Minnesota Joint Analysis Center Privacy Policy

Approved by the Oversight Group
December 20, 2011

Contents

I. MNJAC Purpose

The Minnesota Joint Analysis Center (MNJAC) is a fusion center that develops information for and by Participating and Stakeholder Agencies. The decisions by agencies to participate in the MNJAC and which databases to provide for MNJAC use are voluntary and are controlled by the laws and rules governing those individual agencies.

The MNJAC provides timely sharing and exchange of crime-related information. A primary focus of the MNJAC is developing and disseminating criminal investigative information. 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 Policy Purpose

The MNJAC 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 privacy 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. Definitions

The following terms are used in this Privacy 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 MNJAC.

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

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. "MNJAC" means the Minnesota Joint Analysis Center; the fusion center consisting of analysts, training and liaison officers, and managers.

I. "MNJAC Database" means the case management system used by the MNJAC to store, document, and audit MNJAC information.

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

K. "MNJAC Suspicious Activity Report/Tips and Leads" or "MNJAC 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 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 MNJAC staff person appointed by the Director to manage the MNJAC Operations Unit including product development, analysis, dissemination and records management.

N. "Oversight Group" means the management body overseeing the direction of the MNJAC. Each Participating Agency has a representative on the Oversight Group.

O. "Participating Agencies" means the agencies that provide staff to the MNJAC and are listed in the MNJAC Memorandum of Understanding.

P. "Personal Data" means any data or information relating to an identifiable individual.

Q. "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.

R. "Reasonable Suspicion" means that sufficient facts are established to give a trained law enforcement officer or MNJAC employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise.

S. "Requestor" means the state, local or federal law enforcement officer or agency making a Request for Information from, or reporting an incident to, the MNJAC.

T. "Request for Information" or "RFI" means a request from a law enforcement, Participating, or Stakeholder Agency to the MNJAC for information the requesting agency needs in support of an ongoing criminal investigation. It also means a non-criminal homeland security information request.

U. "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.

V. "Stakeholder Agencies" means Participating Agencies and agencies that have representatives vetted in ICEFISHX.

W. "Suspicious Activity Report" or "SAR" means a MNJAC 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.

IV. Governance and Oversight

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

The MNJAC also has an Oversight Group whose members represent the Participating Agencies. In coordination with the BCA's Superintendent, the Oversight Group is responsible for the operation of the MNJAC. To provide daily operational direction and ensure compliance, the Oversight Group and Superintendent have designated a Director for the MNJAC. The Director is responsible for the MNJAC's overall operation.

The MNJAC Oversight Group, through the Director, will ensure that access to MNJAC's information resources is secure. Unauthorized access or use of the resources is forbidden. The Oversight Group reserves the right to restrict the qualifications and number of personnel having access to the MNJAC and to suspend or withhold service to any individual violating this Privacy Policy. The Oversight Group further reserves the right to conduct inspections concerning the proper use and security of the information received from the MNJAC.

In order to preserve privacy, civil rights and civil liberties, the MNJAC has created a privacy committee. The members of the committee work 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 committee has examined and recommended standards the MNJAC follows for the collection, use, and security of information and technology, as well as accountability guidelines for the management of the information. The MNJAC's Privacy Policy incorporates fair information practices and principles.

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

The MNJAC Privacy Officer will provide a point of contact and coordination for alleged data or information errors, complaints, privacy policy violations and

liaison for the ISE. The MNJAC Privacy Officer will coordinate conflict resolution under MNJAC's redress policy and enforcement and sanctions outlined in the Accountability and Enforcement section of this policy (see section XVI).

The MNJAC Privacy Officer has been and will continue to be trained. The Privacy Officer can be contacted at the following address: "privacyofficer@icefishx.org." A staff attorney within the BCA will work with the MNJAC Privacy Policy Committee to ensure that privacy and civil rights are appropriately protected by the MNJAC's information acquisition, dissemination and retention practices.

V. Policy Applicability and Legal Compliance

All MNJAC personnel, which includes Participating Agency personnel, private contractors, and other authorized individuals, including those state employees providing technical services, with direct access to MNJAC data bases, are required to abide by this Privacy Policy. These individuals and any other recipient of MNJAC information must also follow all applicable laws which govern the treatment of the information the MNJAC collects, receives, maintains, archives, accesses, discloses, or disseminates, including information within the ISE. See the MNJAC Memorandum of Understanding that is attached as Appendix A. In addition, Stakeholder Agencies receive information from the MNJAC through ICEFISHX. The notice participants receive when utilizing ICEFISHX is attached as Appendix B.

The MNJAC will make a printed or electronic copy of this policy available to all MNJAC and non-MNJAC 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 MNJAC 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 C.

VI. Information

All Personal Data collected by the MNJAC, 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 (Data Practices), the approved MNJAC Minnesota Records Retention Schedule (currently 09-141 and 012-014), and any other applicable federal or state laws governing information practices. The

MNJAC 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 MNJAC should meet all of the following requirements:

1. The source of the information is reliable and verifiable, and

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, and

3. The information was collected in a lawful manner, and

4. The information is accurate and current.

The MNJAC will retain 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 MNJAC approved records retention schedule (unofficial compilation attached as Appendix D). 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 MNJAC Database with the other MNJAC data and so the SARs are secured in the same way as all other data.

The MNJAC 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 MNJAC information. The MNJAC identifies and reviews Protected Information that may be disclosed by the MNJAC 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 MNJAC will abide by daily operating procedures for the initial collection and verification of information, including the screening process 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. Suspicious Activity Reports 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 MNJAC will not open a BCA Case File.

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

Lawfully collected information that meets MNJAC's Privacy Policy will be stored in the MNJAC 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:

a. Information on an individual or group merely on the basis that such individual or group support unpopular causes;

b. Information on an individual or group merely on the basis of race, gender, age, citizenship, disability, sexual orientation, place of origin, or ethnic background;

c. Information on an individual or group merely on the basis of religious or political affiliations, or beliefs;

d. 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

e. Information obtained in violation of any applicable federal or state rules or statutes.

All MNJAC information is managed through the MNJAC 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 MNJAC Database will be conducted by the Operations Manager and records that may be purged will be disposed. Additional information about records destruction can be found in Section XV of this policy.

On receipt of information, MNJAC 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, MNJAC 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 four types of operating files within the MNJAC. 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 MNJAC Database and a BCA case number is automatically generated.

2. Request for Information (RFI)

An RFI must be supported by a reasonable suspicion or homeland security concern that is provided to the MNJAC. MNJAC personnel cannot answer an RFI unless it contains a Reasonable Suspicion or homeland security concern.

3. Suspicious Activity Report (SAR)

A SAR will be entered into the MNJAC Database. A SAR should be reported to the MNJAC by a law enforcement entity or security related to a CIKR site once it has been reported to a local law enforcement agency. The MNJAC receives SARs by the following means:

- The secure information-sharing platform
- Fax
- Telephone
- Email

4. Dissemination Log (LOG)

The LOG is used as a tracking device for bulletins, briefs and assessments disseminated by the MNJAC. LOG entries will include weekly bulletins and special assessments. Copies of products are attached to the LOG entry. The analysts that disseminate either Law Enforcement (LE) or Critical Infrastructure (CI) Briefs will log the dissemination of these products. Any special bulletin, brief or assessment will be logged by the disseminating analyst. Special assessments do not need a separate LOG entry if attached as part of the LE Brief or CI Brief.

C. Labels

The MNJAC 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 MNJAC 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 MNJAC 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 MNJAC will keep a record of the source of all information sought and collected by it.

VII. Acquiring and Receiving Information

The MNJAC and Participating Agencies will inform the public about information collection practices and comply with Minnesota Statutes, Chapter 13.

Information obtained from or through the MNJAC 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 MNJAC.

The information maintained by the MNJAC is obtained through Participating Agencies, Stakeholder Agencies, federal agencies, and open source resources. Individual users of MNJAC 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 MNJAC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

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

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

VIII. Information Quality Assurance

The MNJAC is required by Minn. Stat. §13.05, subd. 5 to assure that data are accurate, complete, current and secure. The MNJAC 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 of this policy has been met.

MNJAC 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 MNJAC's 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 MNJAC 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 MNJAC's 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 MNJAC will also adhere to this standard although it is not an operational agency conducting investigations.

When determining information confidence, MNJAC personnel will use the following confidence labeling standards for source reliability and content validity.

1. Source Reliability

The source is the person or agency who gives MNJAC the information. The source's reliability is evaluated according to the following.

(a) Reliable means the source is unquestioned or has been tested in the past. All law enforcement agencies are classified as completely reliable.

(b) Usually Reliable means the majority of the information provided by the source in the past has proved to be reliable.

(c) Unreliable means the source has provided reliable information sporadically in the past.

(d) 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.

2. 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.

(a) Confirmed means the information has been corroborated by an investigator or another reliable, independent source.

(b) Probable means the information is consistent with past accounts.

(c) Doubtful means the information is inconsistent with past accounts.

(d) Cannot Be Judged means the authenticity of the information has not yet been determined by either experience or investigation.

3. Classification

The MNJAC uses two classifications or sensitivity structures since the MNJAC 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, MNJAC 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, MNJAC 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 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. 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. 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.

4. In addition to using the labels and classification structures listed above, MNJAC personnel will utilize the following standards to ensure that data quality is maintained.

(a) The MNJAC investigates, in a timely manner, alleged errors and deficiencies and corrects, deletes, or refrains from using information found to be erroneous or deficient.

(b) The labeling of retained information will be reevaluated by MNJAC when new information are gathered that have an impact on the confidence (source reliability and content validity) of previously retained information.

(c) The MNJAC 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.

(d) Originating agencies are responsible for the quality and accuracy of the information accessed by or provided to the MNJAC. The MNJAC 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.

(e) When information is found to be inaccurate, incomplete, out of date or unverifiable, the MNJAC will notify recipient agencies in writing and will maintain documentation of the notification.

IX. Collation and Analysis

Access to the MNJAC 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 MNJAC 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 MNJAC Oversight Group. 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 Information Section.

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

- Management and developing of information sharing through the MNJAC's 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, and local agencies to produce joint products
- The coordination and facilitation of regional training opportunities in support of the MNJAC mission
- The identification of crime patterns and trends

X. 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
- 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.

XI. Use of Information by the MNJAC

Information obtained from or through the MNJAC 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 MNJAC will use Information on a Need to Know basis, and in accordance with applicable laws.

Credentialed, role-based access criteria will be used by MNJAC, 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.

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

1. Individual passwords will not be disclosed to any other person, except as authorized by MNJAC management.
2. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
3. Background checks will be completed on personnel who will have direct access to the MNJAC at a level determined by the Oversight Group and consistent with BCA policy.
4. Use of the MNJAC's data in an unauthorized or illegal manner will subject the requestor to denial of further use of the MNJAC; discipline by the requestor's employing agency, and/or criminal prosecution.

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

The MNJAC 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.

XII. Disclosure of Information Outside the MNJAC

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

(1) The Law Enforcement Brief (LE Brief) is a law enforcement sensitive brief compiled from MNJAC information, and other federal, state, and local reports which may contain comprehensive law enforcement data.

This brief is disseminated to law enforcement personnel who are vetted by MNJAC staff.

(2) The Critical Infrastructure Brief (CI Brief) is a non-law enforcement; sensitive information brief complied from open source internet sites and other federal, state, and local reports. A CI Brief may contain U/For Official Use Only documents and materials. This brief is disseminated to first responder, government, and private sector personnel.

No briefs or assessments can be disseminated outside of the MNJAC unless reviewed by the MNJAC Privacy Officer or designee and approved for dissemination by MNJAC Operations Manager, the 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 MNJAC Database along with what was disclosed and the identity of the recipient. A Stakeholder Agency may not re-disclose information from the MNJAC until it has received permission from the MNJAC.

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

XIII. Redress

A. Disclosure to a Data Subject

An individual who is the subject of data at the MNJAC 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 MNJAC, to have copies of the data, and to have the meaning of the data explained. When data are classified as private, the MNJAC 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 MNJAC 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-dat-rights.aspx.

A record of these disclosures is kept by the MNJAC.

B. Disclosure to the Public

The public has the right to access public data maintained at the MNJAC. 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 MNJAC 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 MNJAC 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." MNJAC's responsible authority is the Commissioner of the Department of Public Safety.

The Commissioner 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 MNJAC; and
- allegedly has resulted in demonstrable harm to the complainant,

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

On receipt of the complaint at Privacyofficer@icefishx.org, 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 MNJAC 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 MNJAC 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, MNJAC 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 MNJAC.

E. MNJAC Principles

Information gathered or collected and records retained by MNJAC 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.

MNJAC 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.

XIV. Security Safeguards

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

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

MNJAC 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 MNJAC's Security Officer.

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 MNJAC documents or software will be stored on MNJAC 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.

XV. 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 MNJAC 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 D for a copy of the approved records retention schedule.

The MNJAC 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 MNJAC 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.

XVI. Accountability and Enforcement

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

The MNJAC 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: privacyofficer@icefishx.org.

Queries made to the MNJAC Database will be auditable and be logged, identifying the user initiating the query. MNJAC information application logs will be made available for audit. When information is disseminated outside of the MNJAC, 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 MNJAC secondary dissemination log will include:

1. Date of release.
2. The subject of the information
3. To whom the information was released, including address and telephone number.
4. An identification number or other indicator that clearly identifies the information released.
5. The purpose for which the information was requested.

The MNJAC Oversight Group will be responsible for conducting or coordinating annual and random internal or external audits, including audits by the legislative auditor, and for investigating misuse of MNJAC's information systems. All confirmed or suspected violations of MNJAC policies will be reported by MNJAC personnel and other authorized users to the MNJAC Privacy Officer, who will investigate them and report confirmed violations to the Director and to the Oversight Group. If verified, violations will be sanctioned in accordance with the

MNJAC Memorandum of Understanding (Appendix A) and the discipline policies of the agency responsible for the individual in question.

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

The MNJAC will prepare an annual report to the MNJAC Oversight Group regarding Privacy Policy status and information access issues.

XVII. Training

All staff members assigned to the MNJAC from Participating Agencies are required to attend annual MNJAC Privacy Policy training conducted by the MNJAC 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 MNJAC.
- Personnel providing information technology services to the MNJAC.

The MNJAC'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 MNJAC 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 Joint Analysis Center (MNJAC)
Memo of Understanding

The establishment of an integrated system of gathering, analyzing and reporting all- crimes, all-hazards information must be a high priority for all local, state, 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 Joint Analysis Center (MNJAC) is formed as an investigative unit at the Minnesota Bureau of Criminal Apprehension.

I. Participants:

Federal Bureau of Investigation
State of Minnesota / Bureau of Criminal Apprehension (BCA)
State of Minnesota / Homeland Security and Emergency Management, (HSEM)
State of Minnesota / Department of Corrections (DOC)
Minnesota Department of Military Affairs
Dakota County Sheriff's Office
Hennepin County Sheriff's Office
Washington County Sheriff's Office
Minneapolis Police Department
Saint Paul Police Department
Saint Paul Fire Department
Eden Prairie Police Department
Plymouth Police Department
Olmsted County Sheriff's Office
Lake of the Woods County Sheriff's Office
Saint Louis County
Stearns County Sheriff's Office
City of North Mankato

II. Responsibilities

a. The MNJAC will be guided by the following mission statement:

The mission of the Minnesota Joint Analysis Center (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.

b. The roles of the MNJAC include but are not limited to:

i. ICEFISHX Infrastructure Development: This includes building an ICEFISHX user base for reviewing and sharing data received and made available by FBI through the FBI'S ICEFISHX website and connecting with different groups to add members to MNJAC from different disciplines. Of special importance is establishing a link to the critical infrastructure group.
ii. Bulletin Production and Dissemination: With the approval of the data originator, the MNJAC will produce timely and meaningful bulletins to share with a statewide audience including the FBI. No approval will be required for open source information.
iii. Provide Basic investigation and analysis of Submissions to the MNJAC: MNJAC personnel will review the submissions initially using open source data bases and agency/state data bases brought into the Center to try to determine if submissions should move to the FBI's Intelligence Program or other appropriate agency(s). MNJAC personnel with the appropriate clearances could perform other checks by utilizing FBI databases, as maintained and approved by the FBI. Additionally, MNJAC personnel will provide assistance for the FBI Intelligence Program pursuant to applicable state and federal law. Each local representative in the MNJAC will provide a physical tie to their respective department/office and internal group (as it exists) in order to provide a conduit for information belonging to those jurisdictions.
iv. Response to Request for Information (RFI): Provide a timely response to requests from agencies, fusion centers, and the U. S. Department of Homeland Security (DHS) for information and services available through MNJAC to include but not limited to assessments, analytical products, and open source background materials.

v. MNJAC Establishment: The building of the MNJAC with the appropriate policy and procedure development.
vi. Training: The MNJAC will coordinate training relative to the function of the MNJAC.

III. Composition

a. The MNJAC will be staffed with representatives from the participating agencies as defined in the designated grant agreements and for the period of time authorized by these grants, but not exceeding a total of five (5) years from the execution date of this MOU. Participating agencies providing MNJAC staffing not covered by grants will provide their employees at the sending agency's own expense.
b. The MNJAC is established as an investigative unit of the Minnesota Bureau of Criminal Apprehension (BCA). Management of the MNJAC is provided by the BCA subject to approval by the Superintendent of the Bureau of Criminal Apprehension.
c. The Oversight group as established by the MNJAC Memorandum of Understanding (MOU) to provide input and recommendations regarding policy and operations.
d. Overall supervision and management of the MNJAC will be the responsibility of the State of Minnesota Bureau of Criminal Apprehension with the MNJAC Director acting as its agent having authority to schedule center staff, assign work, and control access to MNJAC facilities and secure data subject to approval by the Superintendent of the Bureau of Criminal Apprehension. Discipline issues will be handled in consultation with the contracting/employing agency. Also, to the greatest extent possible, agencies' employees assigned to the MNJAC will serve on the MNJAC for the MNJAC'S entire existence. Changes to the MNJAC staff will require the approval of the Superintendent of the Bureau of Criminal Apprehension and MNJAC'S Oversight Group.
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 MNJAC Oversight Group. . Disagreements among MNJAC participating agencies regarding operational issues will be brought to the attention of the MNJAC Director for response. If not satisfactorily resolved, the order of appeal is to the Oversight Group and then the Superintendent of the BCA.

Participating agencies acknowledge that it is their sole responsibility to provide all salary compensation and fringe benefits to their employees participating in the MNJAC and all participating employees will remain under the supervision of the contracting agency.

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 there from 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 there from.
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. Oversight Group

There shall be established an Oversight Group consisting of executives or designees with decision making authority from the participating agencies. Oversight Group members will have voting rights regarding MNJAC policies and procedures subject to approval by the Bureau of Criminal Apprehension. In addition to representation by the participant agencies, the Oversight Group will have non-voting member representatives from; the Minnesota Chiefs of Police Association, the Minnesota Sheriffs Association, and others as identified by the Oversight Group.

VI MNJAC Management

There shall be established a MNJAC management team consisting of the Director, the Training / Liaison Manager & the Operations Manager. Under the guidance of the MNJAC

Director, the management team will develop MNJAC policy and procedure proposals for the Oversight Group and also ensure the implementation of these policies and procedures.

VII. Technological Support

a. It is the intent of the MNJAC to be equipped with BCA updated 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. MNJAC personnel shall have exclusive and secure access to their contracting/employing agencies' Law Enforcement and Public Safety Information systems to facilitate streamlined information sharing capabilities. Contributing member agencies will grant their contractors/representatives exclusive access to their information systems to meet MNJAC needs and to keep systems compliant with member agencies computer and system standards and/or requirements. These contractor/representatives must therefore agree to the confidentiality provisions of this MOU regarding any data they have access to.

b. In order to work towards the goal of MNJAC to be a regional supporting information sharing center, MNJAC should serve as a primary gateway for the electronic sharing of information using, but not limited to, previously established information systems (*i.e. ICEFISHX, Regional Information Sharing System® (RISS), Law Enforcement Online, FBI Guardian, HSIN-Intel).*

IX. Training

a. Members assigned to MNJAC 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 MNJAC Director or designee will maintain documentation

of group and individual training consistent with LEIU standards.

XI. 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. MNJAC must adhere to the applicable state and federal law and US 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. MNJAC 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 MNJAC shall remain the property and in the constructive possession of the originating agency. Dissemination of information or documents outside the MNJAC not accessible to the general public shall require permission of the originating agency and comply with all applicable state and federal law.

XII. Termination

Any party to this Memo of Understanding (MOU) may terminate this MOU, specifically for themselves, at any time, with or without cause, upon 30 days written prior notice to all other parties of this MOU. The MOU will continue and remain effective for the remaining parties to the MOU.

Participants to the MNJAC entering into this Memo of Understanding are listed below. Changes in participants to the MNJAC may be made at any time, as approved by the Superintendent of the Bureau of Criminal Apprehension and the MNJAC Oversight Group. Changes will require the added agency sign an additional signature page to this MOU, which will be incorporated by reference and made a part of this MOU and kept on file at the MNJAC.

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

Minnesota Joint Analysis Center Privacy Policy

Appendix B
ICEFISHX Notice

What follows is the text from the ICEFISHX registration forms. The registrant has to click on a separate box to agree and continue with the registration process. The notice explains the need to comply with the Privacy Policy.

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 MNJAC and those that the MNJAC disseminates for other agencies. Those terms include but are not limited to:
No portion of MNJAC documents should be released to the media or general public.
MNJAC documents contain data protected by state and federal law and are subject to distribution restrictions.
MNJAC authorization is required prior to disseminating any MNJAC 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.

Minnesota Joint Analysis Center Privacy Policy

Appendix C
List of Applicable Statutes

The following is a list of legal provisions that affect the operation of the Minnesota Joint Analysis Center (MNJAC), 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 be routinely 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

Minnesota Joint Analysis Center Privacy Policy

Appendix D

MNJAC Records Retention Schedule (unofficial compilation)

1. Schedule Number 012-014 **Date 8/3/**2011	**2. New** **Revision of** 09-141	**MINNESOTA RECORDS RETENTION SCHEDULE**
3. Agency **Department of Public Safety**	**4. Division/Section** Bureau of Criminal Apprehension Investigations Unit - Minnesota Joint Analysis Center (MNJAC)	**6. Page 1 of** **UNOFFICIAL - documents combined for ease of understanding**
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 ***Date*** **(signature)**	**11. Minnesota Historical Society, Director** **Date**
9. Type Name / Phone E. Joseph Newton 651-201-7170	**12. Legislative or State Auditor** **Date**
10. Agency Head or Designee **Date** **(signature)**	**13. Attorney General** **Date**

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 a 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
3	**Law Enforcement Brief** Weekly bulletin created by MNJAC staff to provide information to law enforcement agencies to help prevent and respond to terrorist activities	1 year		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
6	**MNJAC Assessments** Reports, incident briefs and research compiled by MNJAC staff for dissemination.	3 years		Yes	No
7	**Training files** Lesson plans, content of training provided by and to MNJAC staff	3 years		No	No
8	**Secure information-sharing platform participating agency documentation**	Purged when participant goes to inactive status		Yes	No
9	**ICEFISHX resource library materials**	3 years		No	No
10	**Dissemination log** Record of bulletins, briefs and assessments disseminated by MNJAC; includes copy of product, including recipient information	1 year		Yes	No
11	**Purge logs** Record of Suspicious Activity Reports purged from the records system; includes subject name, date of birth and submitting agency	5 years		Yes	No
12	**Grant documents** All documents required for grant applications and reporting	Current fiscal year plus 3 fiscal years after the final action or audit		No	No
13	**Personnel files** Emergency contact information, policy acknowledgments and training records	5 years after employee leaves MNJAC		No	No
14	**Significant event list** List of events or assemblies whose organizers or participants have a history of criminal activity or the event is a potential target of criminal or terrorist activity	3 years		Yes	No

15A	**Suspicious Activity Report** Electronic record whose source is reliable and verifiable, there is reasonable suspicion that criminal conduct is or could occur, the information was collected in a lawful manner and is accurate and current.	3 years		Yes	No
15B	**Suspicious Activity Report** Paper based record described in 15A	Until entered in the electronic records system		No	No
16A	**Information Sharing Environment Suspicious Activity Report (ISE SAR)** Electronic suspicious activity report that has a potential terrorism nexus.	3 years		Yes	No
16B	**Information Sharing Environment Suspicious Activity Report (ISE SAR)** Paper based suspicious activity report that has a potential terrorism nexus.	Until entered in the electronic records system		No	No
17	**Secure internal website accessed by MNJAC staff**	Until replaced		No	No
18	**Maps and related data found on secure information sharing platform** Maps, summary of the events, photographs, law enforcement contact information	1 year		Yes	No
19A	**Administrative files** Electronic records documenting data requests, general queries and other administrative records	1 year		No	No
19B	**Administrative files** Paper records documenting data requests, general queries and other administrative records	Until entered into electronic records system		No	No