PRIVACY POLICY

DELAWARE INFORMATION AND ANALYSIS CENTER

VERSION 1.0

FEBRUARY, 2011

DELAWARE INFORMATION AND ANALYSIS CENTER
PRIVACY POLICY

TABLE OF CONTENTS

Delaware Information and Analysis Center

Privacy Policy

1.0 Statement of Purpose

This privacy policy will allow the Delaware Information and Analysis Center (DIAC) to establish how protected information is collected, used, and secured in order to apply this policy to daily operations. As a result, the privacy policy will clearly define the law, policy, and procedure that the DIAC, participating agencies, and authorized users need to comply with in order to appropriately protect privacy, civil rights, and civil liberties.

The goal of establishing and maintaining the DIAC is to further the following purposes:

(a) Increase public safety and improve national security;
(b) Minimize the threat and risk of injury to specific individuals;
(c) Minimize the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health;
(d) Minimize the threat and risk of damage to real or personal property;
(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;
(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;
(h) Support the role of the justice system in society;
(i) Promote governmental legitimacy and accountability;
(j) Not unduly burden the ongoing business of the justice system; and
(k) Make the most effective use of public resources allocated to public safety agencies.

The DIAC is a participant in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The shared space is a networked data and information repository which is under the control of the submitting agencies and provides for the sharing of terrorism-related SAR information to participants in the NSI.

2.0 Compliance with Law Regarding Privacy, Civil Rights, and Civil Liberties

All DIAC personnel, participating agency personnel, personnel providing information technology services to the DIAC, private contractors, and users will comply with this privacy policy and all applicable law protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information to DIAC personnel, governmental agencies (including ISE participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

External agencies that access the DIAC's information or share information with the center are governed by the law governing those individual agencies, including applicable federal and state law.

The DIAC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating agencies and individual users. Written acknowledgement will be obtained to verify that the personnel and participating users received the policy and agree to be in compliance with the policy. This includes SAR information that source agencies collect and the DIAC receives as well as ISE-SAR information identified, submitted to the shared space, and accessed by or disclosed to DIAC personnel, participating agencies, and individual users. All DIAC members are operating under a Memorandum of Understanding and each is required to sign a non-disclosure agreement to participate. The documents, including participating agencies User Agreements and Individual User Agreements, are reviewed by the DIAC privacy officer and are physically maintained in the DIAC.

Applicable law includes Delaware state statutes and regulations, but not to be exclusive of Delaware title 11, chapters 85, 86, and sections 935 and 9403. In addition, the DIAC is in compliance with the following federal law: 28 Code of Federal Regulations Parts 20, 22, and 23; 5 U.S.C. § 552a and 5 U.S.C. § 552a (b); Executive Order 12333; Public Law 107-56 (USA Patriot Act); and Public Law 82-352 (78 Stat. 241) (Civil Rights Act of 1964). The DIAC is in compliance with the U.S. and Delaware constitutions and the law cited above.

The DIAC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the law cited above.

3.0 Definitions

3.10 **AGENCY/CENTER**
Agency or Center refers to the DIAC and all participating state agencies of the DIAC.

3.20 **INFORMATION**
Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

3.30 **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.

3.40 **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.

3.50 **PUBLIC**
Public includes:

(a) Any person and any for-profit or nonprofit entity, organization, or association;
(b) Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
(c) Media organizations; and
(d) 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:

(a) Employees of the agency;
(b) 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
(c) Public agencies whose authority to access information gathered and retained by the agency is specified in law.

3.60 **QUALIFIED INDIVIDUAL**

Qualified Individual refers to DIAC staff including Critical Infrastructure Specialists, Analysts, Investigators, and Administrators. They are granted direct access to DIAC information. Qualified individuals have obtained the proper background and security clearances necessary to gain access to the requested information.

3.70 **AUTHORIZED USER**

An Authorized User is an individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

3.80 **PERSONAL INFORMATION**

Personal Information refers to any information that relates to in identifiable individual (or data subject).

3.90 **PROTECTED INFORMATION**

Protected Information includes personal information about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Delaware Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal law.

3.91 **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.

3.92 **SUSPICIOUS ACTIVITY**

As defined in the ISE-SAR Functional Standard (Version 1.5), Suspicious Activity is "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

3.93 **SUSPICIOUS ACTIVITY REPORT (SAR)**

Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious Activity Report information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with

the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

3.94 **TERRORISM INFORMATION**

Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Terrorism Information is all information relating to: (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials 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; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

3.95 **TERRORISM-RELATED INFORMATION**

In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (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 may include intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

3.96 **TIPS AND LEADS INFORMATION or DATA**

Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

4.0 Seeking and Retaining Information

4.10 The DIAC was created in response to the 9/11 Commission's recommendations for enhanced information sharing. By gathering criminal information related to domestic and international terrorist threats, criminal activity and criminal enterprises, natural disasters as well as other emergencies, this fusion center analyzes and then disseminates the information to the appropriate entities.

4.20 What Information May Be Sought or Retained

(a) The DIAC will seek or retain only information relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences, the prevention of crime, or that is useful in a crime analysis or in the administration of criminal justice and public safety.

(b) The DIAC will seek or retain criminal intelligence information where there is reasonable suspicion that a specific individual or organization has committed a criminal offense, is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity.

(c) The DIAC will not seek or retain and information-originating agencies will agree not to submit information about an individual or organization solely on the basis of their religious, political, or social views or activities, their participation in a particular organization or event, or solely because of their race, ethnicity, citizenship, and place of origin, age, disability, sex, or sexual orientation.

(d) This DIAC will not seek or retain information about the political, religious or social views, participation in a particular organization or event, or activities of any individual or their race, ethnicity, citizenship, place of origin, age, disability, sex, or sexual orientation unless such information is:

(1) Relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal (including terrorist) activity; or

(2) Needed by the DIAC:

(a) To identify an individual;

(b) In order for the center to operate effectively; or

(c) To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

(e) The DIAC shall keep a record of the source of all information retained by the center.

(f) The DIAC shall categorize and label all information.

4.30 Methods of Seeking or Receiving Information

(a) Information gathering and investigative techniques used by the DIAC and affiliated agencies, such as the Delaware State Police will comply with all state and federal law as referenced in section 2.0.

(b) The DIAC 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:

(1) The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to personnel within the center, except if the individual did not act as an agent of or the direction of any bona fide law enforcement officer participating with the center;

(2) The individual or information provider used methods for collecting the information that center personnel could not legally use, unless the individual did not act as an agent of, or at the direction of, any bona fide law enforcement officer participating in the center;
(3) The specific information sought from the individual or information provider could not legally be collected by any participating agency or the center; or
(4) The center or any of its participating agencies have not taken the steps necessary to be authorized to collect the information.

(c) Information gathering and investigative techniques used by the DIAC will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain pursuant to Section 4.10.

(d) The DIAC will retain information long enough to evaluate a tip or lead or SAR information in order to determine its value and credibility. As a general rule, SAR information should be reviewed and evaluated within 90 days and purged within a five year period of inactive status.

4.40 The DIAC will only contract with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable state, local, and federal laws, statutes, and regulations.

5.0 Information Quality

(a) The DIAC will make every reasonable effort to ensure that information sought or retained is:
(1) Derived from dependable and trustworthy sources of information;
(2) Accurate;
(3) Current;
(4) Complete, including the relevant context in which it was sought or received and other related information;
(5) Merged with other information about the same individual or organization only when the applicable standard (see Section 6.20) has been met; and
(6) Updated or corrected as necessary when new information becomes available.

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

(c) The DIAC will make every reasonable effort to ensure that only qualified individuals are allowed to add, change, or delete information in their systems.

(1) The labeling of retained information will be reevaluated and relevant information may be added, changed, or deleted when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

(d) The DIAC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

(e) The DIAC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is:

(1) erroneous, misleading, obsolete, or otherwise unreliable;

(2) The center did not have the authority to gather the information or to provide the information to another agency; or

(3) The center used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

(f) Originating agencies external to the DIAC are responsible for reviewing the quality and accuracy of the data provided to the center. The DIAC will review the quality of information it has received from an originating agency and will advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable pursuant to Subsection (d).

(g) The DIAC will advise recipient agencies, in writing or electronically, when information previously provided to them is deleted or changed pursuant to Subsection 5.0 (c) when the requesting agency has specifically requested to be notified.

6.0 Collation and Analysis of Information

6.10 Collation and Analysis

(a) Information subject to collation and analysis is information as defined and identified in Section 4.20 and 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; ESAR and/or ISE-SAR information posted by the DIAC to the shared space or accessed from the shared spaces under the NSI will be analyzed for intelligence purposes only by qualified DIAC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly, including training on the implementation of this policy. These personnel shall share ESAR and/or ISE-SAR information only through authorized analytical products designed:

(1) To 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, including terrorist, activities generally; or

(2) To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the DIAC.

(b) Information sought or received by the DIAC or other sources will not be analyzed or combined in a manner or for a purpose that violates Subsection 4.10 (b).

(c) The DIAC requires that all analytical products be reviewed by the Privacy Officer (or in the Privacy Officer's absence, his designee) to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

6.20 Merging of Information from Different Sources

(a) Information 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.

(b) The set of identifying information sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match.

(c) If the matching requirements are not fully met but there is a strong 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.

6.30 Suspicious Activity Report (SAR) information

(a) The DIAC receives and collects tips and leads related to terrorism in adherence to this policy as well as the SAR policy established in the ISE-SAR Functional Standard, Version 1.5.

(b) The SAR information is collected and assessed for credibility and value.

(c) The information is classified, labeled, and stored according to Sections 7.0 and 8.0 of this policy and the information is only accessible and disseminated by qualified individuals to the appropriate agencies.

(d) Refer to Appendix 1, DIAC Privacy Policy Appendix for Nationwide Suspicious Activity Report (SAR) Initiative (NSI) and Automated Reporting Information Exchange System Electronic Suspicious Activity Report (ESAR) for specific privacy restrictions on SAR information.

7.0 Classification

7.10 Prior to entering information into any DIAC information/intelligence system, intelligence personnel shall classify the data in order to protect sources, investigations, and the data subject's right to privacy. Intelligence personnel will treat information pertaining to any individual (regardless of citizenship or U.S. residency status) with the same level of privacy protection. Classification also indicates whether internal approval must be completed prior to the release of the information to persons outside DIAC.

7.20 DIAC classifies data into the following categories:

(a) Confidential

(1) Confidential information is the highest level of unclassified but sensitive information. Access to information defined as "confidential" is limited, even among law enforcement officers.

(b) Law Enforcement Sensitive (LES)

(1) LES information is middle level unclassified but sensitive information. LES may be disseminated to law enforcement personnel only.

(c) For Official Use Only (FOUO)

(1) FOUO is unclassified information of a sensitive nature which can be disseminated outside the scope of law enforcement personnel (i.e., participating agency personnel, private contractors, and other authorized individuals).

(2) FOUO may not be released to the general public.

(d) Protected Critical Infrastructure Information (PCII)
    (1) Protected Critical Infrastructure Information (PCII) is a subset of Critical Infrastructure Information for which protection is requested under the PCII Program by the requestor.
    (2) Critical Infrastructure Information is information related to the security of critical infrastructure or protected systems that are not customarily in the public domain.
(e) Open Source (OS)
    (1) Open source information is any information that is publicly available.

Classification --All information/intelligence information has its security classification marked directly on the information file.

Re-evaluation of Classification --Re-evaluations can be based upon time (i.e., tied to the five-year retention/renewal); the addition of new information affecting access or disclosure limitations; or at the time of a request for the information.

8.0 Labeling

8.10 DIAC 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.

8.20 Intelligence Information
(a) All criminal intelligence information disseminated will be labeled (by record, data set, or system of records) and classified under the following categories: Confidential, Law Enforcement Sensitive, For Official use only, Protected Critical Infrastructure Information. As such so that the recipient can handle the information in accordance with applicable legal requirements.

8.30 Non-Intelligence Information
(a) Information labeled as non-intelligence information will be maintained and disseminated as labeled (by record, data set, or system of records) on the document." non-Intelligence Information pertains to information other than criminal intelligence information.

8.40 Identification of Information

(a) The data contained within DIAC criminal intelligence systems will be identified as intelligence or non-intelligence information and any applicable legal requirements for handling such data indicated is provided in Section 7.0 of this policy.

9.0 Sharing and Disclosure of Information

9.10 Sharing Information within the DIAC and with Other Justice System Partners.

(a) Access to protected information retained by the DIAC will only be provided to persons within the DIAC or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for whom the person is working. However these agencies cannot receive personally identifiable information regarding criminal subjects from the DIAC criminal intelligence information center without a need and a right to know the information in the performance of a law enforcement activity.

(b) The Director of the DIAC, and/or administrator(s) designated by the Director, shall establish requirements and record all personnel as to their access authority and permission to access DIAC information.

(c) Permissions regarding viewing, adding, editing and printing of DIAC information are controlled by DIAC's administrator(s) on all DIAC information.

(d) All DIAC personnel, with approval from the Director, or his designee, may disclose DIAC information pursuant to applicable policy.

(e) An audit trail will be kept of access by or dissemination of information to such persons.

(f) Agencies external to the DIAC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

9.20 Sharing Information with Those Responsible for Public Protection, Safety, or Public Health

(a) Information retained by the DIAC may be accessed by or disseminated to those responsible for public protection, public safety or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures in Section 2.0.

(b) The DIAC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

(c) An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

(d) Agencies external to the DIAC may not disseminate information received from the DIAC without approval from the originator of the information

9.30 Sharing Information for Specific Purposes

(a) Information gathered and retained by the DIAC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law.

(b) The DIAC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

(c) An audit trail sufficient to allow the identification of each individual who requested, accessed or received information retained by the center; the nature of the information requested, accessed or received; and the specific purpose will be kept by the center will be kept for a minimum of 18 months by the center.

(d) Agencies external to the DIAC may not disseminate information received from the DIAC without approval from the originator of the information

9.40 Sharing information through the Information Sharing Environment (ISE)

(a) Individual users and user agencies will adhere to DIAC's ISE information sharing policy and procedure.

(b) This center coordinates and assists other agencies in investigating and correcting identified information deficiencies in information shared through the ISE.

(c) The center has put in place notice mechanisms, such as metadata or data field labels, for enabling ISE-authorized users to determine the nature of the protected information that the center is making available through the ISE and complies with the federal guidelines, 28 Code of Federal Regulations Parts 20, 22, and 23 (listed in Section 2.0), such

that participants can handle the information in accordance with applicable legal requirements.

(d) DIAC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with each record, data set, or system of records containing personally identifiable information, including terrorism-related information shared through the ISE, which will be assessed, used, and disclosed in compliance with the DIAC's ISE information sharing policy. The types of information include:

- The name of the originating center, department or agency, component, and subcomponent.
- The name of the center's justice information system from which the information is disseminated.
- The date the information was collected and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

(e) The Privacy Officer shall be appointed by the center Director (or his designee) and is assigned as the ISE privacy official.

(f) Complaints that are suspected to be or are specifically ISE information will be dealt with in accordance to the DIAC's ISE information sharing policy.

9.50 Disclosing Information to the Public

(a) Information gathered or collected and records retained by the DIAC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record under 29 Del. Code §10002(g) (or otherwise appropriate for release to further the center's mission) and is not exempt from disclosure by statute or common law under 29 Del. Code §10002(g) (6). Such information may only be disclosed in accordance with the law and procedures applicable to the DIAC for this type of information.

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

(c) An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

(d) Agencies external to the DIAC may not disseminate without approval from the originator of the information.

9.60 Disclosing Information to the Individual about Whom Information Has Been Gathered/Exemptions from Disclosure

(a) Upon satisfactory verification (fingerprints) of his or her identity and subject to the conditions specified in (9.60 b), an individual is entitled to know the existence of and to review public record information, including the individual's personal criminal record under 29 Del. Code §10002(g) (4) that has been gathered and retained by the DIAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The DIAC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.

(b) There are several categories of records that will ordinarily ***not be provided*** to the public:

- Records required to be kept confidential by law are exempted from disclosure requirements under 29 Del. Code §10002(g) (6).

- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, E.O. Classified National Security Information Program or State, Local, Tribal, and Private Sector Entities, August 18, 2010.

- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under 29 Del. Code §10002(g) (3). However, certain law enforcement records must be made available for inspection and copying under 29 Del. Code §10002(g) (4).

- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under 29 Del. Code §10002(g) (16). This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under 29 Del. Code §10002(g)(16) (5)**,** including an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

- A violation of an authorized nondisclosure agreement under 29 Del. Code § 10002(g) (2).

(c) The existence, content, and source of the information will not be made available to an individual when:

(1) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution; Del. Code §10002(g)(3)

(2) Disclosure would endanger the health or safety of an individual, organization, or community; Del. Code §10002 (g)(4)
(3) The information is in a criminal intelligence system subject to 28 CFR Part 23.20(e);
(4) The information relates to Title 11, Chapters, 85, and 86; or
(5) The information is in intelligence files compiled for law enforcement purposes, the disclosure of which would constitute an endangerment to the local, state, or national welfare and security. Del. Code §10002 (g)(5)

The center will notify the source agency of the request and its determination that disclosure by the center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

(d) If an individual has objections to the accuracy of completeness of the information retained about him or her, the DIAC will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if requests for correction are denied. The individual will also be informed of the procedure for appeal when the center has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

(e) A record will be kept of all requests and of what information is disclosed to an individual.

9.70 Conditions under which center will not disclose information

(a) Information will not be sold, published, exchanged, or disclosed for commercial purposes; will not be disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or disclosed to unauthorized persons.

10.0 Information Retention and Destruction

10.10 Review of Information Regarding Retention

(a) All criminal intelligence information will be reviewed for record retention (validation or purging) at least every five (5) years, consistent with 28 CFR Part 23.
(b) Other information retained by the DIAC, but not subject to 28 CFR Part 23, will also be reviewed for record retention (validation or purging) at least every five (5) years.

10.20 Destruction of Information

(a) The DIAC will delete information or return it to the source, unless it is updated, every five (5) years, and be compliant with 28 CFR Part 23.

(b) Permission to destroy or return information or records will be presumed if the applicable information is not updated within the specified time period (See Section 10.20 (a)).

(c) Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and according to the Freedom of Information Act exemption (b) (2).

(d) A record of information to be purged will be maintained by the DIAC, for appropriate system(s), 30 days prior to the required purge date.

(e) No record of the purged information will be maintained by the DIAC, to satisfy the integrity and completeness of the purged information from appropriate system(s).

11.0 Complaints and Corrections

11.10 Individual Complaints Originating from DIAC Information

(a) If an individual has complaints or objections to the accuracy or completeness of information about him or her originating from DIAC information, the DIAC's Privacy Officer will inform the individual of the procedure for submitting complaints or objections (if not properly communicated) or requesting corrections, including appeal rights if requests are denied in whole or in part.

(b) If an individual's complaint or objection cannot be resolved after review at the DIAC, the individual may request a review of that decision, by the Secretary of the Delaware Department of Safety and Homeland Security. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

11.20 Individual Complaint Originating from Another Agency

(a) If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, the DIAC will notify the source agency of the complaint or request for correction, and coordinate with the source agency to ensure that the individual is provided with applicable complaint submission or corrections procedures.

(b) A record will be kept of all such complaints and request for corrections, and the resulting action taken, if any.

(c) The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the DIAC, or the originating agency.

11.30 Complaints to Accuracy or Completeness of terrorism-related information that allegedly Results in Harm to an Individual

(a) If an individual has complaints or objections to the accuracy or completeness of DIAC terrorism-related protected information allegedly held by the DIAC that is exempt from disclosure, has been or may be shared through the ISE, and has resulted in specific, demonstrable harm to such individual, the DIAC will inform the individual of the procedure for submitting complaints or requesting corrections (if not properly communicated). Complaints will be received by the center's Director at the Delaware State Police Headquarters, 1441 North DuPont Hwy., Dover DE 19903.

(b) The Director will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence or nonexistence of any DIAC terrorism-related information in privacy fields that identifies the individual unless otherwise required by law. However, any personal information will be reviewed and corrected in, or deleted from, DIAC terrorism-related information, including ISE-SAR information in the DIAC's shared space if the information is determined to be erroneous, included incorrectly merged information, or is out of date.

(c) If the information did not originate with the center, the Director will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved.

(d) A record will be kept of all complaints and requests for corrections, and the resulting actions, if any.

(e) To delineate protected information shared through the ISE from other data, DIAC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

12.0 Accountability and Enforcement

12.10 Information System Transparency

(a) This policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and posted online at **www.dsp.delaware.gov/.**

(b) The Director of the DIAC will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or

accessed by the center. The Director can be contacted at Delaware State Police Headquarters, 1441 North DuPont Hwy., Dover DE 19903.

(c) The center Director will oversee the responsibility of developing and enhancing the privacy policy and assign the Privacy Officer to recommend annual updates and enhancements to the policy.

12.20 Accountability for Activities

(a) Primary responsibility for the operation of the DIAC, its justice information systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, and dissemination of information; and the enforcement of this policy is assigned to the Director of the center.

(b) The DIAC has established procedures, practices, system protocols, and use of software, information technology tools, and physical security measures that protect the information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The electronic methods and techniques used shall be consistent with that of Delaware State Police, Information Support Section and or the State of Delaware, Department of Technology and Information.

(c) The DIAC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as designated by the Director of the center.

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

(e) The DIAC 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, including but not limited to those outlined in Section 2.0. This will include watch logs to maintain audit trails of requested and disseminated information. DIAC will conduct periodic auditing of these systems, so as to not establish a pattern of the audits. Information regarding the logging access of these systems will be disseminated as needed. Electronic access to the center's data identifies the user. These audits will be mandated at least quarterly and a record of the audit will be maintained by the Director (or his designee) of the center.

(f) The DIAC will require any individuals authorized to use these systems to agree in writing to acknowledge receipt of the policy and to comply with the provisions of this policy.

(g) The DIAC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s).

The audit will be conducted by a designated, independent panel of trusted personnel from the Delaware Homeland Security Advisory Council comprised of the following members;

1. The Secretary of the Department of Safety and Homeland Security
2. The Homeland Security Advisor
3. The Adjutant General of the Delaware National Guard, or a designee
4. The Chief Information Officer of the State of Delaware, or a designee
5. The Secretary of the Department of Natural Resources and Environmental Control, or a designee
6. The Secretary of the Delaware Department of Transportation or a designee
7. The Secretary of the Delaware Department of Education, or a designee
8. The Secretary of the Delaware Department of Agriculture, or a designee
9. The Commissioner of the Delaware Department of Correction or a designee
10. The Superintendent of the Delaware State Police, or a designee
11. The Director of the Delaware Division of Public Health, or a designee
12. The Director of the Delaware Emergency Management Agency or a designee
13. The Director of the Division of Motor Vehicles, or a Designee
14. The Executive Secretary of the Delaware Volunteer Firefighters' Association or a designee
15. The Chair of the Delaware Police Chiefs' Council, or a Designee
16. The President of the League of Local Governments, or a Designee
17. Other representatives from federal, state, and local governments, private sector partners, academia, and emergency service organizations, as recommended by the Secretary of Safety and Homeland Security and appointed by the Governor.

This independent panel has the option of conducting a random audit, without announcement, at any time, and without prior notice to the DIAC. This audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system.

(h) The DIAC Director will annually update this policy in response to recommendations made by the Privacy Officer in response to changes

in applicable law, technology, the purpose and use of the information systems and public expectations. Revision dates will be included in the updated policy to ensure the most recent policy is referred to by all personnel.

(i) The Director will notify an individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person. The 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 release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release. Notice need not be given if doing so meets the criteria specified in Subsection 9.50 (b). In adherence to Delaware title 11, chapters 85, 86, and regulations in Section 2.0.

(j) Any reported errors or confirmed or suspected violations of agency policies shall be reported to the Director (or his designee) who will take appropriate action following this policy and will also ensure that the center adheres to the ISE Privacy Guidelines and other requirements for participation in the ISE.

12.30 Enforcement

(a) The DIAC Director ensures that the policy enforcement procedures and sanctions outlined below are adequate and enforced. If an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the DIAC will:

1) Suspend or discontinue access to information by the user;
2) Apply administrative actions or sanctions as provided by Delaware State Police rules and regulations;
3) If user is from an agency outside of the Delaware State Police, request the relevant agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or
4) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy as stated in Section 1.00.

(b) DIAC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or

participating agency personnel violating the center's privacy policy.

13.0 Security Safeguards

(a) The DIAC has established procedures, practices, system protocols, and use of software, information technology tools, and physical security measures that protect the information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The electronic methods and techniques used shall be consistent with that of Delaware State Police, Information Support Section and or the State of Delaware, Department of Technology and Information.

(b) The DIAC is committed to protecting privacy and maintaining the integrity and security of personal information. DIAC shall be responsible for implementing the security requirements in Subsections (d) – (j), below, for its information and intelligence systems.

(c) The DIAC has formally adopted the Criminal Justice Information Systems (CJIS) Security Policy of the U.S. Department of Justice, Federal Bureau of Investigation, and Criminal Justice Information Services Division and applies these provisions to DIAC operations. DIAC will develop a separate security policy.

(d) Firewalls are in place to prevent unauthorized agencies or entities from accessing DIAC resources.

(e) Role-based user access – The intelligence systems that intelligence personnel access utilize various levels of role-based user access.
    (1) Each user's role shall determine the types of information accessible to the user.
    (2) Each user's role contains certain permissions to add, modify, delete or print records.
    (3) Each user's role shall determine to whom, individually, the information can be disclosed and under what circumstances.

(f) Security breaches and security breach notification –Delaware State Police will monitor and respond to security breaches or breach attempts.
    (1) In the event that intelligence personnel become aware of a breach of the security of unencrypted personal information, Delaware State Police will notify an individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical, reputational or financial harm to the person.

(2) Any necessary 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 release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release.

(g) Physical Safeguards – DIAC systems shall be located in a physically secured area that is restricted to designated authorized personnel.
   (1) Only designated authorized personnel will have access to information stored in the DIAC data systems.
   (2) All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility.
   (3) All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.

(h) Disaster Recovery – Delaware State Police has appropriate disaster recovery procedures for DIAC data outlined in the Delaware State Police's Disaster Recovery Plan.

(i) Information Security Officers - Federal agencies housed at DIAC each have a dedicated information security officer. DIAC has an Information Security Officer who is trained and handles network access/security.

(j) Assessment Storage - Risk and vulnerability assessments are stored separately from law enforcement and intelligence data. Risk and vulnerability assessments are not available to the public.

14.0 Training

(a) The DIAC will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:
   (1) All assigned personnel of the center;
   (2) Personnel providing information technology services to the DIAC;
   (3) Staff in other public agencies or private contractors providing services to the center; and
   (4) Users who are not employed by the agency or a contractor.

(b) The DIAC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

(c) The training program will cover:
    (1) Purposes of the privacy, civil rights, and civil liberties protection policy;
    (2) Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the DIAC;
    (3) Originating and participating agency responsibilities and obligations under applicable law and policy;
    (4) How to implement the policy in the day-to-day work of the user;
    (5) The impact of improper activities associated with infractions within or through the agency;
    (6) Mechanisms for reporting violations of center privacy protection policies and procedures; and,
    (7) The nature and possible penalties for policy violations, including possible administrative, civil and criminal liability, to include Delaware Title 11, Chapters 85, 86, and sections 935, 9403, and 28 CFR Part 23.

(d) Qualified Individuals will learn how to share protected information with the agencies through the ISE

15.0 Governance and Oversight

(a) The DIAC Director shall have primary responsibility for the operation of the DIAC, and the coordination of personnel; the receiving, retention, evaluation, information quality, analysis, sharing, disclosure, and destruction of information.

(b) The DIAC's privacy compliance is guided by a trained Privacy Officer who is appointed by the DIAC Director and who receives reports of regarding alleged errors and violations of the provisions of this policy and who is the liaison for the ISE. The Privacy Officer can be contacted at Delaware State Police Headquarters, 1441 North DuPont Hwy., Dover DE 19903.
The Privacy Officer shall provide oversight to the policy, and will periodically review and recommend updates to the policy pursuant to Section 4.30 (d) and Appendix 1 Section C (2).

(c) The Privacy Officer shall annually conduct an audit and inspection of the information contained in the criminal intelligence system. A designated panel of trusted personnel from the Delaware Homeland Security Advisory Council will also conduct an annual audit of the Criminal Intelligence System.

Appendix 1

Delaware Information and Analysis Center (DIAC) Privacy Policy Appendix for Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) and Automated Reporting Information Exchange System Electronic Suspicious Activity Report (ESAR)

A. Purpose Statement

1. The purpose of this appendix to the DIAC Privacy Policy is to provide detailed privacy, civil rights and civil liberties guidance to DIAC personnel concerning the Nationwide SAR Initiative (NSI) and the DIAC Automated Reporting Information Exchange System Electronic Suspicious Activity Report system (ESAR). NSI is a US DHS, DOJ, and ODNI initiative. It involves a suspicious activity report (SAR) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. U.S. Departments of Justice and Homeland Security will provide guidance to all Fusion Centers to create a uniform national process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the Information Sharing Environment (ISE). ESAR is a legacy DIAC initiative under which an ESAR Report is electronically submitted to DIAC.

2. To ensure that DIAC all personnel and participating user agencies comply with applicable federal, state, local, and tribal laws, regulations, and policies and assists participants in:
    - Safeguarding of individual privacy, civil rights, civil liberties.
    - Increasing public safety and improving national security.
    - 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.

B. Policy Enforcement and Legal Compliance

1. All participating DIAC personnel, including personnel providing information technology services to the DIAC, and other authorized participants will comply with applicable provisions of the DIAC Privacy Policy concerning personal information, including:
    - SAR information the source agency collects and the DIAC receives.
    - The ISE-SAR information identified, submitted to a shared space, and accessed by or disclosed to DIAC personnel.

- ESAR information the source agency collects and the DIAC receives.

2. The DIAC will provide a printed copy of its Privacy Policy including this appendix to all DIAC personnel, non-agency personnel assigned to the DIAC, and to each source agency and DIAC authorized user and will require both a written or electronic acknowledgement of receipt of this policy and a written or electronic agreement to comply with applicable provisions of this policy.

3. All DIAC personnel, participating agency personnel, personnel providing information technology services, and other authorized users shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution and state, local, and federal privacy, civil rights, civil liberties legal requirements applicable to the DIAC and/or other participating agencies.

C. Governance and Oversight

1. The Fusion Center Director will have primary responsibility for operating the DIAC, ESAR, ISE-SAR information system operations, and coordinating personnel involved in the NSI; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR, ESAR and ISE-SAR information; and enforcing the provisions of this policy.

2. The DIAC's participation in the NSI will be guided by a trained Privacy Officer who is appointed by the Fusion Center Director to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will review a monthly comprehensive report of SAR information pursuant to Section 4.30. The privacy officer shall receive and review reports regarding alleged errors and violations of the provisions of this policy. The Privacy Officer can be contacted at Delaware State Police Headquarters, 1441 North DuPont Hwy., Dover DE 19903.

D. Information

1. The DIAC will seek, retain, and/or share through the ISE only that information which a source agency (the DIAC or other agency) have determined constitutes "suspicious activity" and which:
    - Is based, on (a) a criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct.
    - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime.
    - The source agency assures was acquired in accordance with agency policy and in a lawful manner.

2. Source agencies will agree not to collect and submit SAR information and the DIAC will not retain SAR, ESAR or ISE-SAR information about any individual that was gathered solely on the basis of that individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or gathered on the basis of race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. Upon receipt of SAR information from a source agency that has processed the information in accordance with this policy, designated DIAC personnel will:
   - Personally review and vet the SAR information and provide the two-step assessment set forth in the US DHS Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) (SAR Functional Standard) to determine whether the information qualifies as ESAR and/or an ISE-SAR, DIAC personnel will confirm that such an assessment has been conducted by an authorized source agency.
   - Enter the information following Information Exchange Package Documentation (IEPD) standards and code conventions to the extent feasible.
   - Provide appropriate labels as required.
   - Submit the ESAR and/or ISE-SAR to the DIAC shared spaces.
   - Notify the source agency that the SAR has been identified as ESAR and/or ISE-SAR and submitted to the shared spaces.

4. The DIAC will ensure that certain basic and special descriptive information is entered and electronically associated with ESAR and/or ISE-SAR information, including:
   - The name of the source agency.
   - The date the information was submitted.
   - The point of contact information for the SAR-related data.
   - Information reflects applicable laws, rules or policies regarding access, use, and disclosure.

5. Information provided in the ESAR and/or ISE-SAR shall indicate, to the maximum extent feasible and consistent with the current version of the SAR Functional Standard:
   - The nature of the source: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source.
   - Confidence levels, including:
   - The reliability of the source

   If the reliability of the source is doubtful or has been determined to be unreliable, the DIAC will not retain information within a DIAC record system. Due diligence will be exercised in determining source reliability and content validity.

Information determined to be unfounded will be purged from the shared space. 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 validate it through their own investigation.

6. At the time a decision is made to submit ESAR and/or ISE-SAR information to the shared spaces, DIAC personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the SAR Functional Standard, to reflect any limitations on disclosure based on sensitivity of disclosure in order to:
   - Protect an individual's right of privacy, civil rights, and civil liberties.
   - Protect confidential sources and police undercover techniques and methods.
   - Prevent interference or compromise of pending criminal investigations
   - Provide any legally required protection based on an 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.

7. The DIAC will share ESAR and/or ISE-SAR information with authorized non-fusion center agencies and individuals only in accordance with established Fusion Center policy and procedure.

8. The DIAC will ensure that ESAR and/or ISE-SAR information in the shared spaces that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will be updated to so indicate. Information determined to be unfounded will be purged from the shared space.

9. The DIAC incorporates the gathering, processing, reporting, analyzing, and sharing of SAR, ESAR and/or ISE-SAR information (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as the privacy, civil rights, and civil liberties of individuals.

10. Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

E. Acquiring and Receiving Information

1. Information acquisition and investigative techniques used by source agencies must comply with and adhere to applicable law, regulations, and guidelines, including, where applicable, including:
    a. 28 CFR Part 23 regarding criminal intelligence information;
    b. The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy); and,
    c. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ)

2. Law enforcement officers and other personnel at the DIAC and source agencies who acquire SAR information that may be shared with the DIAC will be trained to recognize behavior that is indicative of criminal activity related to terrorism.

3. When a choice of investigative techniques is available, information documented as a SAR, ESAR and/or ISE-SAR should be acquired or investigated by the DIAC and originating agencies using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

4. Access to and use of ESAR and/or ISE-SAR information is governed by the U.S. Constitution, the state constitution, applicable federal and state laws and local ordinances, and Program Manager for the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) (NSI PMO) policy guidance applicable to the NSI.

F. Information Quality Assurance

1. The DIAC will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the DIAC. The DIAC will advise the appropriate contact person in the source agency in writing this would include electronic notification, if SAR information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

2. The DIAC will make every reasonable effort to ensure that SAR information collected and ESAR and/or ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy source agencies and is as accurate, current, and complete as possible.

3. At the time of posting to the shared space, ESAR and/or ISE-SAR information will be labeled according to the level of confidence in the information source reliability and content validity to the maximum extent feasible.

4. The labeling of ESAR and/or 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 previously retained information.

5. Alleged errors or deficiencies, misleading, obsolete, or otherwise unreliable, in ESAR and/or ISE-SAR information will be investigated in a timely manner and the Center will correct, delete or refrain from using protected information found to be erroneous or deficient information in the shared space.
6. The DIAC will provide written notice, this would include electronic notification to the source agency that provided the SAR and to any user agency that has accessed the ESAR and/or ISE-SAR information posted to the shared spaces when ESAR and/or ISE-SAR information posted to the shared spaces by the DIAC is corrected or removed from the shared spaces by the DIAC because it is erroneous or deficient such that the rights of an individual may be affected.

G. Analysis

1. ESAR and/or ISE-SAR information posted by the DIAC to the shared spaces or accessed from the shared spaces under the NSI will be analyzed for intelligence purposes only by qualified DIAC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly, including training on the implementation of this policy. These personnel shall share ESAR and/or ISE-SAR information only through authorized analytical products.

2. ESAR and/or ISE-SAR information is analyzed according to priorities and needs, including analysis to:
   - Further terrorism prevention, investigation, force deployment, or prosecution objectives and priorities established by the DIAC.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in terrorism-related activities.

H. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used, as appropriate, to determine which system users will be authorized to view privacy fields in ESAR and/or ISE-SAR information in response to queries made through a federated ESAR and/or ISE-SAR search.

2. Unless an exception is expressly approved by the NSI PMO, the DIAC will adhere to the SAR Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, NSI-approved data collection codes, and ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. ESAR and/or ISE-SAR information retained by the DIAC and entered into the DIAC's shared spaces will be accessed by or disseminated only to persons within the DIAC or, as expressly approved by the ESAR and/or NSI PMO, users who are authorized to have access and need the information for specific purposes authorized by law. Access and disclosure of personal information will only be allowed to agencies and individual users for legitimate law enforcement and public protection purposes and only for the performance of official duties in accordance with law.
4. ESAR and/or ISE-SAR information posted to the shared space by the DIAC may be 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 Fusion Center mission and is not exempt from disclosure by law.

I. Disclosure and Correction/Redress

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2, below, an individual who is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the DIAC or a source agency participating in the NSI may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The DIAC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A separate file will be kept by the DIAC Privacy Officer of all requests for records, of all replies to such requests and of what information is disclosed to an individual. Such records shall be retained by DIAC for not less than three (3) years.
2. The existence, content, and source of the information will not be made available to an individual when under: the record is an investigatory record of a law enforcement agency and:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   - Disclosure would endanger the health or safety of an individual, organization, or community.
3. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the DIAC. The individual will also be informed of the procedure for appeal when the DIAC or the source agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates.
4. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the DIAC, the DIAC, as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.
5. The DIAC will acknowledge the complaint and state that it will be reviewed but will not confirm the existence of any ISE-SAR that contains information in

privacy fields that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from the ISE-SAR shared space if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

J. Security Safeguards

1. The DIAC Information Security Officer will also serve as the Security Officer for the ESAR and/or NSI.

2. The DIAC will operate in a secure facility protecting the facility from external intrusion. The DIAC will utilize secure internal and external safeguards against network intrusions of ESAR and ISE-SAR information. Access to the DIAC's ISE-SAR shared space from outside the facility will be allowed only over secure networks.

3. The DIAC will secure ESAR and ISE-SAR information in the DIAC's shared space in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by DIAC personnel authorized to take such actions.

4. Access to ESAR and ISE-SAR information will be granted only to DIAC personnel whose positions and job duties require such access; who have successfully completed a background check and any applicable security clearance; and who have been selected, approved, and trained accordingly.

K. Information Retention for Sharing and Destruction

1. The DIAC will ensure that all ESAR and ISE-SAR information is reviewed for record retention (validation or purge) in accordance with the time period(s) specified for retaining ESAR and ISE-SAR information in the ISE shared space.

2. The DIAC will retain ESAR or ISE-SAR information in the ISE shared space for five (5) years to permit the information to be validated or refuted and its credibility and value to be periodically reassessed. The DIAC shall assign a "disposition" label so that a subsequent authorized user knows the status and purpose for the retention and will retain the information based on any retention period associated with the disposition label.

3. At the time the DIAC's ESAR and ISE-SAR information has been retained in the ISE shared space for five (5) years, the DIAC shall purge the information from the ISE shared space. In order to ensure the rights and privacy of individuals and organizations, the ESAR or ISE-SAR information may be purged prior to the five (5) year limit if the DIAC determines, for any reason, that the information no longer meets the requirements for retention in the ISE.

L. Transparency, Accountability, and Enforcement

L1. Information System Transparency

1. The DIAC will be open with the public in regard to SAR collection and ESAR and ISE-SAR information policies and practices. The DIAC will make the DIAC's Privacy Policy available upon request.

2. The DIAC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections relating to ESAR and ISE-SAR information.

L.2. Accountability

1. The audit log of queries for ESAR and ISE-SAR information will identify the user initiating the query.

2. The DIAC will have access to an audit trail of inquiries to and information disseminated from the shared spaces.

3. The DIAC will adopt and follow procedures and practices to evaluate the compliance of its authorized users with ESAR and ISE-SAR information policy and applicable law. This will include periodic and random audits of logged access to the shared spaces in accordance with NSI policy. A record of the audits will be maintained by the DIAC Privacy Officer.

4. All DIAC personnel shall report violations or suspected violations of the DIAC's NSI privacy policy to the DIAC Privacy Officer.

5. The DIAC will conduct periodic audit and inspection of the information contained in its ESAR and ISE-SAR shared spaces. The audit will be conducted by the DIAC Privacy Officer or an independent auditor, as provided by NSI policy. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the ESAR and ISE-SAR information maintained by the DIAC in the shared space and any related documentation.

The DIAC's appointed and trained Privacy Officer or other expert individual or group designated by the DIAC will periodically review the Privacy Policy, and the DIAC will make appropriate changes in response to changes in applicable law or policy determinations.

M. Enforcement

1. The DIAC reserves the right to restrict the qualifications and number of user agencies and authorized user agency personnel that it certifies for access to ESAR and ISE-SAR information and to suspend or withhold service to any of its user agencies **o**r authorized user agency personnel violating this privacy policy. The DIAC further reserves the right to deny access or participation in the ESAR and NSI to its participating agencies that fail to comply with the applicable restrictions and limitations of the DIAC's privacy policy.

N. Training

1. The following individuals will participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the DIAC.
   - Personnel providing information technology services to the DIAC.
   - Staff in other public agencies as appropriate, providing SAR, ESAR and ISE-SAR information technology or related services to the DIAC.
   - Source agency personnel providing organizational processing services for SAR information submitted to the DIAC.
   - User agency personnel and individuals authorized to access ISE-SAR information who are not employed by the DIAC.

2. The DIAC's privacy policy training program will cover:
   - Purposes of the privacy, civil rights and civil liberties protection policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR, ESAR and ISE-SAR information maintained or submitted by the DIAC to the shared spaces.
   - Originating and participating agency responsibilities and obligations under applicable law and policy.
   - How to implement the policy in the day-to-day work of a participating agency.
   - The impact of improper activities associated with violations of the policy.
   - Mechanisms for reporting violations of the policy.
   - The possible penalties for policy violations, including transfer, dismissal, and criminal liability, and immunity if any.

Appendix 2

Federal Laws, Regulations and References:

U.S. Constitution, First, Fourth, Sixth, Thirteenth and Fourteenth Amendments

USA Patriot Act, Public Law No. 107-56 (October 26, 2001), 115 Stat. 272

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Presidential Executive Order 13526
Classified National Security Information

Classified Information, 32 CFR 2003

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

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

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Homeland Security Act of 2002
codified at 6 U.S.C. § 482(f)(1)

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Intelligence Identities Protection Act,
50 USC 421,

Internal Security Act,
50 USC 783,

IRTPA, as amended by the 9/11 Commission Act

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Law Enforcement Intelligence Systems, National Child Protection Act of 1993, Pub. L. 103-209 (December 20, 1993), 107 Stat. 2490

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

United States Criminal Laws, including 18 USC 641, 783, 793, 794, 798, 952, 1924

Appendix 3

State Laws, Regulations and References:

Delaware Title 11 Chapters 85, 86, Sections 935, 9403

§ 8501. Purpose of Subchapter.

(a) The purpose of this subchapter is to create and maintain an accurate and efficient criminal justice information system in Delaware consistent with this chapter and applicable federal law and regulations, the need of criminal justice agencies and courts of the State for accurate and current criminal history record information, and the right of individuals to be free from improper and unwarranted intrusions into their privacy.

(b) In order to achieve this result, the General Assembly finds that there is a need:

(1) To designate the State Bureau of Identification as the central state repository for criminal history record information;

(2) To require the rapid identification, classification and filing of fingerprints;

(3) To require the reporting of accurate, relevant and current information to the central repository by all criminal justice agencies;

(4) To insure that criminal history record information is kept accurate and current; and

(5) To prohibit the improper dissemination of such information.

(c) This subchapter is intended to provide a basic statutory framework within which these objectives can be attained.

63 Del. Laws, c. 188, § 1.;

§ 8502. Definitions.

The following words, terms and phrases, when used in this subchapter, shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

(1) "Administration of criminal justice" shall mean performance of any of the following activities: Detection, apprehension, detention, pretrial release, post trial release, prosecution, adjudication, correction supervision, or rehabilitation of accused persons or criminal offenders, criminal identification activities, and the collection, storage and dissemination of criminal history record information.

(2) "Conviction data" means any criminal history record information relating to an arrest which has led to a conviction or other disposition adverse to the subject. "Conviction or other disposition adverse to the subject" means any disposition of charges, except a decision not to prosecute, a dismissal or acquittal; provided, however, that a dismissal entered after a period of probation, suspension or deferral of sentence shall be considered a disposition adverse to the subject.

(3) "Criminal history background check" means the acquisition of state or federal criminal history record information for an individual.

(4) "Criminal history record information" shall mean information collected by state or federal criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information or other formal criminal charges and any disposition arising therefrom, sentencing, correctional supervision and release. "Criminal history record information" shall include the names and identification numbers of police, probation, and parole officers, and such information shall not be within the definition of a "public record" for purposes of the Freedom of Information Act, Chapter 100 of Title 29. Pursuant to the provisions of this subchapter, upon application the State Bureau of Investigation shall release to members of the news media, and to individuals and agencies as defined by this subchapter, a random number that is unique and permanent to each arresting officer as a surrogate for the officer's agency or department-issued identification number. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. Nor shall the term include information contained in:

a. Posters, announcements or lists for identifying or apprehending fugitives or wanted persons;

b. Original records of entry such as police blotters maintained by criminal justice agencies which are compiled chronologically and required by law with long-standing custom to be made public, if such records are organized on a chronological basis;

c. Court records of public judicial proceedings;

d. Published court or administrative opinions or public judicial, administrative or legislative proceedings;

e. Records of traffic offenses maintained by the Division of Motor Vehicles for the purpose of regulating the issuance, supervision, revocation or renewal of driver's, pilot's or other operator's licenses;

f. Announcements of executive clemency.

(5) "Criminal justice agency" shall mean:

a. Every court of this State and of every political subdivision thereof;

b. A government agency or any sub-unit thereof which performs the administration of criminal justice pursuant to statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice. Such agencies shall include, but not be limited to, the following:

1. The Delaware State Police;

2. All law-enforcement agencies and police departments of any political subdivision of this State;

3. The State Department of Justice;

4. The Office of the Solicitor of the City of Wilmington;

5. The Delaware Criminal Justice Information System, Office of the Director

6. The Department of Correction;

7. The Division of Youth Rehabilitative Services;

8. The Division of Family Services;

9. The Division of Alcohol and Tobacco Enforcement;

10. The Federal Bureau of Investigation; and

11. The Division of Professional Regulation.

(6) "Criminal Justice Information System" shall mean the computer hardware, software and communications network managed, operated and/or maintained for the Delaware Criminal Justice Information System.

(7) "Disposition" shall include, but not be limited to, trial verdicts of guilty or not guilty, nolle prosequis, Attorney General probations, pleas of guilty or nolo contendere, dismissals, incompetence to stand trial, findings of delinquency or nondelinquency and initiation and completion of appellate proceeding.

(8) "Dissemination" shall mean the transmission of criminal history record information, or the confirmation of the existence or nonexistence of such information. The term shall not include:

a. Internal use of information by an officer or employee of the agency which maintains such information;

b. Transmission of information to the State Bureau of Identification;

c. Transmission of information to another criminal justice agency in order to permit the initiation of subsequent criminal justice proceedings;

d. Transmission of information in response to inquiries from criminal justice agencies via authorized system terminals, which agencies provide and/or maintain the information through those terminals.

(9) "Governmental agency" shall mean any agency of the government of the United States or the State of Delaware or any political subdivision thereof. It does not include a private individual, any private corporate entity or other nongovernmental entity.

(10) "Law-enforcement officer" shall include police officers, special investigators pursuant to § 9016 of Title 29, the Attorney General and the Attorney General's deputies, state fire marshals, municipal fire marshals that are graduates of a Delaware Police Academy which is accredited/authorized by the Council on Police Training, sworn members of the City of Wilmington Fire Department who have graduated from a Delaware Police Academy which is authorized/accredited by the Council on Police Training, environmental protection officers, enforcement agents of the Department of Natural Resources and Environmental Control, environmental protection officers, enforcement agents of the Department of Natural Resources and Environmental Control, sheriffs and their regular deputies, agents of the State Division of Alcohol and Tobacco Enforcement correctional officers and constables.

(11) "Nonconviction data" means arrest information without disposition if an interval of 1 year has elapsed from the date of arrest and no active prosecution of the charge is pending, or information disclosing that the police have elected not to refer a matter to a prosecutor, or that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals.

(12) "Recipient agency" means any government agency which is directed or authorized by law to conduct a criminal history background check for the purposes of employing or licensing any individual in this State.

(13) "Release status" shall mean information concerning whether or not an individual is incarcerated and the reason therefor, which shall include but is not limited to information concerning releases on bail, or on own recognizance, commitments in default of bail, referrals to other agencies, decision of prosecutors not to commence or to postpone criminal proceedings, release from institutions and any conditions imposed concerning those released.

63 Del. Laws, c. 188, § 1; 65 Del. Laws, c. 452, §§ 1-3; 68 Del. Laws, c. 101, § 1; 70 Del. Laws, c. 186, § 1; 71 Del. Laws, c. 199, §§ 12, 13; 71 Del. Laws, c. 205, § 1; 72 Del. Laws, c. 50, § 1; 72 Del. Laws, c. 371, § 3; 72 Del. Laws, c. 379, §§ 4, 5; 73 Del. Laws,

c. 249, § 3; 73 Del. Laws, c. 252, §§ 1-5; 74 Del. Laws, c. 224, § 1; 74 Del. Laws, c. 250, § 2; 77 Del. Laws, c. 326, § 1.;

§ 8503. Function; administration; appointment of Director.

(a) The State Bureau of Identification, hereinafter referred to as the "Bureau," is continued within the Division of State Police. The Bureau shall be the central state repository for criminal history record information (CHRI) and such additional information as specified in this subchapter.

(b) Subject to this subchapter, the Bureau shall be administered by the Superintendent of State Police. It shall be equipped and maintained by the State Police as a separate budget unit within the Department of Safety and Homeland Security.

(c) The Superintendent of State Police shall appoint, subject to the approval of the Department of Safety and Homeland Security, a Director of the Bureau. The Director shall be a regularly appointed member of State Police, who shall be trained and experienced in the classification and filing of fingerprints, and the Director and all other employees of the Bureau shall be subject to the same rules and regulations governing the State Police.

(d) A representative of the Bureau to be designated by the Superintendent shall be a member of any board or regulatory body established for the collection, retention and dissemination of criminal history information.

42 Del. Laws, c. 181, § 1; 11 Del. C. 1953, § 8501; 57 Del. Laws, c. 670, §§ 4A, 4B; 63 Del. Laws, c. 188, § 1; 70 Del. Laws, c. 186, § 1; 74 Del. Laws, c. 110, § 138.;

§ 8504. Personnel.

The Bureau personnel shall consist of regular appointed members of the State Police, and such other personnel as may be deemed necessary to carry out this chapter. The personnel so appointed shall each be experienced in the work to be performed by them.

42 Del. Laws, c. 181, § 2; 11 Del. C. 1953, § 8502; 63 Del. Laws, c. 188, § 1.;

§ 8505. Duty to provide security of criminal history record information and security investigations.

(a) The Director shall provide security of criminal history record information contained in the facilities of the Bureau.

(b) The Director shall establish procedures to assure that Bureau records, under the control or custody of any authorized agency, shall be protected from unauthorized access, disclosure or dissemination.

(c) Each employee of the Bureau working with or having access to criminal history record information shall be made familiar with the substance and intent of this chapter.

(d) Direct access to criminal history record information from the Bureau shall be available only to authorized officers or employees of a criminal justice agency, and, as necessary, to other authorized personnel essential to the proper operation of the criminal history record information system.

(e) The Director shall be responsible for investigations of violations of this chapter.

63 Del. Laws, c. 188, § 1; 68 Del. Laws, c. 101, § 2.;

§ 8506. Duty to maintain complete and accurate records; performance of annual audit.

(a) The Bureau shall maintain in a complete and accurate manner information received pursuant to this subchapter to the maximum extent feasible.

(b) Any and all criminal history records and other information which is transmitted directly by computer terminal by a criminal justice agency shall be deemed to have been transmitted to the Bureau within the meaning of this subchapter.

(c) The Bureau shall file all information received by it and shall make a systematic record and index thereof, to the end of providing a method of convenient reference and consultation. No information identifying a person received by the Bureau may be destroyed by it until 10 years after the person identified is known or reasonably believed to be dead, or until that person reaches age 80 or reaches age 75 with no criminal activity listed on the person's record in the past 40 years, whichever shall first occur, except as otherwise provided by statute.

(d) A criminal justice agency shall, upon finding inaccurate criminal history record information of a material nature, notify all criminal justice agencies, and all other persons and agencies, known to have received such information.

(e) When a criminal justice agency receives notification that an inaccuracy appears in criminal history record information having originated with that agency, such agency shall take appropriate steps to correct the inaccuracy.

(f) The Bureau shall assure that an annual audit is conducted of a representative sample of agencies accessing or maintaining data files as provided in this subchapter. This audit shall encompass both manual and computerized data systems, and shall be conducted at such time and according to procedures as the Bureau shall prescribe. A full report of the findings of each audit made pursuant to this subsection shall be communicated to the individual agency so audited.

42 Del. Laws, c. 181, § 9; 11 Del. C. 1953, § 8509; 63 Del. Laws, c. 188, § 1; 67 Del. Laws, c. 379, § 1; 70 Del. Laws, c. 186, § 1.;

§ 8513. Dissemination of criminal history record information.

(a) Upon application, the Bureau shall furnish a copy of all information available pertaining to the identification and criminal history of any person or persons of whom the Bureau has a record to:

(1) Criminal justice agencies and/or courts of the State or of any political subdivision thereof or to any similar agency and/or court in any State or of the United States or of any foreign country for purposes of the administration of criminal justice and/or criminal justice employment;

(2) Any person or the person's attorney of record who requests a copy of the person's own Delaware criminal history record, provided that such person:

a. Submits to a reasonable procedure established by standards set forth by the Superintendent of the State Police to identify one's self as the person whose record this individual seeks; and

b. Pays a reasonable fee as set by the Superintendent, payable to the Delaware State Police;

(3) The State Public Defender when requesting information about an individual for whom the State Public Defender is attorney of record.

(b) Upon application, the Bureau shall, based on the availability of resources and priorities set by the Superintendent of State Police, furnish information pertaining to the identification and criminal history of any person or persons of whom the Bureau has a record, provided that the requesting agency or individual submits to a reasonable procedure established by standards set forth by the Superintendent of the State Police to identify the person whose record is sought. These provisions shall apply to the dissemination of criminal history record information to:

(1) Individuals and public bodies for any purpose authorized by Delaware state statute or executive order, court rule or decision or order;

(2) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. Said agreement shall embody a user agreement as prescribed in § 8514 of this title;

(3) Individuals and agencies for the express purpose of research, evaluative or statistical activities pursuant to a specific agreement with a criminal justice agency. Said agency shall embody a user agreement as prescribed in § 8514 of this title;

(4) Individuals and agencies for purposes of international travel;

(5) Individuals and agencies required to provide a security clearance for matters of national security.

(c) Upon application the Bureau may, based upon the availability of resources and priorities set by the Superintendent of State Police, furnish information pertaining to the identification and conviction data of any person or persons of whom the Bureau has record, provided that the requesting agency or individual submits to a reasonable procedure established by standard set forth by the Superintendent of State Police to identify the person whose record is sought. These provisions shall apply to the dissemination of conviction data to:

(1) Individuals and agencies for the purpose of employment of the person whose record is sought, provided:

a. The requesting individual or agency pays a reasonable fee as set by the Superintendent, payable to the Delaware State Police; and

b. The use of the conviction data shall be limited to the purpose for which it was given;

(2) Members of the news media, provided that the use of conviction data shall be limited to the purpose for which it was given, and the requesting media or news agency pays a reasonable fee as set by the Superintendent, payable to the Delaware State Police.

(d) Dissemination of criminal history record information by any person or agency other than the Bureau or its designee is prohibited. This provision shall not prohibit dissemination by any criminal justice agency in those cases in which time is of the essence and the Bureau is technologically incapable of responding within the necessary time period. Under such circumstances the foregoing rules concerning dissemination are to be adhered to.

(e) Appropriate records of dissemination shall be retained by the Bureau and criminal justice agencies storing, collecting and disseminating criminal history record information to facilitate audits. Such records shall include, but not be limited to, the names of persons and agencies to whom information is disseminated and the date upon which such information is disseminated.

(f) Unless otherwise specified by the court order directing that a record be sealed, such sealing shall not preclude dissemination of the arrest or conviction information concerning the subject of the court order, nor shall it preclude dissemination of the fact a sealed record exists, providing any dissemination made is pursuant to this chapter and Chapter 43 of this title.

(g) Notwithstanding any law or court rule to the contrary, the dissemination to the defendant or defense attorney in a criminal case of criminal history record information pertaining to any juror in such case is prohibited. For the purposes of this subsection,

"juror" includes any person who has received notice or summons to appear for jury service. This subsection shall not prohibit the disclosure of such information as may be necessary to investigate misconduct by any juror.

(h) [Repealed.]

42 Del. Laws, c. 181, § 11; 11 Del. C. 1953, § 8511; 59 Del. Laws, c. 551; 63 Del. Laws, c. 188, § 1; 70 Del. Laws, c. 186, § 1; 73 Del. Laws, c. 385, § 1; 76 Del. Laws, c. 392, § 5; 77 Del. Laws, c. 348, § 8.;

§ 8513A. Governmental agency access to the Criminal Justice Information System (CJIS)

Access to the Criminal Justice Information System, including computerized criminal history, shall be available to governmental agencies (as defined by this statute); provided, that the requesting agency meets the following conditions:

(1) In order to be eligible to obtain information from CJIS, an agency must offer written evidence that the public interest in dissemination or access outweighs the security and privacy interests of the person or persons upon whom access is sought, and that access is germane to the mission of the agency.

(2) The agency shall submit to an application procedure as established by the Board of Managers. Said procedure shall identify the specific information being sought.

(3) Approval of the agency's application, which may be in whole, in part, or as modified by the Board, shall require a two-thirds majority of the entire Board of Managers.

(4) Upon approval of the agency's application, the agency shall enter into a user's agreement as prescribed in § 8514 of this title.

(5) The agency shall bear all costs associated with CJIS access, once granted. This section does not pertain to access to police complaint information contained in CJIS collected as a result of the requirements as specified in § 8507(a)(4) of this title. Such access shall remain within the discretion of the Director of the State Bureau of Identification.

71 Del. Laws, c. 205, § 2.;

§ 8514. User agreements.

(a) Use of criminal history record information disseminated to noncriminal justice agencies shall be restricted to the purpose for which it was given.

(b) No criminal justice agency shall disseminate criminal history record information to any person or agency pursuant to § 8513(a)(3) and (b)(1), (2) and (3) of this title unless

said person or agency enters into a user agreement with the Bureau, which agreement shall:

(1) Specifically authorize access to the data or information;

(2) Limit the use of the data or information to purpose for which it was given;

(3) Ensure the security and confidentiality of the data or information consistent with this chapter.

(c) An individual or agency which has entered into a user agreement as prescribed by subsection (b) of this section, and which knowingly or recklessly violates the terms of that agreement, shall be guilty of a class A misdemeanor and shall be punished according to Chapter 42 of this title. Upon such violation, the user agreement shall be terminable at the option of the Bureau.

63 Del. Laws, c. 188, § 1.;

§ 8601. Purpose.

The purpose of this chapter is to maintain an accurate and efficient criminal justice information system in Delaware consistent with Chapter 85 of this title and applicable federal law and regulations, the need of criminal justice agencies and courts of the State for accurate and current criminal history record information, and the right of individuals to be free from improper and unwarranted intrusions into their privacy.

63 Del. Laws, c. 352, § 1.;

§ 8602. Definitions.

The following words, terms and phrases, when used in this chapter, shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

(1) "Administration of criminal justice" shall mean performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correction supervision or rehabilitation of accused persons or criminal offenders, criminal identification activities, and the collection, storage and dissemination of criminal history record information.

(2) "Criminal history record information" shall mean information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision and release. "Criminal history record information" shall include the names and identification numbers of police, probation, and parole officers, and such information shall not be

within the definition of a "public record" for purposes of the Freedom of Information Act, Chapter 100 of Title 29. Pursuant to the provisions of this subchapter, upon application the State Bureau of Investigation shall release to members of the news media, and to individuals and agencies as defined by this subchapter, a random number that is unique and permanent to each arresting officer as a surrogate for the officer's agency or department-issued identification number. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. Nor shall the term include information contained in:

a. Posters, announcements or lists for identifying or apprehending fugitives or wanted persons;

b. Original records of entry such as police blotters maintained by criminal justice agencies which are compiled chronologically and required by law with long-standing custom to be made public, if such records are organized on a chronological basis;

c. Court records of public judicial proceedings;

d. Published court or administrative opinions or public judicial, administrative or legislative proceedings;

e. Records of traffic offenses maintained by the Division of Motor Vehicles for the purpose of regulating the issuance, supervision, revocation or renewal of driver's, pilot's or other operator's licenses;

f. Announcements of executive clemency.

(3) "Criminal justice agency" shall mean:

a. Every court of this State and of every political subdivision thereof;

b. A government agency or any subunit thereof which performs the administration of criminal justice pursuant to statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice. Such agencies shall include, but not be limited to, the following:

1. The Delaware State Police;

2. All law-enforcement agencies and police departments of any political subdivision of this State;

3. The State Department of Justice;

4. The Office of the Solicitor of the City of Wilmington;

5. The Department of Correction;

6. The Division of Youth Rehabilitative Services;

7. The Delaware Criminal Justice Information System, Office of the Director;

8. The Division of Professional Regulation.

(4) "Criminal Justice Information System" shall mean the computer hardware, software and communication network managed, operated and maintained by the Delaware Criminal Justice Information System.

(5) "Disposition" shall include, but not be limited to, trial verdicts of guilty or not guilty, nolle prosequis, Attorney General probations, pleas of guilty or nolo contendere, dismissals, incompetence to stand trial, findings of delinquency or nondelinquency and initiation and completion of appellate proceeding.

(6) "Dissemination" shall mean the transmission of criminal history record information, or the confirmation of the existence or nonexistence of such information. The term shall not include:

a. Internal use of information by an officer or employee of the agency which maintains such information;

b. Transmission of information to the State Bureau of Identification;

c. Transmission of information to another criminal justice agency in order to permit the initiation of subsequent criminal justice proceedings;

d. Transmission of information in response to inquiries from criminal justice agencies via authorized system terminals, which agencies provide and/or maintain the information through those terminals.

(7) A "governmental agency" shall mean any agency of the government of the United States or the State of Delaware or any political subdivision thereof. It does not include a private individual, corporation or other nongovernmental entity.

63 Del. Laws, c. 352, § 1; 65 Del. Laws, c. 451, §§ 1-3; 68 Del. Laws, c. 103, §§ 1, 2; 71 Del. Laws, c. 204, § 1; 74 Del. Laws, c. 224, § 2; 77 Del. Laws, c. 326, § 3.;

8604. Board of Managers -- Duty to insure compliance with statute.

The Board shall insure that the State Bureau of Identification and all other criminal justice agencies collecting, storing or disseminating criminal history record information

and other information concerning crimes and offenders comply with this chapter and Chapter 85 of this title.

63 Del. Laws, c. 352, § 1.;

§ 8605. Rules and regulations.

The Board shall have the power and authority to promulgate rules and regulations to insure compliance with this chapter not inconsistent with Chapter 85 of this title.

63 Del. Laws, c. 352, § 1; 68 Del. Laws, c. 103, § 5.;

§ 8606. Office of the Director; function and duties.

(a) Appointment and duties of Executive Director. -- The Executive Director shall be appointed by and serve at the pleasure of the Board. The duties of the Executive Director shall include, but not be limited to:

(1) The employment and supervision of required employees.

(2) The preparation and management of an annual budget, and such other funds as are designated for the development and operation of the Criminal Justice Information System.

(3) Provide such administrative support to the Board as may be necessary.

(4) The preparation of policy, procedure and directives as may be required to implement this chapter and Chapter 85 of this title, or as the Board may require.

(5) Be the Chief Operational Officer of the Criminal Justice Information System, as per this title and established Board policy.

(6) The preparation of an annual report on the status of the Criminal Justice Information System.

(b) Primary functions. -- The primary function of the Office of the Director shall be the assurance of the efficient and reliable development and operation of the hardware, software and database which comprise the Criminal Justice Information System; thereby, effectively collecting, storing and disseminating through the automated system, for all authorized users, criminal justice information, including criminal history record information.

(c) Duty to provide security. -- The Office of the Director shall provide for automated security as follows:

(1) Provide for secure system access for all criminal justice information system users through the administration of the Delaware Criminal Justice Information System security programs;

(2) Employ effective and technologically adequate software and hardware designs to prevent unauthorized access or modifications to any information contained within the Criminal Justice Information System;

(3) Insure that access to computer facilities, systems operating environments, data file contents and system documentation whether in use or stored in a media library, shall be restricted to specifically authorized organizations and/or personnel;

(4) Procedures shall be instituted to assure that all Delaware Justice Information System facilities provide safe and secure record storage;

(5) Procedures shall be instituted to assure that any agency or individual authorized access to the information system shall be responsible for the physical security of criminal history record information, or other such sensitive information, under its control or in its custody, and such information shall be protected from unauthorized access, disclosure or dissemination;

(6) Direct access to criminal history record information, or other such sensitive information, shall be available only to other authorized personnel essential to the proper operation of the Criminal Justice Information System;

(7) Each employee, office or contracted employee, working with, or having access to the Criminal Justice Information System shall be made familiar with the substance and intent of this chapter and Chapter 85 of this title.

(d) Duty to maintain complete and accurate records; performance of an audit. -- The Office of the Director, or such contracted firms as may be employed, shall conduct an audit of the Criminal Justice Information System files and of the agencies accessing the system. The audit will be conducted according to established systems auditing procedures, and other such procedures as the State Bureau of Identification may prescribe. An audit will be conducted upon concurrence of the Board.

(e) Duty to provide training. -- The Office of the Director shall assure that training programs are established for all automated systems within the scope of the Criminal Justice Information System and provide for adequate documentation and manuals for the use of such systems.

(f) Duty to assure system operations. -- The Office of the Director shall provide for the continued operation of the Criminal Justice Information System, including such maintenance as required.

(g) Duty to provide information resource management. -- The Office of the Director shall provide the management of the Criminal Justice Information System data, assuring the effective use of the information resource.

(h) Duty to assure compliance with state criminal justice system; duty to provide effective management. -- The Office of the Director shall have the duty to assure that all Criminal Justice Information System developments shall meet the requirements of the state criminal justice system and its member agencies and courts, and provide for the effective management of the development process.

(i) Duties pursuant to cooperative agreement or express policy. -- The Office of the Director shall perform such duties as the Board deems necessary within the bounds of the Criminal Justice Information System, its management and maintenance, as established through cooperative agreement or express Board policy.

68 Del. Laws, c. 103, § 5.;

§ 8607. Violations and investigations.

All suspected or reported violations of Chapter 85 or subchapter III, subpart K of Chapter 5 of this title shall be reported to the Director of the State Bureau of Investigation, with said agency having responsibility for the investigation of the reported violation.

68 Del. Laws, c. 103, § 6.;

§ 8608. Personnel.

(a) No person shall be appointed, promoted or transferred to any position with an agency which has or allows access to criminal history record information facilities, systems operating environments or data file contents, whether while in use or stored in a media library, without a criminal history record check by the employing agency. No person shall be appointed, promoted or transferred to such a position by an agency if promotion or transfer could endanger the security, privacy or integrity of such information.

(b) The Board shall initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have access to such information, where such personnel violated Chapter 85 of this title.

(c) The Board shall provide for the establishment of a plan for resolving employee grievances, complaints and appeals.

63 Del. Laws, c. 352, § 1; 68 Del. Laws, c. 103, § 5.;

§ 8609. Denial of appointment, etc., to position allowing access to criminal history record information.

(a) Nothing in this chapter or in any rule promulgated hereunder shall limit the authority of a criminal justice agency or of the Board under § 8605 of this title to deny the appointment, promotion or transfer of any person to any position which has or allows access to criminal history record information.

(b) The Board shall have authority under the rules to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel of a criminal justice agency who are authorized to have or allow access to criminal history record information where such personnel violate Chapter 85 of this title.

(c) Any person who is otherwise qualified for a position under this chapter who is denied appointment, promotion or transfer to such position or who is transferred or removed from such position under § 8605 of this title shall be given a written statement of the reason or reasons therefore by the agency responsible for such action, and the agency shall promptly give written notice of its action to the Board.

63 Del. Laws, c. 352, § 1; 68 Del. Laws, c. 103, § 5.;

§ 8610. Access; conditions.

Access to the Criminal Justice Information System, including computerized criminal history, shall be available to governmental agencies (as defined by this statute) provided that the requesting agency meets the following conditions:

(1) In order to be eligible to obtain information from CJIS, an agency must offer written evidence that the public interest in dissemination or access outweighs the security and privacy interests of the person or persons upon whom access is sought, and that access is germane to the mission of the agency.

(2) The agency shall submit to an application procedure as established by the Board of Managers. Said procedure shall identify the specific information being sought.

(3) Approval of the agency's application, which may be in whole, in part, or as modified by the Board, shall require a two-thirds majority of the entire Board of Managers.

(4) Upon approval of the agency's application, the agency shall enter into a user's agreement as prescribed in § 8514 of this title.

(5) The agency shall bear all costs associated with CJIS access, once granted.

This section does not pertain to access to police complaint information contained in CJIS collected as a result of the requirements as specified in § 8507(a)(4) of this title.

Such access shall remain within the discretion of the Director of the State Bureau of Identification.

71 Del. Laws, c. 204, § 2.;

§ 935. Misuse of computer system information.

A person is guilty of the computer crime of misuse of computer system information when:

(1) As a result of accessing or causing to be accessed a computer system, the person intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system;

(2) That person intentionally or recklessly and without authorization:

a. Alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system; or

b. Interrupts or adds data to data residing within a computer system;

(3) That person knowingly receives or retains data obtained in violation of paragraph (1) or (2) of this section; or

(4) That person uses or discloses any data which that person knows or believes was obtained in violation of paragraph (1) or (2) of this section.

64 Del. Laws, c. 438, § 1; 70 Del. Laws, c. 186, § 1.;

§ 9403. Nondisclosure of information about victim.

(a) Unless a victim or witness waives confidentiality in writing, neither a law-enforcement agency, the prosecutor, nor the corrections department may disclose, except among themselves or as authorized by law, the residential address, telephone number or place of employment of the victim or a member of the victim's family, or the identity, residential address, telephone number or place of employment of a witness or a member of the witness's family, except to the extent that disclosure is of the site of the crime, is required by law or the Rules of Criminal Procedure, is necessary for law-enforcement purposes, or is permitted by the court for good cause.

(b) A court may not compel a victim or witness or a member of the victim's or witness's family testifying in a criminal justice proceeding to disclose a residential

address or place of employment on the record unless the court finds that disclosure of the information is necessary.

(c) The victim's address, place of employment and telephone number and any witness's identity, address, place of employment and telephone number, maintained by a court, prosecutor or law-enforcement agency pursuant to this chapter is exempt from disclosure under the Freedom of Information Act [Chapter 100 of Title 29].

68 Del. Laws, c. 445, § 1; 69 Del. Laws, c. 167, § 1; 72 Del. Laws, c. 211, §§ 3-5.;