

SOUTHEASTERN WISCONSIN Threat Analysis Center

Privacy Policy Version 1.8



This policy details the privacy procedures of the Southeastern Wisconsin Threat Analysis Center, participants and source agencies submitting, receiving, or disseminating criminal intelligence or criminal investigative information, including suspicious activity reports (SARs), to the Center and users of the ACISS, and eGuardian Systems.

Southeastern Wisconsin Threat Analysis Center Privacy Policy

Table of Contents

| | |
|----------------------------------------------|----|
| A. Intent | 4 |
| B. Background | 4 |
| C. Purpose | 4 |
| D. Policy Applicability and Legal Compliance | 5 |
| E. Membership of the STAC | 6 |
| F. Governance and Oversight | 6 |
| G. Definitions | 7 |
| H. Information | 7 |
| I. Acquiring and Receiving Information | 11 |
| J. Information Quality Assurance | 13 |
| K. Collation and Analysis | 14 |
| L. Merging Records | 14 |
| M. Sharing and Disclosure | 15 |
| N. Redress | 17 |
| N.1 Disclosure | 17 |
| N.2 Complaints and Corrections | 18 |
| O. Security Safeguards | 19 |
| P. Information Retention and Destruction | 20 |
| Q. Accountability and Enforcement | 20 |
| Q1. Information System Transparency | 20 |
| Q2. Accountability | 21 |
| Q3. Enforcement | 22 |

| | |
|---------------------------------|----|
| R. Training | 22 |
| Appendix 1 | 23 |
| Terms and Definitions | 23 |
| Appendix 2 | 35 |
| Intelligence Purge | 35 |
| Intelligence Purge Activity | 40 |
| Intelligence Purge Requirements | 41 |
| Purge Notifications | 42 |
| Case and Tip Review Process | 43 |

A. Intent

The Southeastern Wisconsin Threat Analysis Center (STAC) is committed to the responsible and legal compilation and utilization of criminal investigative and criminal intelligence information and other information important to protecting the safety and security of the people, facilities, and resources of the City of Milwaukee, the State of Wisconsin and the United States. All compilation, utilization, and dissemination of personal data by STAC participants and source agencies will conform to requirements of applicable state and federal laws, regulations and rules, and to the greatest extent practicable be consistent with Fair Information Practices. The intent of this policy is to ensure compliance with all privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines and the National SAR Initiative. All local, state, tribal and federal agencies providing suspicious activity reports (SAR) with a nexus to Wisconsin or participating with the Southeastern Wisconsin Threat Analysis Center by virtue of submitting, receiving or disseminating SAR information, criminal intelligence or criminal investigative information via the STAC are required to adhere to the requirements of the Southeastern Wisconsin Threat Analysis Center Privacy Policy.

B. Background

A Fusion Center is a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the Center with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity utilizing an all crimes/all hazards approach. The Southeastern Wisconsin Threat Analysis Center is inclusive of and a component within the City of Milwaukee Police Department's Intelligence Fusion Center, located in Milwaukee, Wisconsin. The STAC consists of City of Milwaukee Departments, federal agencies, state multi-disciplinary partners, local law enforcement, emergency service and criminal justice agencies. The STAC also engages in active outreach to private sector entities. Information utilized by the STAC includes suspicious activity reports documented by local, state, tribal and federal agencies in a variety of systems to include the SAR component of the ACISS System (hereafter "ACISS"). Suspicious activity is defined as: "Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Suspicious Activity Reports (SARs) are defined as "official documentation" of suspicious activity (See ISE Functional Standard for Suspicious Activity Reporting, Version 1.5). SARs are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the designated fusion center. SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

C. Purpose

To facilitate the prevention of crime, including terrorism, the STAC will be a participant in the National Suspicious Activity Reporting (SAR) Initiative (hereafter "NSI"). SARs with a nexus to terrorism (hereafter "ISE-SARs") will be provided to the NSI and placed into the shared space (data repository) by the STAC after appropriate review by STAC personnel. The shared space is a networked data and information repository which is under the control of submitting agencies

and provides ISE-SAR information, applications, and services to other NSI participants. Many of these ISE-SARs will be documented initially as SARs by source agencies within the ACISS system. SARs with no nexus to terrorism (ISE-SARs), as determined by STAC, will not be provided to the NSI, will be deleted from the STAC information repository and will be destroyed consistent with the STAC record retention schedule.

The purpose of this privacy policy is to promote STAC, source agency, and user agency (hereafter collectively referred to as “participating agencies” or “participants”) conduct which complies with federal, state, local and tribal laws, regulations, and policies applicable to information and intelligence collection, use, and sharing and assists them in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Increasing public safety and national security while maintaining appropriate levels of operational transparency.
- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to public safety agencies.

D. Policy Applicability and Legal Compliance

All STAC personnel, IT personnel, private contractors, and other authorized users will comply with applicable provisions of the STAC’s privacy policy concerning the information the center collects, receives, maintains, archives, accesses, or discloses to center members, governmental agencies, and participating agencies, as well as to private contractors and the general public. This includes SAR information that source agencies collect and the STAC receives as well as ISE-SAR information identified, submitted to the shared space, and accessed by or disclosed to STAC personnel. All STAC members are operating under a Memorandum of Understanding and each member is required to sign a non-disclosure agreement to participate. These documents are physically maintained in the STAC. All agencies providing criminal intelligence or SAR information to ACISS are operating under Agency User Agreements and Individual User Agreements, which are physically maintained by the State of Wisconsin Division of Criminal Investigation in Madison, Wisconsin.

All members of the STAC are required to review the Privacy Policy. All participants and source agencies, to include all individual users of ACISS are required to review and adhere to the Privacy Policy. The STAC will provide a printed copy of this policy upon request to all entities participating in the STAC and will require a written acknowledgement to comply with this policy and the provisions it contains. The Privacy Policy will also be posted to the STAC’s public SAR website “WiWATCH.”

All STAC personnel, participating agency members and personnel providing information technology services to the agency, private contractors, ACISS users, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties as listed in the following paragraph and defined in Appendix 1.

The STAC has adopted internal operating policies and/or procedures that are in compliance with applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, the U.S. and Wisconsin Constitutions; Wis. Stat. §§ 19.31-19.37 (Wisconsin public records law); Wis. Stat. § 19.62-19.80 (personal information practices); Wis. Stat. § 100.525 (Telephone records; obtaining, selling, or receiving without consent); Wis. Stat. § 134.98 (Notice of unauthorized acquisition of personal information); Wis. Stat. § 230.13 (Closed records); Wis. Stat. § 323 (Emergency Management); Wis. Stat. § 943.201 (Unauthorized use of an individual's identifying information); Wis. Stat. § 943.203 (Unauthorized use of a business's identifying information); Wis. Stat. § 995.50 (Right of privacy);

E. Membership of the STAC

All local and state agencies participating in operations of the STAC must enter into a memorandum of understanding (MOU) with the STAC outlining and agreeing to the terms for such participation. An MOU with federal agencies participating in the STAC will also be secured.

Members assigned to the STAC will be expected to participate in a capacity as deemed appropriate by the member's agency and will have the ability to be virtually connected to the STAC. Agencies utilizing ACISS are considered contributors or source agencies for the STAC.

F. Governance and Oversight

Primary responsibility for the operation of the STAC is assigned to the Milwaukee Police Lieutenant Jason Smith, who has been assigned as the "Commander" of the STAC and is under the direct command of a Milwaukee Police Department Captain (Commander of the Intelligence Fusion Center) who in turn reports to the Assistant Chief of Police for the Criminal Investigation Bureau. The STAC Commander (or their designee) will have the responsibility for coordinating personnel from the STAC and other agencies involved in the NSI. Each person assigned to the STAC, users of ACISS or participants utilizing STAC resources are personally responsible and will be personally accountable for adhering to this policy, maintaining information standards, processes, procedures and practices. Individuals assigned to the STAC from outside agencies are also bound by the Non-Disclosure Agreement.

The Commander of the STAC has designated a Privacy Officer for STAC. The Privacy Officer has been tasked with responsibility for STAC information privacy issues, including implementation of Privacy Policy requirements related to the ISE, periodic privacy policy review and update, and handling reports and complaints regarding alleged errors and Privacy Policy violations. The Privacy Officer shall be trained and will receive assistance from a staff attorney assigned by the City Attorney's office for the City of Milwaukee, who shall collaborate with community privacy advocacy groups to ensure that privacy and civil rights are appropriately protected by the center's information acquisition, dissemination and retention practices as

defined by STAC's written policy and implemented through training of those operating within the STAC.

G. Definitions

For primary terms and definitions, refer to Appendix 1, Terms and Definitions.

H. Information

1. The STAC will seek or retain information that:

- Is based upon reasonable indication that the information constitutes a credible criminal predicate or a potential threat to public safety; or
- Is based upon reasonable suspicion that an identifiable individual or organization has committed, is committing, or is planning to commit criminal conduct or activity that presents a threat to any individual, the community, or the nation; or
- Is relevant to an active or ongoing investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort; and
- Is such that the source of the information is reasonably believed to be reliable and is verifiable or, when appropriate, the limitations on the reliability or veracity of the information are clearly stated; and
- Is information that was collected in a fair and lawful manner, not otherwise prohibited by law, and with the consent of the affected individual to share the information being clearly noted when such consent has been provided.

2. The STAC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate, or prevent criminal activity and that information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal relationship exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or STAC personnel to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information. No personally identifiable information will be gathered or collected, retained and shared by the STAC unless it is authorized open source information or commercial data, SAR information, criminal intelligence information, information gathered as part of an authorized investigation, or information related to the arrest or conviction of any individual.

3. The STAC may retain protected information that is based on a level of suspicion that is less than “reasonable suspicion,” such as tip and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy within ACISS or contributed to the shared space only for the length of time allowed under the retention limitations established by the ACISS Operating Guidelines, and as defined in the STAC record retention schedule. As a general rule, SARs should be reviewed and evaluated for contemporaneous value within 90 days and purged within a two year window of inactive status. In addition, STAC may require a contributing agency to justify why any particular tip, lead, or SAR should remain in the system if it appears to STAC that the information is no longer active or otherwise of intelligence or investigative value. Failure to satisfy STAC’s request may result in the information being unilaterally removed from the system by STAC. Notice of any such removal will be made to the contributor.
4. The STAC will identify and review protected information that is originated by the STAC prior to sharing that information in the ISE.
5. The STAC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
 - The name of the originating department, component, and subcomponent.
 - The name of the agency’s justice information system from which the information is disseminated
 - The date the information was collected and, to the extent possible, the date its accuracy was last verified.
 - The title and contact information for the person to whom questions regarding the information should be directed and who is accountable for the decision to submit the information and assuring it is believed to otherwise conform to STAC submission standards.
6. The STAC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.
7. Prior to allowing access to or dissemination of the information, STAC participating agency personnel will assess the information to validate or refute the information, as well as, assessing the information for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The STAC will use a standard reporting format and data collection codes for SAR information. Members of the STAC will assign information to categories to indicate the result of the assessment, such as:

- Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence information;
 - The nature of the source (for example, anonymous tip, interview, public records, private sector);
 - The reliability of the source
 - **Reliable** – the source has been determined to be reliable
 - **Unreliable** – the reliability of the source is doubtful or has been determined to be unreliable
 - **Unknown** – the reliability of the source cannot be judged or had not as yet been assessed
 - The validity of the content
 - **Confirmed** – the information has been corroborated by a trained law enforcement analyst or officer or other reliable source
 - **Doubtful** – the information is of questionable credibility but cannot be discounted based on the knowledge and skills of the reviewer
 - **Cannot be judged** – the information cannot be confirmed at the time of review
 - Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be “unknown” and content validity “cannot be judged.” In such case, users must independently confirm source reliability and content validity with the source or submitting agency or through their own investigation.
 - Due diligence will be exercised by source or submitting agency as well as STAC personnel in determining source reliability and content validity. STAC personnel may reject information as failing to meet any criteria for inclusion, and return such information to the submitting party with an indication of why it was rejected.
 - Information determined to be unfounded will be purged from WIN and from the shared space.
8. The STAC participating agency personnel upon receipt of designated SAR information will:
- Review and vet the SAR information and provide the two-step assessment set forth in the current version of the SAR Functional Standard to determine whether the information qualifies as an ISE-SAR for contribution to the shared space
 - Provide appropriate reliability and validity labels

- Pursuant to ACISS Operating guidelines, all ISE-SARs provided via the ACISS system will be contributed to the shared space unless the source agency requests otherwise.
 - No personally identifying information shall be attached to any SAR unless there exists reasonable suspicion to investigate or arrest.
9. At the time a decision is made to retain information in STAC databases, including contributing ISE-SAR information to the shared space, STAC personnel or source agency personnel will label it (by record, data set, or system of records and to the extent feasible, consistent with the current version of the SAR Functional Standard) pursuant to applicable limitations on access and sensitivity of disclosure in order to:
- Protect an individual’s right of privacy and civil rights and civil liberties;
 - Protect confidential sources and police undercover techniques and methods;
 - Not interfere with or compromise pending criminal investigations; and
 - Provide any legally required protection based on the individual’s status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter, etc.
10. At the time information is retained, the date of review of such information to determine whether it should be purged or continued to be retained will be noted (this can be done electronically via date stamping within the ACISS system).
- Records that are five years old and determined to be no longer active intelligence or criminal investigative information will be purged in accordance with approved records retention schedules, with only statistical information being kept.
 - Tip or SAR information will be reviewed 90 days after entry to make a determination of its status. Tips that are determined not to be valid will be purged from the system. Tips that are unsubstantiated within a two year period will be reviewed to determine if the records should be purged from the system.
11. The retention or classification of existing information will be reevaluated whenever:
- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
 - New information is gathered that has an impact on confidence (source reliability and content validity) in the information.
 - There is a change in the use of the information affecting access or disclosure limitations.
 - Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

12. STAC members are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tips and leads and suspicious activity reports (SARs) information.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information. The storage of STAC SAR's will be through the ACISS system.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of tips, leads, and SAR information to other entities or individuals, including the public, when credible information indicates potential imminent danger to life or property.
- Retain information long enough to work a tip or lead to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows that status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SARs will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.
- Routinely and regularly review information to determine if it should be purged.

I. Acquiring and Receiving Information

1. The STAC will keep a record of the source of all information retained by the center.
2. Information gathering and investigative techniques used by the STAC and affiliated agencies will comply and adhere to the following regulations and guidelines:
 - The center will follow 28 CFR Part 23 with regard to criminal intelligence information.
 - The center will adhere to criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
 - The center will adhere to the obligations of law, including Wisconsin Statutes (Wisconsin's Public Records Law), as well as any regulations that apply to multi-jurisdictional intelligence databases.

- The center will adhere to emergency government guidelines and all other state and federal laws related to Homeland Security.
3. The STAC's 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. Law enforcement officers and STAC personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
 4. The STAC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in behaviors that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties (e.g., race, culture, religion, or political associations) will not be intentionally or inadvertently gathered, documented, processed, and shared.
 5. Regardless of the criminal activity involved, no information which a user has reason to believe may have been obtained in violation of law shall be entered into ACISS or submitted to or received by the STAC. If the STAC is notified or otherwise learns that information has been obtained illegally, it will be removed.
 6. Agencies which participate in the STAC and which provide information to the center are governed by state and local laws and rules governing them, as well as by applicable federal laws. The STAC will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, tribal, territorial, and federal laws and regulations and that such gathering is not based on misleading information collection practices.
 7. The STAC will not directly or indirectly receive, seek, accept, or retain information from:
 - An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; or
 - The source used prohibited means to gather the information.
 8. Law enforcement officers and personnel at source agencies and the STAC who acquire SAR information that may be shared with the STAC will be trained to recognize behavior that is indicative of criminal activity related to terrorism. The responsibility for this training resides with the contributing agency.
 9. When a choice of investigative techniques is available, information, including information documented as a SAR or ISE-SAR, should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.
 10. Access to and use of ISE-SAR information is governed by the U.S. Constitution, the Wisconsin Constitution, applicable federal and state laws and local ordinances, and the

Office of the Program Manager for the Information Sharing Environment (PM-ISE) policy guidance applicable to the ISE-SAR EE initiative.

J. Information Quality Assurance

1. To the maximum extent practical, the STAC will implement the “Fair Information Practices” as detailed by the Department of Justice’s Global Initiative, recognizing that some of the practices (such as allowing individuals about whom information is retained to review the information for accuracy) do not apply to an intelligence-gathering initiative. All contributors of information to the STAC should be familiar with the Global “Fair Information Practices” and will apply those practices to the best extent practicable to the information gathered, retained and reported to the STAC.
2. The STAC will make every reasonable effort to ensure that information sought or retained, to include ISE-SAR information is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.
3. At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).
4. State, Local, and Tribal (SLT) agencies, including agencies participating in the Information Sharing Environment (ISE), are primarily responsible for the quality and accuracy of the data accessed by or shared with the center, to include SAR data. Data, including ISE-SAR information, that is to be retained or posted to the shared space, will be labeled according to the level of confidence in the information to the maximum extent feasible. The labeling of all information, including ISE-SAR information, will be periodically evaluated and updated in the shared space when new information is acquired that has an impact on confidence in the information. Originating agencies providing data remain the owners of the data contributed.
5. Information provided through ACISS, the shared space or by the STAC is not designed to provide users with information upon which official actions may be taken. The mere existence of records in ACISS or the shared space or provided by the STAC should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant or serve as documentation in court proceedings. Only the facts, which led to the entry of the record into ACISS or the shared space, can be used to establish probable cause in an affidavit. The source agency should be contacted to obtain and verify the facts needed for any official action.
6. The STAC will investigate, in a timely manner, alleged errors and deficiencies to data, including ISE-SAR information, and will correct, delete, or refrain from using protected information found to be erroneous or deficient. The STAC will advise the appropriate data owner in writing (to include electronic notification) if its data contributed to the STAC, ACISS, or the shared space is found to be inaccurate, incomplete, out of date, or unverifiable. In addition, STAC will provide documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed

by STAC because it is erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of an individual data subject may be affected. Any needed corrections to or deletions made to ISE-SAR information will be made to such information in the shared space.

7. ISE-SAR information will be removed from the shared space if it is determined the source agency did not have the authority to acquire the original SAR information, used prohibited means to acquire it, or did not have the authority to provide it to the STAC or the ACISS system. Information subject to an expungement order in state or federal court that is enforceable under state law or policy will also be removed from ACISS and the shared space.

K. Collation and Analysis

1. Information acquired by the STAC, to include ISE-SAR information, or accessed from other sources will only be analyzed by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
2. Information acquired by the STAC as described in Section H of this policy, including ISE-SAR information, is analyzed according to priorities and needs and will only be analyzed to:
 - Further crime/terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by the STAC, and
 - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities, including criminal solicitations, criminal conspiracies, and/or attempts to obstruct justice.

L. Merging Records

1. Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match.
2. Sufficient identifying information may include the name (full or partial) and in most cases, one or more of the following:
 - Date of Birth;
 - Law Enforcement or Corrections System Identification Number;
 - Individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars;
 - Social Security Number;

- Driver’s License Number; or
- Other biometrics, such as DNA, retinal scan, or 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. The reality that identities can be stolen by those who perpetrate crimes makes the verification of factors in support of merging of records particularly important. Innocent individuals’ identities may be utilized by criminals and merging of an innocent individual’s information into records related to the criminal without explanation or other appropriate safeguards against misinterpretation of the information should not occur.

3. If the matching requirements are not fully met but there is an identified 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 and a reminder that identity theft may be the reason there has been the partial match.

M. Sharing and Disclosure

1. Credentialed security access will be utilized to control:
 - What information a class of users can have access to;
 - What privacy fields in ISE-SAR shared space a class of users have access to;
 - What information a class of users can add, change, delete, or print; and
 - To whom the information can be disclosed and under what circumstances.
2. Personal identifiable information (such as social security numbers) will be removed from disseminated products as appropriate, specifically when dissemination includes non law enforcement entities.
3. Agencies contributing information to the STAC will indicate at the time of submission the intent to have said information disseminated by STAC to other appropriate fusion or criminal justice partners. In the absence of a request for additional dissemination, the STAC will operate according to the Third Agency Rule unless otherwise instructed by law, rule or Memorandum of Understanding, therefore, STAC participating agencies may not unilaterally disseminate information received from STAC without approval from the originator of the information. There is a presumption that all records contributed to ACISS and the shared space are intended to be shared with other agencies participating in said systems.
4. Records retained by the STAC may be accessed or disseminated *within the STAC or to those responsible for law enforcement, public health and safety protection, prosecutions, or justice purposes derived from criminal investigations or prosecutions* only for such purposes and then only in the performance of official duties in accordance with applicable laws, regulations, and procedures. An audit trail will be kept of access by or dissemination of

information within the STAC or to such persons. Information gathered and records retained by the STAC may be accessed or disseminated *for specific purposes* upon request by persons authorized by law to have such access and only for those users or purposes specified by law.

5. As long as information constitutes active criminal investigative or active criminal intelligence information, or is otherwise within the scope of an applicable exemption or confidentiality provision of Wisconsin law, information gathered and records retained by the STAC, to include ISE-SAR information and those records within ACISS and the shared space, will not be released to the public. ISE-SAR information posted to the shared space by the STAC may be disclosed to a member of the public only if the information is defined by law to be public record or otherwise appropriate for release to further the STAC mission and is not exempt from disclosure by state or federal law, or overriding policy reason. A log of requests, that includes the date of inquiry, requesting persons name and address, the type of information being requested, the date the request was filled or denied and by whom, shall be maintained at the STAC. (WI §19.36)
6. The STAC shall not confirm the existence or nonexistence of information, to include ACISS records or ISE-SAR information to any person or agency that would not be eligible to receive the information itself. ISE-SAR information will not be provided to the public if, pursuant to applicable law (WI §19.36) it is:
 - Required to be kept confidential or exempt from disclosure.
 - Classified as investigatory records and exempt from disclosure.
 - Protected federal, state, or tribal records originated and controlled by the source agency that cannot be shared without permission.
 - A violation of an authorized nondisclosure agreement.
7. Information that is no longer active criminal investigative or active criminal intelligence information will be promptly purged in a manner consistent with Wisconsin law and regulation.
8. Information gathered and records retained by the STAC will not be sold, published, exchanged, or disclosed for commercial purposes. It will not be disclosed or published without prior notice to the contributing agency. Information will not be disseminated to unauthorized persons.
9. Information gathered and records retained by the STAC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the STAC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the laws of the State of Wisconsin for this type of information. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.
10. There are several categories of records that will not ordinarily be provided to the public under Wisconsin Law:

- Wis. Stat. §§ 19.36 (1) Application of Other Laws;
- Wis. Stat. §§ 19.36 (2) Law Enforcement Records;
- Wis. Stat. §§ 19.36 (3) Contractors’ Records;
- Wis. Stat. §§ 19.36 (4) Computer Programs and Data;
- Wis. Stat. §§ 19.36 (5) Trade Secrets;
- Wis. Stat. §§ 19.36 (6) Separation of Information;
- Wis. Stat. §§ 19.36 (7) Identities of Applicants for Public Positions;
- Wis. Stat. §§ 19.36 (8) Identities of Law Enforcement Informants;
- Wis. Stat. §§ 19.36 (9) Records of Plans or Specifications for State Buildings;
- Wis. Stat. §§ 19.36 (10) Employee Personnel Records;
- Wis. Stat. §§ 19.36 (11) Records of Individual Holding a Local Public Office or a State Public Office;
- Wis. Stat. §§ 19.36 (12) Information Relating to Certain Employees;
- Wis. Stat. §§ 19.36 (13) Financial Identifying Information;
- Wis. Stat. § 100.525 Telephone records; obtaining, selling, or receiving without consent;

N. Redress

N.1 Disclosure

1. Information that is retained by the STAC, to include ACISS records and ISE-SAR information, is considered active intelligence or criminal investigative information and, therefore, is exempt from public disclosure. If an individual wants to review information that has been documented in an intelligence file or system or as part of an investigative case management system, a formal public records request must be made via the STAC. Public requests will be processed by STAC, who may contact the City Attorney’s office for legal advice and assistance as necessary. STAC and all participating agencies will refer complaints and redress issues to the Wisconsin Department of Justice, or as otherwise provided by law. A copy of any referrals will be kept by the referring agency.
2. The existence, content, and source of the information will not be made available to an individual (when there is legal basis for denial). To the extent allowed by law, information will not be verified or released if (WI §19.36):
 - The disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;

- The disclosure would endanger the health or safety of an individual, organization, or community;
- The information is in a criminal intelligence system;
- The information is classified under federal law.
- The information source does not reside with the STAC;
- The STAC did not originate or does not have a right to disclose the information; or
- The information is exempt from disclosure by other statutory, common law or public policy reasons, to be determined on a case-by-case basis.

N.2 Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information about him or her *originating with the agency*, including information that may be shared through the ISE, should be made in writing and handled through the STAC, with assistance from the City Attorney's office as necessary. The individual would be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request pursuant to Wis. Stat. § 19.365. The information would then be submitted to the STAC for consideration.
2. If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, including information that is shared through the ISE, the STAC's privacy official or designee will notify the originating agency of the complaint or request for correction and coordinate with the originating agency to assist the individual with complaint and corrections procedures. A record will be kept of all such complaints and requests for corrections and the resulting action taken, if any. Complaints must be directed to the Privacy Officer of the Southeastern Wisconsin Threat Analysis Center at the following address: 749 West State Street, Milwaukee, WI 53233.
3. If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the STAC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the STAC will inform the individual of the procedure for submitting (if needed) and resolving complaints or objections. Complaints should be directed to the STAC Privacy Officer at the following e-mail address: ifc@milwaukee.gov. The STAC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure, as permitted by law. If the information did not originate with the STAC, STAC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies, subject to applicable records retention procedures, or to verify that the record is accurate. Any personal information originating with the STAC will be reviewed and corrected in or deleted from STAC data/records according to applicable records retention procedures if it is determined to be erroneous, include incorrectly merged information, or out of date. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

4. An individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the STAC including ISE participating agencies, and be informed of any existing procedure for appeal.
 - To delineate protected information shared through the ISE from other data, the STAC maintains records of agencies sharing terrorism-related information and audit logs and employs system mechanisms to identify the originating agency when the information is shared.

O. Security Safeguards

1. The Commander of the STAC has designated a sworn STAC member, to serve as the security officer. The security officer shall receive appropriate training to support the security needs of the Southeastern Wisconsin Threat Analysis Center.
2. The STAC will operate in a secure facility protecting the facility from external intrusion. The STAC will utilize secure internal and external safeguards against network intrusions, to include ISE-SAR information and ACISS records. Access to STAC databases, to include ACISS and the ISE-SAR shared space, from outside the facility will only be allowed over secure networks.
3. The STAC will store information, to include ACISS records and ISE-SAR information, in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
4. Access to STAC information, to include ACISS records and ISE-SAR information, will only be granted to STAC members whose position and job duties require such access and who have successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.
5. Queries made to the STAC data applications, to include ACISS and the ISE-SAR shared space, will be logged into the data system identifying the user initiating the query. The STAC will utilize watch logs to maintain audit trails of requested and disseminated information. To prevent inadvertent public records disclosure that would be unlawful or harmful to the public, risk and vulnerability assessments will not be stored with publicly available data.
6. The STAC will, in the event of a data security breach, consider notifying an individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person as required by law. Any notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the breach or any measure necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system.

P. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. When information has no further value or meets the criteria for removal according to the STAC Operating Guidelines and the STAC retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the contributing agency. Notification of proposed destruction of records will be provided to the contributor during the review period.
2. The procedure contained in Wis. Stat. §§ 19.21 will be followed for notification of appropriate parties before information is destroyed or returned.
3. A record of information to be reviewed for retention will be maintained by the STAC, and for appropriate system(s), notice will be given to the individual submitting the information at least 30 days prior to the required review and validation/purge date. Agreement to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period.
4. The STAC will retain ISE-SAR information in the shared space for a sufficient period of time to permit the information to be validated or refuted, its credibility and value to be reassessed, and to the degree possible a “disposition” label will be assigned so that subsequent authorized users know the status and purpose for the retention.
5. All SAR information contained in ACISS and contributed to the shared space by the STAC will be reviewed 90 days after entry to make a determination of its status. SARs that are determined not to be valid will be purged from the system. SARs that are unsubstantiated within a two year period will be reviewed to determine if the records should be purged from the system. All SAR information contained in ACISS and the shared space will follow the procedures defined for review and purge in the ACISS Operating Guidelines and listed as Appendix 2 to this policy.

Q. Accountability and Enforcement

Q1. Information System Transparency

1. The STAC will be open with the public in regard to information and intelligence collection practices. The STAC’s privacy policy will be provided to the public for review via the STAC public website (www.WiWATCH.org).
2. The STAC in consultation with the Milwaukee Police Department and the Milwaukee City Attorney’s office will be responsible for receiving and coordinating a response to inquiries and complaints about privacy, civil rights, and civil liberties protections related to ISE-SAR information, ACISS and the operations of the Southeastern Wisconsin Threat Analysis Center.

Q2. Accountability

1. The STAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. These procedures will be incorporated into the STAC Policy Manual.
2. The Milwaukee Police Department and STAC will have access to an audit trail of inquiries to and information disseminated from the shares space and ACISS.
3. An audit log of queries to the ISE-SAR information and ACISS records will identify the user initiating the query. STAC will adopt and follow procedures and practices to evaluate the compliance of authorized users of ACISS and ISE-SAR information to policy and applicable law. The STAC will conduct these audits. This will include random annual audits of logged access to all STAC systems including the shared space in accordance with audit obligations within the EE Initiative. Records of audits will be maintained by the STAC. Any audits conducted will be in such a manner as to protect the confidentiality, sensitivity, and privacy of the ISE-SAR information and ACISS records as well as any related documentation.
4. The members of the STAC or other authorized users of ACISS or the shared space may report violations or suspected violations of Privacy Policy to the STAC Commander or STAC Privacy Officer.
5. If an authorized user is found to have violated the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the STAC may, in consultation with the Wisconsin Department of Justice or the Milwaukee Police Department and the Milwaukee City Attorney's office:
 - Suspend or discontinue access to information by the user;
 - Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
 - Apply administrative actions or sanctions as provided by applicable personnel rules and regulations or as provided in agency personnel policies;
 - If the user is from an agency external to the center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
 - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.
6. The STAC's Governance Board in consultation with the Commander of the STAC and the Milwaukee Police Department, will annually review and update as appropriate, the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

Q3. Enforcement

The STAC reserves the right to restrict the qualifications and number of personnel having access to STAC information, to include ISE-SAR information and ACISS records, and to suspend or withhold service to any personnel violating the privacy policy. The STAC reserves the right to deny access to ACISS, STAC products or ISE-SAR information to any participating agency or individual user who fails to comply with the applicable restrictions and limitations of the STAC privacy policy.

R. Training

1. All participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to ACISS, the STAC, or having access to the shared space and ISE-SAR information should participate in training programs regarding implementation of and adherence to privacy, civil rights and civil liberties policies and protections pertinent to the scope of their employment and access to said information, including training regarding the sharing of protected information through the Information Sharing Environment.
2. All users of ACISS, participants and source agencies of the STAC and those with access to the ISE-SAR shared space must adhere to this privacy policy and acknowledge observance through a signed user agreement or acknowledgement form.
3. The privacy policy will be posted on the STAC public website for review. All STAC staff with access to criminal intelligence or criminal investigative information, including personal data shared in the ISE and STAC members are required to attend training regarding privacy, civil rights and liberties as determined by the Commander of the STAC, the Privacy Officer, and the Governance Board. These trainings will include the following:
 - Purpose of the Privacy Policy
 - Substance and intent of the provisions of the policy relating to the collection, use, analysis, retention, destruction, sharing and disclosure of SAR and ISE-SAR information
 - 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, to include criminal liability.

Appendix 1

Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the fusion center privacy policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. For data access, access is usually specified as read-only access and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency/Center—Agency/Center refers to the Southeastern Wisconsin Threat Analysis Center or STAC and all participating local, state or federal agencies of the STAC.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center – Center refers to the Southeastern Wisconsin Threat Analysis Center or STAC

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights and the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.

Civil Rights—The term “civil rights” is used to imply that the state (or government) has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security—Protection of information assets through the use of technology, processes, and training.

Confidentiality—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials—Information that includes identification and proof of identification that is utilized by STAC members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates. Credentialed security access will be utilized to control:

- What information a class of users can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably

suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Elements of information, inert symbols, signs or measures.

Data Protection—Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail.

STAC Governance Board- Oversight body comprised of representatives from agencies participating in the STAC.

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")
2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")
3. Ensure data accuracy. ("Data Quality Principle")
4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")

5. Maintain effective security over personal information. (“Security Safeguards Principle”)
6. Promote a general policy of openness about agency practices and policies regarding personal information. (“Openness Principle”)
7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. (“Individual Participation Principle”)
8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. (“Accountability Principle”)

Firewall—a security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity. The STAC is the designated Southeast Wisconsin.

General Information or Data—Information that could include records, documents, or files pertaining to law enforcement operations, such as Computer Aided Dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Advisor- Coordinates the efforts in the ongoing assessment of Wisconsin’s vulnerability to, and ability to detect, prevent, prepare for, respond to, and recover from acts of terrorism within or affecting this state. Appointed by the Governor and acts in the command position on issues involving homeland security for the State of Wisconsin.

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

Identification—a process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a compound of such data as a given and family name, date of birth, and address. An organization’s identification process comprises the acquisition of the relevant identifying information.

Individual Responsibility—since a privacy notice is not self-implementing, an individual within an organization’s structure must also be assigned responsibility for enacting and implementing the notice.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, tips and leads data, and criminal intelligence data.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Invasion of Privacy—Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Information Sharing Environment (ISE)— An approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)]. The ISE is to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. [Extracted from IRTPA 1016(b)(2)]

ISE-SAR—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.

ISE-SAR Information Exchange Package Documentation (IEPD)—A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

1. The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.
2. The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both

(A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associate with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation or accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—The maintenance of information applies to all forms of information storage. This would include electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular content. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based upon the type of information and context of use.

Need to Know— As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Non-repudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Participating Agencies—Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR) information], submitting (the agency or entity posting ISE-SAR information to the shared space), and user (an

agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data—Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother’s maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver’s license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines “United States persons” as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, “persons” means United States citizens and lawful permanent residents.

Privacy—Privacy refers to individuals’ interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical

interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Fields—Data fields in ISE-SAR IEPDs that contain personal information.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing. The process should maximize the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Probable Cause— Facts and circumstances leading to an arrest or seizure must be sufficient to persuade a reasonable person that an illegal act has been or is being committed. Always the test involves the consideration of a particular suspicion and a specific set of facts. Hunches or generalized suspicions are not reasonable grounds for concluding that probable cause exists.

Protected Information—For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, it would include applicable state and tribal constitutions and State, Local and Tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about “United States persons” as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency’s information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

Public Access—Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

Reasonable Suspicion— the U.S. Supreme Court defines reasonable suspicion as “the sort of common-sense conclusion about human behavior upon which practical people...are entitled to rely.” Further, it has defined reasonable suspicion as requiring only something more than an “unarticulated hunch.” It requires facts or circumstances that give rise to more than a bare, imaginary, or purely conjectural suspicion.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—internal procedures to address complaints from persons regarding protected information about them that is under the agency’s control.

Repudiation—the ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention—Refer to “Storage.”

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—the possible right to be left alone, in the absence of some reasonable public interest in a person’s activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

Role-Based Authorization/Access—A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized

users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Space—A networked data and information repository which is under the control of the STAC and takes in information and intelligence from submitting agencies which provide terrorism-related information, applications, and services to other ISE participants.

Sharing—The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

SLT—State, Local and Tribal

Storage—in a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided in (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other “built-in” devices such as the processor’s L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.
3. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.
4. With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Source Agency—the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Submitting Agency—the agency or entity providing ISE-SAR information to the shared space.

Suspicious Activity—Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs) — Reports that record the documentation of a suspicious activity. Suspicious activity reports (SARs) are meant to offer a standardized means for feeding information repositories or data mining tools. Any patterns identified during SAR data mining

and analysis may be investigated in coordination with the reporting agency and the state designated fusion center. Suspicious activity reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of IRTPA, all information relating to the (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (C) communications of or by such groups or individuals, of (D) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism Related Information—In accordance with IRTPA, as recently as amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of “terrorism information,” as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute “terrorism information”: (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not, technically be cited or referenced as a fourth category of information in the ISE.

Third Agency Rule—A traditionally implied understanding among criminal justice agencies that confidential criminal intelligence information, which is exempt from public review, will not be disseminated without the permission of the originator.

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data.

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information hangs between being of no use

to law enforcement and being extremely valuable if time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

User Agency—The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the shared space(s), which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

Vet/Vetting – A two-part process by which a trained law enforcement officer or analyst, to include STAC personnel, determine the usefulness of a SAR. This process entails checking the facts reported in the SAR as well as ensuring that the SAR meets the set of requirements defined in the current version of the SAR Functional Standard. The first step in the vetting process is for a trained officer or analyst at a Fusion Center to determine whether suspicious activity falls within the criteria set forth in Part B – ISE-SAR Criteria Guidance of the current version of the SAR Functional Standard. These criteria describe behaviors and incidents identified by law enforcement officials and counterterrorism experts from across the country as being indicative of criminal activity associated with terrorism. The second step in the vetting process is for a trained expert to determine, based on a combination of knowledge, experience, available information, and personal judgment whether the information has a potential nexus to terrorism.

Wisconsin Privacy Statutes –

Wis. Stat. §§ 19.31-19.37 (Wisconsin public records law);

Wis. Stat. § 19.62-19.80 (personal information practices);

Wis. Stat. § 100.525 (Telephone records; obtaining, selling, or receiving without consent);

Wis. Stat. § 134.98 (Notice of unauthorized acquisition of personal information);

Wis. Stat. § 230.13 (Closed records);

Wis. Stat. § 323 (Emergency Management);

Wis. Stat. § 943.201 (Unauthorized use of an individual’s identifying information);

Wis. Stat. § 943.203 (Unauthorized use of a business’s identifying information);

Wis. Stat. § 995.50 (Right of privacy);

Appendix 2

Intelligence Purge

The Intelligence Purge Module in ACISS Web allows an operator to purge records from the system based on activity in the system. The guidelines for purging records can vary with each Agency and the ACISS System Administrator will customize the requirements for the Agency. Intelligence Purge manages archived records for Cases, Subjects, and Tips.

The Intelligence Purge Module utilizes a batch system as the core of its functionality. Operators will gather records subject to purge in groups which can be saved and edited before being committed permanently to the database. These batches are also stored and searchable for auditing purposes.

The Intelligence Purge system will consider the security of the operator executing the purge batch. Only records that the operator would normally have access to view will be included in the batch. It is recommended that this process be managed by personnel with sufficient access to all records eligible for purge.

1. To start a batch, the user may simply click “Add” (ALT+A) or batches can be searched using the Intelligence Purge Batch search screen. In the Intelligence Purge Module, a batch can have one of three status types – Not Initialized, Pending, and Executed.

Not Initialized: A batch was created but no records were added before the batch was closed. Batches of this type may be opened and used to add records and proceed with a purge.

Initialized: A batch was created and records were included, but the batch was not executed. This is useful because it allows the operator to gather records subject to purge and allow them to be reviewed by other users before being purged completely.

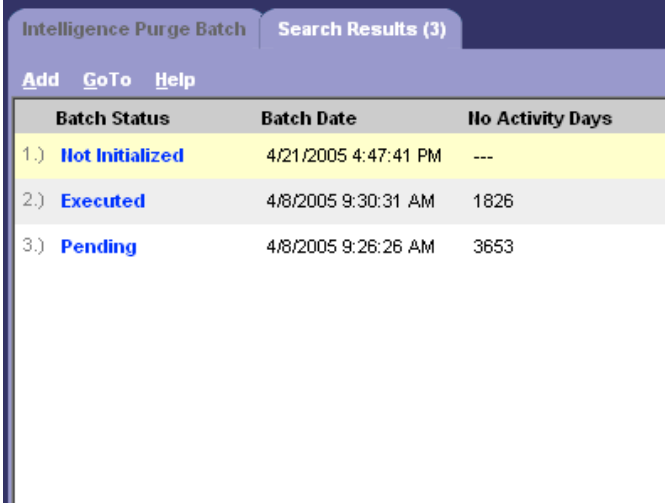
Executed: A batch was created, records were added, and those records were purged from the system. This type of batch can be revisited at a later date for auditing purposes.

The screenshot shows the 'Intelligence Purge Batch' search interface. It features a blue header with two tabs: 'Intelligence Purge Batch' and 'Search Results'. Below the header, there are three navigation links: 'Search', 'Add', and 'Help'. The main content area contains four input fields:

- Batch Status:** A dropdown menu.
- Begin Batch Date:** A date picker.
- End Batch Date:** A date picker.
- Max Results:** A dropdown menu with '100' selected.

2. After providing search criteria, any matching results are displayed. Results are displayed with the most recent batch first and show Batch Status, Batch Date/Time, No Activity Days, and Last Update Operator. At any point in the search process, a user may click the Add button to create a new batch. Unlike most of the modules in ACISS Web, the Intelligence

Purge does not require the operator to search for existing records before adding a new one to the system.



| | Batch Status | Batch Date | No Activity Days |
|-----|-----------------|----------------------|------------------|
| 1.) | Not Initialized | 4/21/2005 4:47:41 PM | --- |
| 2.) | Executed | 4/8/2005 9:30:31 AM | 1826 |
| 3.) | Pending | 4/8/2005 9:26:26 AM | 3653 |

3. Clicking Add will bring the user to batch criteria screen. All Intelligence Purge batches will have a status of Not Initialized when they are first created and will continue to have this status until the Initialize button is clicked. Clicking the Initialize button after providing all required criteria will add matching records to the batch and change its status to Initialized. Clicking the Close button will exit this screen and no records will be included in the batch. The batch itself will still exist in the system with a status of Not Initialized and can be re-opened to include records at a later date. The following criteria are available on this screen:

Purge Cases: A Yes/No field to determine whether or not Cases should be included in the list of purged records. Only Cases will be purged from the system – related entities such as Subjects and Tips will not be purged from the system and explicitly require that the operator to include Subjects and Tips as part of the purge batch in order to be purged from the system.

Purge Subjects: A Yes/No field to determine whether or not Subjects should be included in the list of purged records. Subjects which are not related to a Case or Tip will be included in the batch if set to “Yes”.

Purge Tips: A Yes/No field to determine whether or not Tips should be included in the list of purged records.

No Activity In: Returns matches based on the amount of time where no activity has occurred with Cases, Subjects, or Tips. This field contains a dropdown to specify periods of time, such as Days, Months, or Years.

Subject Type: Specifies the type of Subject to be included in the batch. This field is identical to the Subject Type field in the Subjects Module of Core Entities. This field is not required to Initialize a batch, but it is recommended that Subject Type be specified unless the user wishes to purge all eligible subjects, such as Persons and Businesses.

Tip Status: Determines the status of Tips to be included in the batch. This field is identical to the Tip Status filed in the Tips Module. This field is not required to Initialize a batch, but it is recommended that Tip Status be specified unless the user wishes to purge all eligible tips, regardless of their status.

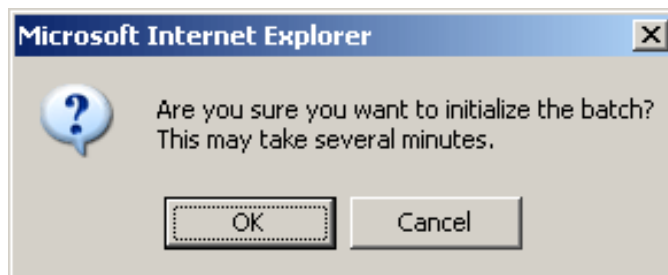
Reviewed Records Only: A Yes/No field limiting the records included in the purge batch to those which have been designated to be purged by an ACISS Web Operator. This option affects Cases and Tips as they are the entities which a System Administrator can specify Review Intervals for. When this option is set to “Yes”, the No Activity In criteria is essentially ignored and all records that have been user-designated to be purged will be included in the batch, regardless of date.

The screenshot shows a web-based interface for an 'Intelligence Purge' operation. The title bar reads '< Intelligence Purge >'. The form contains the following fields and values:

- Batch Status: Not Initialized
- Batch Date: 09/13/2005
- Purge Cases: Yes (dropdown menu)
- Purge Subjects: Yes (dropdown menu)
- Purge Tips: Yes (dropdown menu)
- No Activity In: 1 MONTHS (dropdown menu)
- Subject Type: PERSON (dropdown menu)
- Tip Status: OPEN (dropdown menu)
- Reviewed Records Only: No (dropdown menu)

Below the form, there is a section titled 'Intelligence Purge options' containing three buttons: '>> Initialize', '>> Delete Batch', and '>> Close'.

4. Clicking the Initialize button display the following prompt. This is to inform the operator that this process may take some time to complete. Initializing batches can very demanding on the system overall as it queries the entire database. Times and system resources used during initialization will vary depending on the batch criteria provided – a shorter No Activity In time will generally result in more records included in the batch. Initialization will begin after clicking OK.



5. A summary of the criteria and the resulting matches is displayed once the Initialization has completed:

| < Intelligence Purge > | |
|------------------------|-----------------------------------|
| Batch Status: | Pending |
| Batch Date: | 09/13/2005 |
| Purge Cases: | Yes |
| Purge Subjects: | Yes |
| Purge Tips: | Yes |
| No activity for: | 31 days (as of 09/13/2005) |
| Subject Type: | PERSON |
| Tip Status: | OPEN |
| <hr/> | |
| Excluded Cases: | 0 |
| Pending Cases: | 823 |
| Total Cases: | 823 |
| | |
| Excluded Subs: | 0 |
| Pending Subs: | 2774 |
| Total Subs: | 2774 |
| | |
| Excluded Tips: | 0 |
| Pending Tips: | 305 |
| Total Tips: | 305 |

Below the summary, the results are grouped according to type based on Case, Subject, or Tip and will have any pertinent information displayed for each match. In addition, an Inquiry link is available to allow the operator to view a record's details. This is useful in verifying the identity of a particular record and determining if it should be purged. Because of the potentially large number of records returned, each section displays results in pages, with 1,000 records per page visible on the screen.

Records are included or excluded from the batch using checkmarks. If a record is unchecked, it will not be included in the final purge. Each section header for Cases, Subjects, and Tips contains a checkbox that allows all records on the page for that particular section to be checked or unchecked. This is extremely useful in the event that only a few records need to be purged among a group of thousands.

The Intelligence Purge module is designed so that new records cannot be added to the list after the batch has been initialized. If records are removed accidentally, they will need to be initialized again in a new batch. No record will appear in two different batches – if a record is contained in one batch it will not be included in subsequent batches.

| | <input checked="" type="checkbox"/> | Case Number | Description | Status | |
|-----|-------------------------------------|-------------|------------------------------------------|--------|--|
| 1.) | <input checked="" type="checkbox"/> | 01-1 | MARIJUANA SMUGGLING | OPEN | |
| 2.) | <input checked="" type="checkbox"/> | 01-2 | Heroin Distribution | CLOSED | |
| 3.) | <input checked="" type="checkbox"/> | 01-6 | Stockton Homicide | OPEN | |
| 4.) | <input checked="" type="checkbox"/> | 01-3 | PROSTITUTION AT MASSAGE PARLOR | OPEN | |
| 5.) | <input checked="" type="checkbox"/> | 01-4 | DISTRIBUTION OF MARIJUANA | OPEN | |
| 6.) | <input checked="" type="checkbox"/> | 01-5 | Around The World Escort Service, Killeen | OPEN | |
| 7.) | <input checked="" type="checkbox"/> | 01-7 | 7/11 Robbery | OPEN | |
| 8.) | <input checked="" type="checkbox"/> | 01-8 | Terrorist Attack New York and Washington | OPEN | |

6. Below the lists of records, several options are available to help the user prepare the batch for a purge. Users can remove unchecked items from the batch, send Purge Review emails, purge all items in the batch, delete the batch entirely, or close the batch for the moment.

Remove Unchecked Items from Batch: Removes unchecked items from the batch. This function is performed on a page-by-page basis. If there are multiple pages of records for a section, each page will need to have items unchecked and removed from the list in order to exclude items from the batch.

Delete Batch: Completely deletes the batch. All records included in the batch are returned to their previous state and can be gathered in another batch where the purge criteria permit. The actual batch itself is also deleted from the system entirely. This is especially useful if a batch containing a very large number of records was created in error and needs to be redone.

Send Purge Review Emails for all Items in Batch: Sends ACISS Mail notifications to users associated with a record subject to purge. Each type of record follows certain conditions for a notification to be sent to a user.

Intelligence Purge options

Remove Unchecked Items from Batch

Purge Review Deadline:

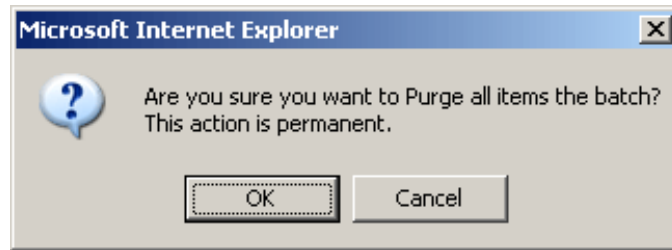
Send Purge Review Emails for all Items in Batch

Purge all Items in Batch

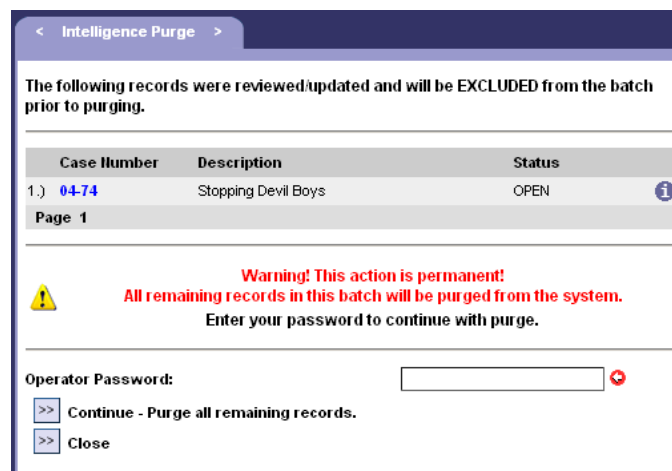
Delete Batch

Close

7. Once an operator is satisfied with the list of records to be purged, clicking the Purge button will display a message reminding the user that purging items from the batch is permanent.



8. After acknowledging the warning about the purge action being permanent, a verification screen will be presented to the administrator. The password of the user executing the batch will be needed to continue the purge process. The verification screen also displays a list of items that have been updated or reviewed the record owner for retention. If items that have been reviewed or updated were not removed from the batch by the administrator prior to purging, a notification will display informing the user that those items will be excluded from the batch.



9. After entering the password and clicking Continue, records will be purged from the system. The time needed to complete the purge will depend on the number of records being purged. **At this point the changes cannot be undone and are permanent.** The message "Purge Completed" will display along with the Done button. Clicking Done will return the operator back to the Intelligence Purge search screen.

Intelligence Purge Activity

The TypOfReport code table in System Administration contains a field in Detail Entry labeled Intelligence Purge Criteria. This is a user-defined setting which allows an agency configure the Intelligence Purge Process based on their guidelines. It has three options for each type of report: Exempt, Activity, and Not Activity.

Exempt: If a report with this setting is added to a case, the Case becomes permanently exempt from Intelligence Purge. This setting would typically be used for public record reports, such as Arrest, Incident, or Offense reports.

Activity: Types of reports with this setting, which are Approved, will be counted towards activity for the case. The Report Date will be used to determine if the case has had activity within the purge criteria guidelines.

Not Activity: Types of reports with this setting will be ignored during the Intelligence Purge activity calculation.

Intelligence Purge Requirements

Records must meet the following criteria to be added to a purge batch:

Cases

Operator must have access to the case.

- No qualifying (according to Intelligence Purge Activity) supplemental reports have been added to the case during the No Activity In period specified within the purge criteria.
- No Retain action has been performed on the case during the No Activity In period specified within the purge criteria.
- No Exempt reports are contained in the case.
- The Date Initiated is not within the No Activity In period specified within the purge criteria.
- Case has not been purged previously.
- Case is not included in another purge batch.

Subjects

- Subject has not been linked to a case, tip, or property report during the No Activity In period specified within the purge criteria.
- Subject is not an Agency or Law Enforcement Official subject type.
- The subject was not created within the No Activity In period specified within the purge criteria.
- Subject has not been purged previously.
- Subject is not included in another purge batch.

Tips

- Tip has never been linked to a case.

- No Retain action has been performed on the tip during the No Activity In period specified within the purge criteria.
- The tip entry date is not within the No Activity In period specified within the purge criteria.
- Tip has not been purged previously.
- Tip is not included in another purge batch.

Purge Notifications

Cases

1. Notifications pertaining to cases are sent in the following order:
2. Lead LEO
3. All operators who are marked as “Notify”
4. Last Update Operator if case is not assigned to an operator.

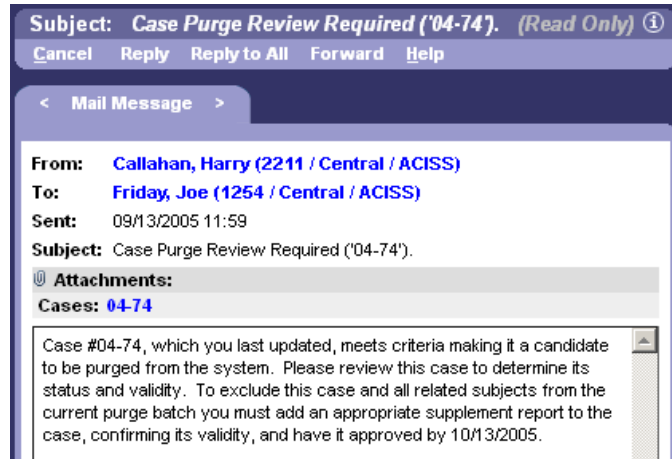
Subjects

1. Lead LEO of Case related to Subject
2. All operators who are marked as “Notify”
3. Last Update Operator if subject is not related to a Case

Tips

1. Operator assigned to Tip
2. All operators marked as “Notify”
3. Last Update Operator if tip is not assigned to an operator

The Purge Review Deadline is included in the message sent in the ACISS Mail notification. This is defaulted to one month from today’s date but can be changed by the operator to accommodate the agency’s requirements. Sending Purge Review Emails allows associated operators the opportunity to update a record with new information that would remove the record from the purge batch.



If a batch is initialized and records subject to purge are updated before the purge is processed, those records will display in the list as unchecked and have a yellow highlight to designate it as an updated record. Updated records will have their checkboxes disabled and they will automatically be excluded from the purge batch when it is executed.

| <input checked="" type="checkbox"/> | Case Number | Description | Status |
|-------------------------------------|-------------|---------------------|--------|
| 1.) <input type="checkbox"/> | 04-74 | Stopping Devil Boys | OPEN |

Page 1

Intelligence Purge options

- >> Remove Unchecked Items from Batch
- Purge Review Deadline: 10/13/2005
- >> Send Purge Review Emails for all Items in Batch
- >> Purge all Items in Batch
- >> Delete Batch
- >> Close

Case and Tip Review Process

Cases and Tips for an agency may be subject to periodic review so that old records with no activity can be removed from ACISS Web or retained if the information is still deemed pertinent.

The actual review process policy may vary between agencies and your System Administrator will configure the maximum number of days between Case or Tip reviews, referred to as the Review Interval. The Review Intervals for Cases and Tips are independent of each other and are configured in separate code tables. The Case Review Interval is configured in the Type of Case (TblCdsTypOfCase) code table; The Tip Review Interval is configured in the Tip Type (TblCdsTipTyp) code table.

Code Table: TblCdsTypOfCase

Save Cancel Save To File Load From File Help

Quick Entry Detail Entry

| Code | Description | Review Interval (Days) | Obsolete Flag |
|-------|---------------------|------------------------|---------------|
| ACC | ACCIDENT | | No X |
| AGGA | AGG ASSAULT | | No X |
| AGG | AGG BATTERY | | No X |
| AGGS | AGG STALKING | | No X |
| AOA | AOA | | No X |
| > ARR | ARREST | 0 | No X |
| ARWA | ARREST WARRANT | | No X |
| ASS | ASSAULT | | No X |
| ATM | ATTEMPT MURDER | | No X |
| BATO | BATTERY 65 OR OLDER | | No X |

Review Interval (Days) (Integer - 6 Characters)

When a Case or Tip exceeds the set review interval, it will be displayed on the appropriate Operator's ACISS Today screen in a specific section named "Cases Awaiting Review" or "Tips Awaiting Review".

Cases (15 items)

- **Cases Awaiting Review**
 1. 06-20 [i](#)
 2. 06-19 [i](#)
- **My Active Cases**
 1. 07-3 (Assigned 10/26/2006) [i](#)
 2. 06-19 (Assigned 10/18/2006) [i](#)
 3. 06-18 (Assigned 08/25/2006) [i](#)
 4. 06-17 (Assigned 08/25/2006) [i](#)
 5. 06-16 (Assigned 08/02/2006) [i](#)
 6. 06-14 (Assigned 07/24/2006) [i](#)

When opened in Entry/Update, the Review Process is the first screen displayed for the Operator.

Entry-Update Menu Case Number: 06-20

Save Cancel Manage WatchDogs Reassign Case Help

< Review Process >

Action: Retain [+](#)

Reason: Please retain this case.

The Review Process contains only two fields: Action and Reason. Both of these fields require input before the Case or Tip can be saved.

Action – determines what course of action will be taken for this record. The choices available are Retain or Purge.

Retain – the record is kept in ACISS Web and will appear on the Reporting LEO's ACISS Today screen in the appropriate section.

Purge – the record is designated to be purged by the System Administrator during an overall purge procedure. **Selecting Purge at this point DOES NOT remove the record**

from the system -- the Operator may reopen the Case or Tip and select Retain to remove it from the Purge queue. Records selected as Purge will be removed from the Reporting LEO's ACISS Today screen.

Reason – a free text area to include comments relevant to the action selected.

After a record has completed the Review Process, the activity is recorded like any other activity in the system and can be viewed in the Activity History screen. The record is then considered current (up to date) until the next Review Interval occurs.

Case Number: 06-20

| Primary Information | | | |
|-----------------------|------------|--|--|
| Date Initiated: | 08/29/2006 | | |
| Type Of Case: | ARREST | | |
| Total Expense Amount: | \$-50.00 | | |

| Case Status | | | |
|------------------------|---------------------|--|--|
| Case Status: | CLOSED | | |
| Case Status Date: | 10/18/2006 | | |
| Case Disposition Code: | ASSIST OTHER AGENCY | | |
| Case Disposition Date: | 10/18/2006 | | |

| Current Assignment | | | |
|--------------------|---------------------------------------------------------------------------------------|--|--|
| Lead LEO: | DEEKEN, ADALBERTO (aciss / Information Management / PINELLAS COUNTY SHERIFF'S OFFICE) | | |
| Agency: | ACISS SYSTEMS | | |
| Bureau: | Support Services | | |
| Division: | Information Management | | |

| Activity History | | | |
|---------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Date/Time | Action | Action Details | Comments |
| 2. 12/22/2006 9:33 | Retain | By: DEEKEN, ADALBERTO (aciss / Information Management / PINELLAS COUNTY SHERIFF'S OFFICE) | Please retain this case. |
| 1. 08/29/2006 16:57 | Assigned | By: DEEKEN, ADALBERTO (aciss / Information Management / PINELLAS COUNTY SHERIFF'S OFFICE) To: DEEKEN, ADALBERTO (Information Management / Support Services / ACISS SYSTEMS) | Initial Assignment |