Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

This document is intended to provide an overview of the privacy, civil rights, and civil liberties protections that serve as a foundational element of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) and are required in order to participate in the initiative. The successful fulfillment of this component is satisfied through the development, adoption and implementation of an appropriate privacy policy, adherence to the privacy due diligence elements of the NSI, and training of local, state, tribal, and federal partners.

The NSI is a partnership among local, state, tribal, and federal agencies that establishes a capacity for sharing terrorism-related SARs or Information Sharing Environment (ISE) SARs (ISE-SARs). The NSI provides law enforcement with another tool to "connect the dots" to combat crime and terrorism by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SARs—also referred to as the SAR process—in a manner that rigorously protects the privacy and civil liberties of Americans. *Suspicious activity* is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. "

The SAR process focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime. The NSI incorporates agencies' individual SAR processes into a nationwide capability and establishes a standardized approach to sharing and analyzing information, with the goals of detecting and preventing criminal activity, including information associated with domestic and international terrorism. The following briefly describes the key privacy components of the NSI effort.

Suspicious activity is defined in the *ISE-SAR Functional Standard (FS): Suspicious Activity Reporting*, Version 1.5, (ISE-SAR FS). The ISE-SAR FS builds upon, consolidates, and standardizes nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, and use of suspicious activity information. The ISE-SAR FS also identifies the types of behaviors that a trained analyst or investigator may deem reasonably indicative of criminal activity related to terrorism and the circumstances under which such information may be shared. These behaviors were identified by subject-matter experts; validated through implementation in the Los Angeles, California, Police Department and the application of ten years of State and Local Anti-Terrorism Training (SLATT®) Program experience; and then adjusted based on input by privacy advocacy representatives. At the completion of this process, in May 2009, the ISE-SAR FS was published, with the entire SAR process anchored on behaviors of suspicious activity, not ethnicity, race, or gender.

<u>NSI Privacy Protection Framework</u>—The NSI requires each site to consider privacy throughout the SAR process by fully adopting the following NSI Privacy Protection Framework prior to NSI participation:

- **Privacy policy:** The adoption and implementation of an approved privacy policy that contains ISE-SAR privacy protections that are in compliance with required provisions contained in the *ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy Template* or the *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*. It is important to note that an NSI program requirement exists that requires sites to have a policy developed and adopted prior to the interstate sharing of ISE-SARs.

- **ISE-SAR Functional Standard:** The application of the ISE-SAR FS, which reinforces constitutional standards, including the protection of rights guaranteed by the First Amendment and limitations on the use of certain factors—including race, ethnicity, national origin, or religious affiliation—in the gathering, collecting, storing, and sharing of information about individuals. The standard also includes reliability indicators, included as a result of input from privacy advocates. The functional standard, through the use of Information Exchange Package Documentation (IEPD), allows the originating agency to include or not include fields that contain personal information based upon the agency's rules and policies.

- **Privacy training:** The delivery of privacy training, through which the ISE-SAR FS is effectively communicated to personnel with responsibilities in the ISE-SAR arena, ensures the proper application of this standard. Furthermore, to expedite privacy policy development and implementation, it is strongly recommended that NSI sites have access to the services of a trained privacy officer who is available to provide ongoing advice and assistance regarding the protection of privacy, civil rights, and civil liberties. Three levels of training have been developed for the NSI, all of which include privacy materials. The NSI training levels are chief executive, analyst investigator, and line officer.

Community Outreach—Advocacy groups served an essential role in the shaping of the privacy protection framework and assisted in the development and review of NSI products. The success of the NSI largely depends on the ability to earn and maintain the public's trust. Consequently, NSI sites are encouraged to engage in outreach to members of the public, including privacy and civil liberties advocacy groups and private sector partners, in the course of privacy policy development and implementation. This outreach will help in addressing concerns of citizens and advocates by adopting and maintaining appropriate privacy and civil liberties safeguards. A transparent process and collaboration with advocacy groups will reinforce the ongoing commitment to earn and maintain the public trust.

The NSI has developed and participated in the Building Communities of Trust (BCOT) initiative. The role of BCOT is to support local law enforcement agencies and fusion centers as they interact with their various communities to explain the SAR process, the NSI, and the role of fusion centers. Additionally, agencies can use this opportunity to present the agency's privacy policy and outline the safeguards built into the information sharing system.

SAR Vetting Process—A key aspect of the NSI is the SAR vetting process. Before an agency can move SARs from the agency systems to the ISE, two forms of vetting must occur. Supervisors who initially receive a SAR from law enforcement officers, public safety agencies, private sector partners, or citizens must initially review the SAR to determine whether it has a nexus to terrorism and whether it includes the behaviors identified in the ISE-SAR FS. Trained analysts must then analyze the SAR against the behaviors identified in the ISE-SAR FS. Throughout the vetting process, privacy, civil rights, and civil liberties are vigilantly and actively protected through the training that analysts receive and through the system attributes that are a part of the NSI.

System Attributes—In addition to multiple levels of SAR review by trained personnel, there are system attributes that support privacy protections for the gathering, collection, storage, and sharing of SAR information, such as:

- Improved data standards for information sharing using the National Information Exchange Model (www.niem.gov).
- Leveraging existing secure systems, networks, and resources, such as the Regional Information Sharing Systems®, Law Enforcement Online, the Homeland Security Information Network, the National Criminal Intelligence Resource Center (www.ncirc.gov), and the Federal Bureau of Investigation's eGuardian system.
- Built-in design privacy protections, such as user authentication, "investigative purposes only" disclosures upon log-in, articulated investigative reason for accessing the system, clearly stated "for official law enforcement use only" warning before system access, and audit logs for capturing search transactions.
- Formatting in accordance with the ISE-SAR FS's IEPD format, which includes the application of privacy fields.

Compliance Verification—The U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative Criminal Intelligence Coordinating Council developed the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* (Compliance Verification document) for the purpose of assisting intelligence enterprises in complying with all applicable privacy, civil rights, and civil liberties protection laws, regulations, and policies while sharing appropriate intelligence and information needed to safeguard America. DOJ and the

U.S. Department of Homeland Security, through the Fusion Process Program, piloted this document to ensure that it contained all appropriate elements. A positive outcome of the pilots was the benefit of a peer-to-peer assessment. The document was well-received, with only minor modifications needed. The Compliance Verification document is anticipated to be released in March 2010. Once released, state and major urban area fusion centers are encouraged to partner with other centers to complete this critical privacy protections assessment.

Future Activity—The NSI is committed to creating a successful information sharing capability to allow local, state, and tribal law enforcement agencies and state and major urban area fusion centers to share SAR information. As sites join this initiative and the NSI grows, information and systems will be audited. The Compliance Verification document is one version of this audit capability for agencies to use internally. The NSI Program Management Office will also conduct periodic audits to ensure that privacy, civil rights, and civil liberties are being thoroughly protected.

Since the inception of the NSI, there has been a continued commitment to transparency. Local, state, and federal partners have met and received input from privacy advocates in the early development stages of the NSI. Law enforcement agencies and fusion centers, through the BCOT program, are meeting with community leaders to engage in dialogue about the NSI. Finally, as updates are made in the NSI and new documents are developed, privacy advocates will be engaged and requested to provide input into these documents.