MNJAC user who fails to comply with the applicable restrictions and limitations of the MNJAC policy."

The policy also provides that MNJAC personnel must agree to these provisions. The auditor confirmed that as of March 12, 2010, the form signed by personnel includes wording recommended by the State Auditor and that all current MNJAC personnel have signed the new form.

8. **Have active files with personal identifiers been reviewed by the Operations Manager or designee every 180 days to determine whether they should remain active?**

Finding: Although the Crucible system did not require automatic review after 180 days, there was a field to track manager review, which was kept current. Under ACISS, review notification is automatic and the information is presented for management review and approval prior to any further dissemination or use of the file.

9. **Are MNJAC data and information resources secure?**

Finding: As noted by the State Auditor, MNJAC data systems and electronic communications systems are managed by the Bureau of Criminal Apprehension (BCA) information technology staff, using BCA's high-level data security requirements. BCA controls and administers MNJAC's servers. Systems are password-protected and accessible only from authorized computers located in the MNJAC facility. Paper files are limited to grant and personnel files.

The State Auditor raised security issues related to the use of USB flash drives and compact discs and use of individual codes for building access. The Director's January 29, 2010, response to these issues was sufficient and was discussed during the exit interview. All security

procedures were in place and followed during the data compliance auditor's time at the facility, including being escorted while entering, being present in, and exiting the facility.

a. **Is unauthorized access or use forbidden?**

Finding: Yes. In addition, MNJAC is subject to periodic and random BCA audit as a remote terminal agency to ensure that BCA information is accessed and used for proper purposes.

b. **Is the access to resources outside MNJAC secure?**

Finding: Yes, Access to outside resources is over the secure BCA network, with access to the Minneapolis records system through a password-protected Web portal. Access to participating agency records is through a password-protected VPN link.

c. **Is there training for staff about password protection?**

Finding: Internal training for MNJAC staff includes password protection as part of annual DHS security training. Meticulous electronic records are kept of staff training, including dates and subject matter.

10. **Is there training for staff on how to appropriately handle data?**

Finding: All MNJAC staff are required to complete and have completed 28 CFR Part 23 online training. This training includes information on protecting privacy, civil rights, and civil liberties, as does other training provided to staff, including periodic training on the Minnesota Data Practices Act. Data privacy training is required of all staff on an annual basis.

Management staff tracks changes in laws, policies, and practices that involve the protection of privacy, civil rights, and civil liberties and incorporates these changes into internal staff training.

11. **Are queries to MNJAC data applications logged?**

Finding: The Crucible system tracked the date and time of all access to a case file, including identification of the user. ACISS identifies data entry to files and establishes an electronic audit trail that identifies each time and by whom a file is queried. Each RFI must indicate a reason for the request that is related to a valid law enforcement purpose by a user from an agency with a right to know the information and a user with a need to know the information in the performance of an authorized law enforcement activity.

12. **Is there a secondary dissemination log?**

    Finding: Yes. MNJAC maintains a secondary dissemination log as indicated above and confirmed through review of Crucible files, ACISS system-description information, and staff discussions. Dissemination of secure data is limited to law enforcement agencies with a right to know and individual users from those agencies with a need to know. The Crucible system logs the date of release; the subject of the data; the identity, e-mail address, and telephone number of the recipient; a file number for the data released; and the purpose of the release. The ACISS system has the capability to provide all this information to management upon request, but all such information is not displayed as part of the file.

RECOMMENDATIONS

MNJAC personnel consistently displayed a high level of professionalism, dedication, commitment to the work of the agency, and sensitivity to the need to conduct MNJAC operations in a manner that complies with applicable privacy, civil rights, and civil liberties law, policy, and procedure in order to maintain the trust and confidence of the citizens of Minnesota. Minnesota's data practice requirements are among the strictest I have seen, yet the MNJAC appears to be providing a consistently high level of critical information and intelligence to its participating jurisdictions. My recommendations, based on 28 CFR Part 23 and best practices of other jurisdictions, are as follows:

1. MNJAC should update its July 2008 privacy policy to reflect the issues and standards contained in the recently published *Fusion Center Privacy Policy Development Template* (Global Advisory Committee, April 2010), including reformatting the policy to follow the logical flow-based structure of the Template rather than the Fair Information Practices. This should include addressing the ISE Privacy Guidelines requirements for the sharing of terrorism-related information and the provisions related to the SAR/ISE-SAR process, expanding the Definitions section of the policy, and considering the Best Practices identified in the Template.

2. Once the privacy policy is drafted, determined by the DHS Privacy Office/Privacy Guidelines Committee to be "at least as comprehensive" as the ISE Privacy Guidelines, MNJAC should become a participant in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI is being implemented in a phased manner in all 72 designated fusion centers by the Program Management Office for the NSI. The goal is to complete implementation by the end of federal fiscal year 2012. The system is decentralized, allowing each center to maintain control of its terrorism-related SARs. Further, no center or agency can participate unless it has an approved privacy, civil rights, and civil liberties protection policy in place.

3. It is recommended as an interim measure that MNJAC revise its suspicious activity reporting form to clearly reflect behaviors that are deemed to be potentially terrorism-related and "other" types of criminal activity (gang, drug, etc.) that are not terrorism-related. Alternatively, the form could continue to provide a broad menu of behaviors (which should include an "Other: Describe_____" category) and have a separate box to check if the source agency has determined that that behavior may be terrorism-related. Further, I suggest that the terrorism behaviors mirror the research-based terrorism-related behaviors identified in the ISE-SAR Functional Standard (Version 1.5), which can be found at http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE_SAR_Functional_Standard_V1_5_Issued_2009.pdf.

4. It is recommended and was discussed with the Director and staff during the on-site review that the ACISS system be reconfigured to provide the capability to reflect confidence codes (source reliability and content validity) for criminal intelligence information, including suspicious activity reports, which, under MNJAC requirements (Retention Schedule 09-141, May 6, 2009), must meet reasonable suspicion in order to be retained as a "permanent" file (up to five-year retention) rather than as a "temporary" file (up to one year). It was discussed that implementing this suggestion would require BCA programming assistance and support.

5. Finally, it is recommended that MNJAC formally adopt the "reasonable indication" standard set forth in the ISE-SAR Functional Standard (Version 1.5) for electronic records of SARs that do not meet the reasonable suspicion standard for creation of a case file (one-year retention under Schedule 09-141, Item No. 2A, May 6, 2009. This would ensure that these "temporary" SARs are retained or shared based on behavior that has been documented and reviewed to determine that it is reasonable to conclude that it may be related to criminal activity, including terrorism. It is a standard that is based on more than a "hunch" or "bare possibility," sometimes referred to as "mere suspicion," but which may be less than "reasonable suspicion."

RESPECTFULLY SUBMITTED:

John J. Wilson
Data Compliance Auditor
June 1, 2010