Minnesota Fusion Center

Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy

Minnesota Fusion Center
Minnesota Bureau of Criminal Apprehension
04 March 2021

TABLE OF CONTENTS

I. MINNESOTA FUSION CENTER MISSION

The Minnesota Fusion Center (MNFC) is the state designated fusion center. The MNFC's purpose is to allow participating agencies to share information about suspected criminal and terrorist activity. Fusion centers provide an environment where stakeholders collaboratively work together gathering information, analyzing data, and sharing information to improve the ability to fight crime and terrorism locally, regionally, and nationally.

The mission of the MNFC is to collect, evaluate, analyze, and disseminate information regarding organized criminal, terrorist, and all-hazards activity in Minnesota, while complying with state and federal law to ensure the rights and privacy of all. A process of information collection, integration, evaluation, analysis, and dissemination is used for law enforcement purposes and in the interest of public safety. The information is made available to law enforcement agencies and certain other entities consistent with Minnesota Statutes Chapter 13, 28 CFR part 23, and other applicable state and federal law.

II. PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES (P/CRCL) POLICY PURPOSE

The MNFC recognizes the importance, and will ensure the protection, of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the information gathering and sharing process. This P/CRCL policy states the legal requirements that will be met as well as the organizational procedures that will be used to ensure that these rights and interests are protected.

III. GOVERNANCE AND OVERSIGHT

The MNFC is part of the Investigations Division within the Minnesota Bureau of Criminal Apprehension (BCA) and is controlled by the BCA's Superintendent. The MNFC is a law enforcement agency for purposes of Minnesota Statutes Chapter 13.

The BCA's Superintendent is responsible for the operation of the MNFC. To provide daily operational direction and ensure compliance, the Superintendent designated a Director for the MNFC. The Director is responsible for the MNFC's overall operation.

In order to preserve privacy, civil rights, and civil liberties, the MNFC works to ensure that safeguards and sanctions are in place to protect personal data in conformance with Minnesota Statutes Chapter 13 and other applicable law.

The MNFC has examined and recommended National Fusion Center Association best practices the MNFC follows for the collection, use, and security of information and technology, as well as accountability guidelines for the management of the information. The MNFC's P/CRCL Policy incorporates fair information practices and principles.

The Director will designate an individual to serve as the MNFC Privacy Officer. The MNFC Privacy Officer will be responsible for information privacy issues, including implementation of P/CRCL Policy requirements. The MNFC Privacy Officer will facilitate an annual review and update of the privacy policy and the MNFC Director will be involved in the review and update process.

The MNFC Privacy Officer will serve as a point of contact and coordination for alleged data or information errors, complaints, privacy policy violations, and liaison for the Information Sharing Environment (ISE). The MNFC Privacy Officer will coordinate conflict resolution under MNFC's redress policy and enforcement and sanctions outlined in the Accountability and Enforcement section of this policy (see section XV).

The MNFC Privacy Officer has been and will continue to be trained relative to privacy laws and recommended best practices. The Privacy Officer can be contacted at the following address: MNFC.PrivacyOfficer@state.mn.us. A staff attorney within the BCA will work with the MNFC to ensure that privacy and civil rights are appropriately protected by the MNFC's information acquisition, dissemination and retention practices.

IV. POLICY APPLICABILITY AND LEGAL COMPLIANCE

All MNFC personnel, which includes participating agency personnel, private contractors, and other authorized individuals, including those state employees providing technical services with direct access to MNFC databases, are required to abide by this P/CRCL Policy. These individuals and any other recipient of MNFC information must also follow all applicable laws which govern the treatment of the information the MNFC collects, receives, maintains, archives, accesses, discloses, or disseminates, including information within the ISE. See the MNFC Memorandum of Understanding, attached as Appendix B. In addition, Stakeholder Agencies receive information from the MNFC through a web portal. The notice participants receive when utilizing the web portal is attached as Appendix C.

The MNFC will make a printed or electronic copy of this policy available to all MNFC and non-MNFC personnel who provide services. All individuals will be required to provide both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy. Nothing in this policy is intended to create a private right of action for any member of the public or alter existing or future federal and state law requirements.

The MNFC has adopted internal operating procedures that are in compliance with all federal and state laws that protect privacy, civil rights, and civil liberties.

The laws referenced in this policy are listed in Appendix D.

V. INFORMATION

All personal data collected by the MNFC, regardless of whether it meets the reasonable suspicion standard in 28 Code of Federal Regulations Part 23, will be retained in compliance with the operating policies of that federal regulation, Minnesota Statutes

Chapter 13 (The Minnesota Government Data Practices Act), the approved MNFC Minnesota Records Retention Schedule (currently 09-141 and 012-014), and any other applicable federal or state laws governing information practices. The MNFC will strive to follow guidelines established under the National Criminal Intelligence Sharing Plan (NCISP) and, to the extent they do not conflict with Minnesota law, the privacy principles put forth in the Organization for Economic Co-operation and Development's Fair Information Practices.

A. COLLECTION REQUIREMENTS

Information collected by the MNFC should meet all of the following requirements:

1. The source of the information is reliable and verifiable;
2. The information supports a reasonable suspicion that the individual or organization is involved in criminal conduct, and the information is relevant to that conduct;
3. The information was collected in a lawful manner; and
4. The information is accurate and current.

The MNFC will retain Suspicious Activity Reports (SARs) that do not meet the reasonable suspicion threshold for one (1) year to permit the possible development of reasonable suspicion. If reasonable suspicion is not developed during that year, the SARs are purged as required by the MNFC approved records retention schedule (Appendix E). During the year, these SARs are stored as temporary files and are disclosed as required or permitted by law. If disclosed, they are clearly labeled as a SAR that does not meet the reasonable suspicion standard. SARs are stored in the MNFC Database with the other MNFC data and so the SARs are secured in the same way as all other data.

The MNFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents into the processes and systems used to manage all other MNFC information. The MNFC identifies and reviews protected information that may be disclosed by the MNFC prior to sharing it through the ISE and provides notice through data field labels to enable authorized users to determine the nature of the information and how to handle it in accordance with applicable legal requirements.

The MNFC will abide by daily operating procedures for the initial collection and verification of information, including the screening process used by an analyst to develop how the four criteria above are met. There is a subsequent review by the Operations Manager or the Operations Manager's designee to substantiate the analysis and to approve the documentation that has been developed. SARs that do not meet all the above standards will not be retained for more than one year. The four criteria above also apply to BCA Case Files. If the criteria are not met, the MNFC will not open a BCA Case File.

A Request for Information (RFI) may meet all four of the criteria above. An RFI may also involve a request that is supported by a homeland security concern, rather than a reasonable suspicion of criminal activity. If homeland security concerns support the RFI, then all of the other criteria above must be met.

Lawfully collected information that meets MNFC's P/CRCL Policy will be stored in the MNFC database. All information is managed according to the approved records retention schedule. When the information describes an individual or organization involved in activities protected by the First Amendment, the information cannot be maintained unless there is specific indication that the individual or organization has, is about to, or has threatened to engage in conduct that constitutes a crime and the First Amendment activities are relevant to the criminal conduct. Specifically excluded material includes:

1. Information on an individual or group merely on the basis that such individual or group support unpopular causes;
2. Information on an individual or group merely on the basis of race, gender, age, citizenship, disability, sexual orientation, place of origin, or ethnic background;
3. Information on an individual or group merely on the basis of religious or political affiliations, or beliefs;
4. Information on an individual or group merely on the basis of personal habits and/or predictions that do not break any laws or threatens the safety of others; or
5. Information obtained in violation of any applicable federal or state rules or statutes.

All MNFC information is managed through the MNFC database and under the direction of the Operations Manager. Open files will be reviewed no less frequently than every 180 days by the Operations Manager or Operations Manager's designee to determine the file's status and whether it should be changed. A yearly records review of the MNFC database will be conducted by the Operations Manager and records that may be disposed of will be purged. Additional information about records destruction can be found in Section XIV of this policy.

On receipt of information, MNFC personnel will assess the information to determine its nature, usability, and quality and assign it to an operating file (See B, below). At the time a decision is made to retain information, including contributing ISE-SAR information to the shared space, MNFC personnel will label it (by record, data set or system of records and to the extent feasible, consistent with the current version of the ISE Functional Standard for SAR), pursuant to applicable limitations on access and disclosure in order to: protect an individual's right of privacy, civil rights, and civil liberties; protect confidential sources, law enforcement undercover techniques and methods; prevent interference with or

the compromise of pending criminal investigations; and provide any legally required protection based on the classification of the data.

B. TYPES OF OPERATING FILES

There are three types of operating files within the MNFC. They are:

1. BCA Case File: A BCA Case File is created when the Operations Manager determines that one should be created. A BCA Case File is entered in the MNFC Database and a BCA case number is automatically generated.
2. Request for Information (RFI): An RFI must be supported by a reasonable suspicion of criminal activity or homeland security concern that is provided to the MNFC. MNFC personnel cannot answer an RFI unless it contains an appropriate predicate.
3. Suspicious Activity Report (SAR): A SAR will be entered into the MNFC Database. A SAR should be reported to the MNFC by a law enforcement entity or security related to a CIKR site once it has been reported to a local law enforcement agency. The MNFC receives SARs by the following means:
    - The secure information-sharing platform
    - Fax
    - Telephone
    - Email

C. LABELS

The MNFC requires certain basic descriptive information to be entered and electronically associated with information, including terrorism-related information and that information shared through the ISE, for which there are special laws, rules, or policies restricting access, use, and disclosure. The types of information include:

- The name of the submitting agency;
- The name of the justice information system from which the information is disseminated or that the information was disseminated from the MNFC database;
- The date the information was collected and, where feasible, the date its accuracy was last verified;
- The title and contact information for the person to whom questions regarding the information should be directed.

The MNFC will attach specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate whether the information is Protected Information and any legal restrictions on information sharing based on information sensitivity or classification. The MNFC will keep a record of the source of all information sought and collected by it.

VI. ACQUIRING AND RECEIVING INFORMATION

The MNFC and participating agencies will inform the public about information collection practices and comply with Minnesota Statutes Chapter 13.

Information obtained from or through the MNFC can only be used for official and lawful purposes. A lawful purpose means the request for information can be directly linked to a law enforcement agency's active criminal investigation, is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety, and is in compliance with Minnesota Statutes Chapter 13 disclosure requirements. This includes disclosing records to those responsible for public protection, public safety, or public health in the performance of official duties when permitted by Minnesota law. An audit trail sufficient to allow the identification of individuals to whom such records are disclosed and the nature of the information disclosed will be kept by the MNFC.

The information maintained by the MNFC is obtained through participating agencies, Stakeholder Agencies, federal agencies, and open source resources. Individual users of MNFC information are solely responsible for the interpretation, further dissemination, and use of information developed in the research process. Additionally, it is the responsibility of the user to ensure the accuracy, validity, completeness, and security of all information obtained prior to official action being taken.

External governmental agencies that access and share information with the MNFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

The MNFC will contract with commercial database entities that provide an assurance that their methods for gathering personal data comply with applicable state and federal laws, and that these methods are not based on misleading information collection practices.

The MNFC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual or information provider who is legally prohibited from obtaining or disclosing the information,or;
- An individual or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or MNFC policy.

VII. INFORMATION QUALITY ASSURANCE

The MNFC is required by Minn. Stat. §13.05, subd. 5 to assure that data are accurate, complete, current and secure. The MNFC will make every reasonable effort to ensure that standard is met and that information is merged with other information about the same individual or organization only when the applicable standard outlined in the Merging Records (section IX) of this policy has been met.

MNFC personnel will determine the accuracy of information received through database searches, by cross-checks with other data systems and open source information. At the

time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

Information files will be labeled to protect sources, investigations, and an individual's right to privacy, as well as to control access to information.

Classification and data labeling shall be reevaluated whenever new information is added to an existing file.

The MNFC ISE-SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Participating Agency personnel, including MNFC personnel, will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism. This training will also be made available to law enforcement officers around the state.

The MNFC ISE-SAR process includes safeguards so that only information about incidents and behaviors that indicate criminal activity related to terrorism but without personal identifiers are documented and shared through the ISE. These safeguards will ensure that the unintentional or inadvertent disclosure of information that could violate civil rights or civil liberties does not occur.

When a choice of investigative techniques is available, information, including information documented as a SAR, should be acquired or investigated using the least intrusive feasible means, taking into account the effect on individual privacy and potential damage to reputation. The MNFC will also adhere to this standard although it is not an operational agency conducting investigations.

A. **Source Reliability:** The source is the person or agency who gives MNFC the information. The source's reliability is evaluated according to the following:

1. *Reliable* means the source is unquestioned or has been tested in the past. All law enforcement agencies are classified as completely reliable.
2. *Usually Reliable* means the majority of the information provided by the source in the past has proved to be reliable.
3. *Unreliable* means the source has provided reliable information sporadically in the past.
4. *Unknown* means the reliability of the source cannot be judged. The authenticity or trustworthiness of the source has not yet been determined by either experience or investigation.

B. **Content Validity:** The validity of information is an indicator of the accuracy or truthfulness of the information. The validity of the information is assessed as follows.

1. *Confirmed* means the information has been corroborated by an investigator or another reliable, independent source.

2. *Probable* means the information is consistent with past accounts.
3. *Doubtful* means the information is inconsistent with past accounts.
4. *Cannot Be Judged* means the authenticity of the information has not yet been determined by either experience or investigation.

C. **Classification**: The MNFC uses two classifications or sensitivity structures since the MNFC maintains federal, state, and local data and information. Classification or sensitivity levels control the handling, dissemination, and release of materials and products. The laws that govern access to and classification of information at the federal level and in other states are different from Minnesota law.

When determining classification and sensitivity, MNFC personnel must determine whether there is a federal law that requires restrictions on access to or dissemination of the data or information or if Minnesota law applies.

When labeling case files and information, MNFC personnel may use one or more of the following:

1. Federal Classifications
   a) *Classified (not public):* document is restricted to individuals who have a security clearance of Secret or higher.
   b) *Unclassified/Law Enforcement Sensitive (LES) (not public):* document is viewable by law enforcement agencies only with the right to know and need to know. The document may contain information related to sources, methods, evidence, and active investigations.
   c) *Unclassified/For Official Use Only (FOUO) (not public):* document is viewable by anyone who is authorized under “Official Use Only” status. User has a right to know and a need to know. The document is not disseminated to or viewed by the general public or media.
2. Minnesota Classifications: The Minnesota Government Data Practice Act, Minnesota Statues, Chapter 13, contains the presumption that all government data are public unless there is a federal law or state statute that classifies the data. The following are Minnesota data classifications.
   a) *Private data* on individuals are about living human beings, not accessible to the public but are accessible by the individual data subject. An individual may consent to the release of private data to a third party. A statute may also authorize the dissemination of private data on individuals to a third party.
   b) *Confidential data* on individuals are not accessible to the public or the individual data subject. Confidential data on individuals

can only be shared with those that have statutory authority to have access.

c) *Nonpublic data* are about anything that is not a living human being, are not accessible by the public and are accessible by the subject of the data. The subject can consent to the release of the data to a third party. A statute may also authorize the dissemination of nonpublic data to a third party.

d) *Protected nonpublic data* are about anything that is not a living human being and are not accessible to the public or the subject of the data. Protected nonpublic data may be shared with those that have statutory authority to have access.

D. **MNFC Data Quality Standards:** In addition to using the labels and classification structures listed above, MNFC personnel will utilize the following standards to ensure that data quality is maintained:

1. The MNFC investigates, in a timely manner, alleged errors and deficiencies and corrects, deletes, or refrains from using information found to be erroneous or deficient.
2. The labeling of retained information will be reevaluated by MNFC when new information are gathered that have an impact on the confidence (source reliability and content validity) of previously retained information.
3. The MNFC will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when it learns that the information are erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.
4. Originating agencies are responsible for the quality and accuracy of the information accessed by or provided to the MNFC. The MNFC will advise the appropriate contact person in the originating agency, in writing, if its information is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.
5. When information is found to be inaccurate, incomplete, out of date or unverifiable, the MNFC will notify recipient agencies in writing and will maintain documentation of the notification.

VIII. COLLATION AND ANALYSIS

Access to the MNFC information sources for the purpose of analysis is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the MNFC will be granted only to fully authorized personnel who have been screened with state and national fingerprint-based background checks, as well as any additional background standards that may be established by the Superintendent of the BCA or the MNFC Director. Access to federally controlled

classified information and systems are based on the individual user's federal security clearance and need to know.

Information subject to collation and analysis is identified in the above Information section (section V).

The MNFC provides a central clearinghouse for information sharing, focusing on homeland security, organized criminal activity, and all-hazards within and surrounding the state of Minnesota. The MNFC will accomplish this through:

- Management and development of information sharing through the MNFC-approved web portal;
- Production and dissemination of bulletins and assessments;
- Investigation and analysis of suspicious activity reports in support of criminal investigations;
- Response to RFIs;
- Collaboration with federal, state, tribal, and local agencies to produce joint products;
- The coordination and facilitation of regional training opportunities in support of the MNFC mission; and
- The identification of crime patterns and trends.

The MNFC requires that all analytical products be reviewed to ensure that the appropriate privacy, civil rights, and civil liberties protections are met prior to dissemination or sharing by the MNFC.

IX. MERGING RECORDS

Multiple records about an individual may be merged when reasonable steps indicate that they are about the same person. Data elements that are used to determine that the same individual is the subject of the multiple records include the name (full or partial) and one or more of the following:

- date of birth;
- state identification number issued by the BCA (SID);
- offender identification number issued by the Minnesota Department of Corrections (OID);
- fingerprints;
- photographs;
- physical description;
- height;
- weight;
- eye and hair color;
- race;
- ethnicity;
- scars, marks or tattoos;
- Social Security number;

- driver's license number;
- DNA profile;
- retinal scan; and
- facial recognition.

The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

If the matching requirements are not fully met but there is a partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

X. USE OF INFORMATION BY THE MNFC

Information obtained from or through the MNFC can only be used for official and lawful purposes. A lawful purpose means the Request for Information can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety.

The MNFC will use Information on a need-to-know basis, and in accordance with applicable laws.

Credentialed, role-based access criteria will be used by MNFC, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

MNFC personnel who have access to MNFC information will be trained as to those regulations and agree to the following:

A. Individual passwords will not be disclosed to any other person, except as authorized by MNFC management.
B. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
C. Background checks will be completed on personnel who will have direct access to the MNFC and consistent with BCA policy.
D. Use of the MNFC data in an unauthorized or illegal manner will subject the requestor to denial of further use of the MNFC; discipline by the requestor's employing agency, and/or criminal prosecution.

Access to or disclosure of records retained by the MNFC will be provided only to persons authorized to have access, and only for legitimate law enforcement or public safety purposes necessary for the performance of official duties. An audit trail sufficient to allow the identification of each individual who accessed information retained or distributed by the MNFC will be kept by the MNFC.

The MNFC reserves the right to deny access to any MNFC user who fails to comply with the applicable restrictions and limitations.

The MNFC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting process, as that is defined in this policy as an ISE- SAR. This includes the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

XI. DISCLOSURE OF INFORMATION OUTSIDE THE MNFC

There are four regular briefs that are produced and disseminated by the MNFC which will follow all classification procedures:

A. *The Law Enforcement Brief (LE Brief)* is a law enforcement sensitive brief compiled from MNFC information, and other federal, state, tribal, and local reports that may contain comprehensive law enforcement data. This brief is disseminated to law enforcement personnel who are vetted by MNFC staff.

B. *The Partner Brief* is a non-law enforcement sensitive information brief complied from open sources and other federal, state, tribal, and local reports. A Partner Brief may contain Unclassified/For Official Use Only documents and materials. This brief is disseminated to first responder, government, and private sector personnel, along with designated law enforcement personnel.

C. *The Training Bulletin* is an unclassified document sent to all registered members of the MNFC. The Training Bulletin contains information regarding upcoming training opportunities within the Minnesota area of responsibility. Information contained includes course descriptions, registration instructions, and contact information for the training opportunities.

D. *The Violent Offender Release (VOR) Brief* is a law enforcement sensitive brief compiled with the support of the Minnesota Department of Corrections, sent through MNFC communication channels to vetted MNFC law enforcement partners. Information includes offender names and photos, offense information, monikers, and release addresses.

No briefs or assessments can be disseminated outside of the MNFC unless reviewed and approved for dissemination by the MNFC Operations Manager, the MNFC Director, or a designee. When reviewing briefs and assessments, particular attention will be focused on content, classification, and compliance with this policy. All attached documents will have the permission of the originating agency for use prior to inclusion in the brief or assessment, and dissemination will be limited to Stakeholder Agencies.

Documentation of the review and approval will be maintained within the disseminated product.
All information that is disclosed shall be recorded within the MNFC Database along with the identity of the recipient. A Stakeholder Agency may not re-disclose information from the MNFC until it has received permission from the MNFC.

Access to the MNFC Database requires authorization from the BCA and the issuance of a user name and password. It is fully auditable and tracks record access.

XII. REDRESS

A. Disclosure to a Data Subject

An individual who is the subject of data at the MNFC has a number of rights that are found in Minn. Stat. §13.04, subd. 3. Those rights include the right to know data exist, to inspect the data at the MNFC, to have copies of the data, and to have the meaning of the data explained. When data are classified as private, the MNFC must verify the identity of the individual data subject using one of the identification methods specified in the BCA's data practices policies and procedures. The MNFC must respond to an individual data subject within ten (10) working days of receipt of a data request for data about that individual.

The BCA's Data Practices Policies and Procedures are available at: https://dps.mn.gov/divisions/bca/Pages/your-data-rights.aspx.

A record of these disclosures is kept by the MNFC.

B. Disclosure to the Public

The public has the right to access public data maintained at the MNFC. See Minn. Stat. §13.03, subd. 3. The rights granted by section 13.03 include the right to inspect, to have copies and to have the meaning of the data explained. The MNFC is required to respond in an amount of time that is appropriate, prompt and reasonable. See Minn. Stat. §13.03, subd. 2(a) and Minn. Rules 1205.9300, subp. 3. The MNFC keeps a record of these disclosures.

All media requests shall be forwarded to the Director for referral to the BCA's Public Information Officer.

C. Corrections

An individual data subject is authorized by Minn. Stat. §13.04, subd. 4 to challenge the accuracy and/or completeness of public or private data. The terms "accuracy" and "completeness" are defined in Minn. Rules 1205.1500, subp. 2. Section 13.04, subd. 4, which requires any challenge to the accuracy or completeness of data to be made to the "responsible authority." MNFC's responsible authority is the Commissioner of the Department of Public Safety.

The Commissioner of Public Safety has 30 days to respond to a data challenge and either change the data or indicate that the data are accurate or complete. If the individual data subject does not agree with the Commissioner's determination, the individual has the right to appeal the determination to the Commissioner of Administration.
The appeal process is described in Minn. Rules 1205.1600.

A record will be kept of all requests for corrections and the resulting action, if any.

D. Complaints

If an individual has a complaint about the accuracy or completeness of terrorism-related information that is:

- classified as confidential by state or federal law;
- is held by the MNFC; and
- allegedly has resulted in demonstrable harm to the complainant,

a complaint may be filed with the MNFC Privacy Officer. The terrorism-related information in the MNFC Database that can be remedied under this paragraph will be identified.

On receipt of the complaint at MNFC.PrivacyOfficer@state.mn.us, the Privacy Officer will acknowledge the complaint and will state that the complaint will be reviewed. If the complaint includes a request from the individual to know if confidential data exist, the Privacy Officer will, following appropriate identification of the individual, as required by Minn. Stat. §13.04, subd. 3, coordinate the response with appropriate BCA personnel.

If the information originated in another agency, the Privacy Officer will give written notification of the complaint to that agency. That notification will occur within 10 business days of receipt of the complaint. The Privacy Officer will ask that the complaint be investigated and the MNFC informed within 30 days whether changes need to be made to make the information accurate or complete.

On receipt of the complaint, information held at the MNFC that are covered by this paragraph will be flagged as having an outstanding complaint and the fact that a complaint has been made will be shared with any party to whom the information is disclosed.

If there is no resolution within 30 days, MNFC will not further share the information until such time as the complaint has been resolved. Once the complaint has been reviewed and a determination made to change the information or that it is accurate or complete, the flag will be removed and any recipients of the information notified of any change in response to the complaint.

A record of complaints and the resulting action taken will be kept by the MNFC.

E. MNFC Principles

Information gathered or collected and records retained by MNFC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed without prior notice to the originating agency unless disclosure is required by law.
- Disclosed to persons not authorized to access or use the information.

MNFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

XIII. SECURITY SAFEGUARDS

The Superintendent, the MNFC Director, or their designee, will identify the technical resources to establish a secure facility for MNFC operations with restricted access, security cameras, and alarm systems to guard against an external breach of the facility. In addition, the Superintendent or their designee will identify the technological support for secure internal and external safeguards against network intrusion of MNFC information systems.

Access to the MNFC database from outside of the facility will only be allowed over secure network lines.

MNFC information will be maintained in so that it cannot be stored, modified, destroyed, accessed, or purged without prior authorization.

The Director will designate and ensure training of the MNFC's Security Officer.

Access to MNFC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and possess an appropriate security clearance, if applicable; and who have been selected, approved and trained accordingly.

Classified information will only be stored on electronic systems or in a safe explicitly approved for classified processing or storage by the U.S. Department of Homeland Security, the FBI, or DPS/BCA as appropriate to the system or information.

SARs information will be stored in the same system as that for all other data, but will be clearly labeled as to its classification when disclosed. This system is compliant with 28 CFR Part 23 security requirements.

All MNFC documents or software will be stored on MNFC computer systems or storage devices and in compliance with DPS/BCA policies. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publically available information.

Minnesota law requires that if a breach of the security of private or confidential data occurs, the state agency that maintains the data must notify the individuals whose data

were disclosed. Methods of notice are provided for in the statute along with the ability, in the appropriate circumstances, to delay notification to permit an active criminal investigation to occur without impediment. Minn. Stat. §13.055.

XIV. INFORMATION RETENTION AND DESTRUCTION

The Minnesota Records Management Act, Minn. Stat. §138.17, requires that an approved records retention schedule be in place before records can be destroyed. An approved records retention schedule for MNFC records is in place and authorizes the destruction of certain records. The retention period varies by record series type. For any records series not on the approved records retention schedule, approval would need to be received before destruction could occur. That approval could be in the form of a new approved records retention schedule or a one-time permission from the State Records Disposition Panel to destroy records that are no longer collected. See Appendix E for a copy of the approved records retention schedule.

The MNFC database is the record of information to be reviewed for retention or destruction. Destruction occurs in a secure manner appropriate to the classification or sensitivity of the information. Thus, if information is classified as something other than public, secure destruction, such as shredding, must be used. Destruction must also be in compliance with state policies governing destruction of electronic information. The MNFC does not notify the originating agency, if any, when destruction occurs, nor is originating agency approval required. A records destruction report is required by state law. Minn. Stat. §138.17.

XV. ACCOUNTABILITY AND ENFORCEMENT

The MNFC will make this Privacy, Civil Rights, and Civil Liberties Policy available for public review, including posting it on the BCA public website: https://dps.mn.gov/divisions/bca/bca-divisions/investigations/Pages/MNFC.aspx.

The MNFC Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system. The Privacy Officer can be contacted at the following address: MNFC.PrivacyOfficer@state.mn.us.

Queries made to the MNFC Database will be auditable and be logged, identifying the user initiating the query. MNFC information application logs will be made available for audit. When information is disseminated outside of the MNFC, a secondary dissemination log will be created in order to capture updated information and provide an appropriate audit trail, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for investigative purposes or to other agencies as provided by law.

The MNFC secondary dissemination log will include:

A. Date of release;
B. The subject of the information;

C. To whom the information was released, including address and telephone number;
D. An identification number or other indicator that clearly identifies the information released; and
E. The purpose for which the information was requested.

The Commissioner of Public Safety, Assistant Commissioner of Public Safety, and the BCA Superintendent, or their designee will be responsible for conducting or coordinating annual and random internal or external audits and for investigating misuse of MNFC's information systems. All confirmed or suspected violations of MNFC policies will be reported by MNFC personnel and other authorized users to the MNFC Privacy Officer, who will investigate them and report confirmed violations to the Director and to the Commissioner of Public Safety, the Assistant Commissioner of Public Safety and the BCA Superintendent. If verified, violations will be sanctioned in accordance with the MNFC Memorandum of Understanding (Appendix B) and the discipline policies of the agency responsible for the individual in question.

Individual users of MNFC information remain responsible for the appropriate use of MNFC information. Each user of the MNFC and each participating agency within the MNFC are required to abide by this Privacy, Civil Rights, and Civil Liberties Policy. Failure to abide by the restrictions for the use of the MNFC information may result in the suspension or termination of user privileges; discipline imposed by the user's employing agency, or criminal prosecution.

XVI. TRAINING

All staff members assigned to the MNFC from participating agencies are required to attend annual MNFC P/CRCL Policy training conducted by the MNFC Privacy Officer.

The following individuals will participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:

- All assigned personnel of the MNFC.
- Personnel providing information technology services to the MNFC.

The MNFC's Privacy Policy training program will cover:

- Purposes of the privacy policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR and ISE-SAR information maintained or submitted by the MNFC to the shared spaces.
- How to implement the policy in the day-to-day work of a Participating Agency.
- The impact of improper activities associated with violations of the policy.
- Mechanisms for reporting violations of the policy.

- The possible penalties for policy violations, including transfer, dismissal, and criminal liability, if any.
- Special training to personnel authorized to share Protected Information through the ISE regarding the center's requirements and policies for collection, use, and disclosure of Protected Information.

APPENDIX A: MINNESOTA FUSION CENTER DEFINITIONS

The following terms are used in this Privacy, Civil Rights, and Civil Liberties Policy and are defined below.

A. "BCA Case File" means a reasonable suspicion exists that criminal activity has occurred, could occur or is being planned. Additionally one or more of the following must occur for a BCA Case to be created;

1. The reported information does not support a currently ongoing criminal investigation.
2. A determination is made that further criminal investigation is needed and that this additional investigative effort would exceed the review done for a Request for Information or a Suspicious Activity Report.

B. "Critical Infrastructure Key Resource" or "CIKR" means the assets, systems, and networks, whether physical or virtual, so vital to the United States or the states that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof and the publicly or privately controlled resources essential to the minimal operations of the economy and government.

C. "Director" means the supervisor appointed by the BCA to oversee the management of the MNFC.

D. "Disclosure" means the sharing of data or information in any manner outside the MNFC.

E. "Fusion center" means the governmental organization that is assigned to collect, integrate, evaluate, analyze, and disseminate data and information from state, local, and federal law enforcement agencies, including fusion centers operating in other states.

F. "Information Sharing Environment (ISE)" means the trusted partnership among all levels of government, the private sector and foreign partners to detect, prevent, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America. This partnership enables the trusted, secure, and appropriate exchange of terrorism information, in the first instance, across the five federal communities, to and from state, local, and tribal governments, foreign allies, and the private sector, and at all levels of security classification.

G. "Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR) means a suspicious activity report that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

H. “MNFC” means the Minnesota Fusion Center; the state designated fusion center consisting of analysts, training and liaison officers, and managers.

I. “MNFC database” means the case management system used by the MNFC to store, document, and audit MNFC information.

J. “MNFC Privacy Officer” means a MNFC staff person assigned by the Director to provide privacy training and ensure compliance with the MNFC Privacy Policy.

K. “MNFC Suspicious Activity Report/Tips and Leads” or “MNFC SAR” means any reported behavior or activity that may result in reasonable suspicion that a crime has occurred, could occur, or is being planned.

L. “Need to know” means the prospective recipient of data requires access to specific information in order to perform or assist in a lawful and authorized governmental or public safety function. In other words, access is required for the performance of official duties.

M. “Operations Manager” means the MNFC staff person appointed by the Director to manage the MNFC Operations Unit including product development, analysis, dissemination, and records management.

N. “Participating agencies” means the agencies that provide staff to the MNFC and are listed in the MNFC Memorandum of Understanding.

O. “Personal data” means any data or information relating to an identifiable individual.

P. “Protected information” means information about individuals and organizations subject to legal protections, including the U.S. and Minnesota constitutions; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state laws.

Q. “Reasonable suspicion” means that sufficient facts are established to give a trained law enforcement officer or MNFC employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise.

R. “Requestor” means the state, local, or federal law enforcement officer or agency making a Request for Information from, or reporting an incident to, the MNFC.

S. “Request for Information” or “RFI” means a request from a law enforcement, participating, or stakeholder agency to the MNFC for information the requesting agency needs in support of an ongoing criminal investigation. It also means a non-criminal homeland security information request.

T. “Right to know” means any agency or organization authorized by federal law or state statute to have access to the data or information. See Minn. Stat. §13.05, subd. 4(b) and 9.

U. “Stakeholder agencies” means participating agencies and agencies that have representatives vetted with the MNFC.

V. “Suspicious Activity Report” or “SAR” means a MNFC SAR, ISE-SAR, or any reported behavior or activity that may result in the reasonable suspicion that a crime has occurred, could occur or is being planned. It also means a bulletin or brief from a fusion center, law enforcement intelligence unit or federal agency to provide situational awareness to Minnesota agencies.

APPENDIX B: MINNESOTA FUSION CENTER MEMRADUM OF UNDERSTANDING

Minnesota Fusion Center (MNFC) Memorandum of Understanding (MOU)

The establishment of an integrated system of gathering, analyzing, and reporting all-crimes, all-hazards, and terrorism information must be a high priority for all local, state, tribal, and federal law enforcement agencies operating within the State of Minnesota.

Pursuant to the Omnibus Crime Control and the Safe Streets Act of 1968, 42 U.S.C. 3711 et. seq. as amended and in accordance with 28 CFR Part 23; a facility is established to assist local, state, and federal law enforcement and private sector resources. The entities involved include local, state, and federal law enforcement; first responders; emergency management; and private sector entities. This facility is created through federal law in cooperation with and for the benefit of participating entities and must comply with all state and federal laws. Information will be shared pursuant to federal and state law to identify all-crimes, all-hazards. To this end, the Minnesota Fusion Center (MNFC) is formed as an investigative support unit at the Minnesota Bureau of Criminal Apprehension.

I. Participants

- US Department of Homeland Security (DHS) and associated agencies
- Federal Bureau of Investigation (FBI)
- State of Minnesota – Bureau of Criminal Apprehension (BCA)
- State of Minnesota – Homeland Security and Emergency Management (HSEM)
- State of Minnesota – State Fire Marshal
- State of Minnesota – Information Technology Services (MNIT)
- State of Minnesota – Department of Corrections (DOC)
- Hennepin County
- Dakota County
- Hennepin County Emergency Medical Services
- Metro Transit Police Department
- Mall of America
- Xcel Energy

II. Responsibilities

A. The MNFC is guided by the following mission statement:

> *The mission of the MNFC is to collect, evaluate, analyze and disseminate information regarding organized criminal, terrorist and all-hazards activity in Minnesota, while complying with state and federal law to ensure the rights and privacy of all.*

B. The role of the MNFC include, but are not limited to the following:

1. **MNFC Website Infrastructure**: This includes building an user base for reviewing and sharing data through the MNFC website and connecting with different groups to add members to MNFC from different disciplines.
2. **Bulletin Production and Dissemination**: With the approval of the data originator, the MNFC will produce timely and meaningful bulletins to share with a statewide audience. No approval will be required for open source information.
3. **Provide Basic Investigation and Analysis of Submissions to the MNFC**: MNFC personnel will review the submissions using open source databases and agency/state databases. Each liaison representative in the MNFC will connect back to their respective department/office in order to provide a conduit for information belonging to those organizations.
4. **Response to Request for Information (RFI)**: Provide a timely response to requests from state agencies, out-of-state agencies, federal partners, and other fusion centers for information and services available through MNFC to include, but not limited to, assessments, analytical products, and open source background materials.
5. **MNFC Establishment:** The building of the MNFC with the appropriate policy and procedure development.
6. **Training:** The MNFC will coordinate training relative to the function of the MNFC, to include Threat Liaison Officer (TLO) training.

III. Composition

A. Staff comprising liaison roles within the MNFC from participating agencies shall be expensed from the participating agencies' funding. Participating agencies acknowledge that it is their sole responsibility to provide all salary compensation and fringe benefits to their employees participating in the MNFC and all liaison employees will remain under the supervision of the contracting agency.

B. The MNFC is established as an investigative support unit within the Minnesota Department of Public Safety, Bureau of Criminal Apprehension (BCA). Management of the MNFC is provided by the BCA subject to approval by the Superintendent of the Bureau of Criminal Apprehension.

C. Executive oversight of the MNFC is conducted by the Commissioner of Public Safety, the Assistant Commissioner of Public Safety, and the Superintendent of the Bureau of Criminal Apprehension, or their designee.

D. Overall supervision and management of the MNFC will be the responsibility of the BCA, with the MNFC Director acting as its agent having authority to schedule center staff, assign work, and control access to MNFC facilities and

secure data, subject to approval by the Superintendent of the BCA. Discipline issues will be handled in consultation with the contracting/employing agency. Changes to the MNFC staff will require the approval of the Superintendent of the BCA or his designee.

E. Management of the information analysis process will comply with all state and federal laws and be guided by specific policy established by the BCA with input and recommendations from the Commissioner of Public Safety, the Assistant Commissioner of Public Safety, the Superintendent of the BCA, or their designee. Disagreements among MNFC participating agencies regarding operational issues will be brought to the attention of the MNFC Director for response. If not satisfactorily resolved, the order of appeal is to the Superintendent of the BCA, and subsequently to the Assistant Commissioner and/or Commissioner of Public Safety.

IV. Indemnification

A. To the extent allowed by Minnesota law, each participating agency agrees that it will be responsible for its own acts and any liability resulting therefrom and related attorney fees to the extent authorized by law, and shall not be responsible for the acts of the other participating agencies or any liability resulting therefrom.

B. To the extent allowed by Minnesota law, each participating agency agrees to defend, indemnify and hold harmless the other participating agencies and employees from any costs or expenses, including reasonable attorney fees, resulting directly or indirectly from any act or omission of a participating agency and their employees while in the performance of activities required by this memo of understanding. The duty to defend, indemnify and hold harmless is subject to the limitations and immunities in Minnesota Statute 3.736 and Chapter 466, which are not waived.

V. Executive Oversight

Oversight of the MNFC consist of the Minnesota Department of Public Safety Commissioner, Assistant Commissioner, and the BCA Superintendent.

VI. MNFC Management

There shall be established a MNFC management team, consisting of the Director/Special Agent in Charge, Assistant Director/Assistant Special Agent in Charge, and the Operations Manager. Under the guidance from the MNFC Director, the management team will develop MNFC policies and procedure proposals, as well as the enforcement of those policies and procedures.

VII. Technological Support

A. It is the intent of the MNFC to be equipped with BCA update technology, equipment, and IT support to allow for computerized information file systems, use of contemporary analytical software, and integrated law enforcement and public safety database sharing.

B. In order to satisfy the mission of MNFC, to be a regional supporting information sharing center, MNFC is the primary gateway for the electronic sharing of information using, but not limited to, previously established information systems (i.e. Regional Information Sharing System® (RISS), Law Enforcement Online, FBI Guardian, HSIN-Intel).

VIII. Training

A. Members assigned to MNFC serving in the capacity of analysts, officers, and managers should receive training to the standards set by the Law Enforcement Intelligence Unit (LEIU) for criminal intelligence officers and managers. This training will allow the standardized collection, storage, and dissemination of materials to ensure compatibility with peer organizations and compliance with governing state and federal regulations ensuring the protection of the civil rights of any person or group.

B. Specific individualized and group training will be required to allow members to operate computerized software systems and to function in an information driven operations center. The MNFC Director or designee will maintain documentation of group and individual training.

IX. Limitations

A. Nothing in this Memo of Understanding is intended or shall be construed, to modify or be in conflict with Minnesota State Statutes, federal law or Code of Federal Regulations. MNFC must adhere to the applicable state and federal law and U.S. Attorney General Guidelines and Title 28, Code of Federal Regulations (CFR) in the lawful collection, maintenance, and dissemination of information for and on behalf of the federal authorities. MNFC will maintain a written policy regarding the handling of data that complies with applicable state and federal law.

B. Information and documents/files maintained or accessed in the MNFC shall remain the property and in the constructive possession of the originating agency. Dissemination of information or documents outside the MNFC not accessible to the general public shall require permission of the originating agency and comply with all applicable state and federal law.

X. Adding Participants

Adding additional participants within the MNFC MOU may be made at any time, as approved by the Superintendent of the BCA, or his/her designee. Additions will required the added agency to sign an additional signature page attached to the MOU, which will be incorporated into the original MOU and kept on file by the MNFC.

XI. Termination

Any party to this Memo of Understanding (MOU) may terminate this MOU, specifically for themselves, at any time, with or withoutcause. The MOU will continue and remain effective for the remaining parties to the MOU.

When fully executed, this MOU supersedes and replaces any and all previous Memoranda of Understanding between the participants pertaining to the establishment and operation of the MNFC.

APPENDIX C: MINNESOTA FUSION CENTER NOTICE

What follows is the text from the MNFC registration forms. The registrant has to click on a separate box to agree to the terms, as noted below. This notice explains the need to comply with the MNFC Privacy, Civil Rights, and Civil Liberties Policy.

> *I agree to terms and conditions of the MNFC Terms and Conditions. I agree to not share my log-on and password with another party. I agree to abide by all classification and dissemination terms that are placed on all products produced by the MNFC and those that the MNFC disseminates for other agencies. Those terms include but are not limited to: No portion of MNFC documents should be released to the media or general public. MNFC documents contain data protected by state and federal law and are subject to distribution restrictions. MNFC authorization is required prior to disseminating any MNFC document or portion of outside of the intended recipients' agency. I understand that any release of this information could adversely affect or jeopardize investigative activities. I also understand that the MNFC will use private data I have provided to contact me or to permit others to contact me about information I have provided to or requested from the MNFC.*

APPENDIX D: LIST OF APPLICABLE STATUTES

The following is a list of legal provisions that affect the operations of the Minnesota Fusion Center (MNFC), the classification of data it holds, and how access and dissemination of that data occurs.

This list is current as of the date it is developed and will routinely be reviewed and modified.

Federal Provisions

United States Constitution, including the **Bill of Rights**

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22

Crime Identification Technology, 42 U.S.C.§ 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23

Criminal Justice Information Systems, 28 CFR Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682

Electronic Communications Privacy Act of 1986,18 U.S.C. §§ 2510–2522, 2701–2709

Fair Credit Reporting Act, 15 U.S.C. § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983 Federal Records Act, 44 U.S.C. § 3301

Freedom of Information Act (FOIA), 5 U.S.C.

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301

IRTPA, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Pub. L. 103-209 (December 20, 1993)

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616 Privacy Act of 1974, 5 U.S.C. § 552a,

Privacy of Consumer Financial Information, 16 CFR Part 313

Protection of Human Subjects, 28 CFR Part 46,

Safeguarding Customer Information, 16 CFR Part 314 Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201

USA PATRIOT Act, Public Law No. 107-56 (October 26, 2001)

Minnesota Provisions

Minnesota Constitution

Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13 and enabling rules found in Minnesota Rules, Chapter 1205

Official Records Act, Minnesota Statutes, section 15.17

Records Management Act, Minnesota Statutes, section 138.0163. et. seq.

Minnesota Health Records Act, Minnesota Statutes, section 144.291, et. seq.

Minnesota Statutes, Chapter 243 - corrections

Minnesota Statutes, Chapter 260B - juveniles alleged or adjudicated delinquent

Minnesota Statutes, Chapter 299C - Bureau of Criminal Apprehension

Minnesota Statutes, Chapters 609-643 -provisions relate to crimes and offenses, rehabilitation and incarceration

APPENDIX E: MINNESOTA FUSION CENTER RECORDS RETENTION SCHEDULE

1. Schedule Number	Date	2. New	Revision of	MINNESOTA RECORDS RETENTION SCHEDULE
012-014	8/3/2011		09-141	
3. Agency **Department of Public Safety**		4. Division/Section Bureau of Criminal Apprehension Investigations Unit - Minnesota Joint Analysis Center (MNJAC)		6. Page 1 of 3
5. Address 111 Washington Avenue South, Suite 820 Minneapolis, MN 55401				See attached page(s) for records description

7. *For Use By Records Panel Only*

AUTHORIZATION: Under the authority of M.S. 138.17, it is hereby ordered that the records listed on this application be disposed per approved schedule.	Notice: This retention schedule has been reviewed by the State Records Disposition Panel in accordance with Minnesota Statutes 138.17. The records listed on this schedule have been reviewed for their historical, fiscal, and legal value.
8. Agency Records Management Officer (signature) E. Joseph Newton **Date** 8-1-11	**11. Minnesota Historical Society, Director** Charles A. Bruger **Date** 2 August 2011
9. Type Name / Phone E. Joseph Newton 651-201-7170	**12. Legislative or State Auditor** Dan Nelson **Date** 8/8/11
10. Agency Head or Designee (signature) Mary Ellen **Date** 8/1/11	**13. Attorney General** Patricia Nolte **Date** 8/11/11

Original-State Records Disposition Panel

Copy 1-Agency (after approval)

Form Version: 21 July 2003; Revised April 2008

1. Schedule No.	3. Agency Department of Public Safety	4. Division/Section: Bureau of Criminal Apprehension Investigations Unit - Minnesota Joint Analysis Center (MNJAC)	6. Page ____of _3__

14. Item No.	15. Record Series Title and Description	16. Retention Instructions	17. Statute	18. Vital? (Yes/no)	19. Archival? (Yes/no)
1A	**Case files** Electronic BCA Case Files where reasonable suspicion exists and either the reported information does not support an currently ongoing criminal investigation or a determination is made that further investigation is needed.	3 years	28 C.F.R. §23.20 (h)	Yes	No
1B	**Case files** Paper-based BCA Case Files as described in 1A	Until entered in to the electronic records system	28 C.F.R. §23.20 (h)	No	No
2A	**MNJAC Suspicious Activity Report/Tips and Leads** An electronic report of behavior or activity that may result in reasonable suspicion that a crime has occurred or could occur.	1 year		Yes	No
2B	**MNJAC Suspicious Activity Report/Tips and Leads** A paper-based report of behavior or activity that is described in 2A	Until entered into the electronic records system		No	No
4	**Critical Infrastructure Brief** A bulletin created by MNJAC staff to provide information to participating agencies to help prevent and respond to terrorist activities	1 year		No	No
5	**Request for Information** Request from law enforcement, participating or stakeholder agency for information needed in support of an on-going investigation. Also includes a non-criminal homeland security information request.	3 years		Yes	No
8	**Secure information-sharing platform participating agency documentation**	Purged when participant goes to inactive status		Yes	No

1. Schedule No.	3. Agency Department of Public Safety	4. Division/Section: Bureau of Criminal Apprehension Investigations Unit - Minnesota Joint Analysis Center (MNJAC)	6. Page ____of _3__