National Security State Information Center's Privacy Policy

STRENGTH THROUGH COLLABORATION

I. Acknowledgements

The National Security State Information Center (NSSIC) Privacy Policy is a living document developed through the joint efforts of the Puerto Rico Office for Public Security Affairs, now known as the Puerto Rico Homeland Security Office (PRHSO), the Puerto Rico Department of Justice and agencies such as the Puerto Rico Emergency Management Agency.

Key members and Agencies which supported this project were:

Rafael Muñoz, PRHSO's Director
Lawyer Karla M. Rivera, Puerto Rico Dept. of Justice
Mr. Orlando Morales PRHSO's
Christina Abernathy and John Wilson, Institute for Intergovernmental Research

In addition, documents such as the Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems, and the Freedom of Information Act played a crucial role in the development of this Policy.

II. Introduction

September 11, 2001 will always remain in our memories and in our history as the day we were awakened to the knowledge that Global Terrorism had reached our coasts. It brought into focus the need to reassess our methods of gathering/sharing/using information on terrorists, criminal activities, and the individuals and organizations likely involved. It also highlighted the need to do so in an efficient and effective manner, one that would systematically minimize any negative effect not only on the State but also on the People, and ultimately, The Nation. One aspect crucial in improving our capacity to prevent harm is the use new technology to supply clear, concise, and rapid information to those who will be able to maximize its usage. However, the benefits reaped from this aspect cannot compromise another aspect: ***the individuals' privacy, civil rights, and civil liberties***.

The following privacy policy protects these rights while improving public safety. When individuals are sufficiently comfortable with the integrity of information system operations, they are more likely to cooperate with and support them, thus enhancing public safety and our way of life.

The policy here drawn represents a commitment of the Puerto Rico Fusion Center to uphold the rights granted by U.S. Constitution, the Puerto Rico State laws and other laws adopted over time for the protection of Human Rights and Civil Liberties.

III. Table of Revisions

The following table defines dates and descriptions of changes done to the NSSIC's Privacy Policy through the years, location of changes and the authors of said changes. The table defines the reason for the changes, if the changes are based on corrections, inclusions, omissions, or general changes defined by stakeholders such as State and federal agencies, presidential directives and/or changes in state laws affecting in any way the procedures of the NSSIC. The changes will appear in green Arial 14 font to be easily recognized. The new versions will absorb previous changes to minimize misunderstandings.

Version	Change date	Authors	Description
1	**N/A**	**O. Morales**	**Original release**
2	**N/A**	**O. Morales**	**Changes include integration into the document of comments from IIR and State laws that can have impact on the privacy policy (stricter, prohibitive, etc.). This revision protocol was not determined until September 7, 2010, so changes were in different fonts/colors.**
3	**Sept. 7, 2010**	**K. Rivera, O. Morales**	**A new format was implemented to streamline the information; the official name of NSSIC was introduced; ISE and SAR information was integrated in the Policy.**
4	**November 3, 2010**		**Updated version based on a Webinar session with members of the DOJ/DHS Fusion Center Privacy Technical Assistance providers (Privacy Policy Review Team) to assist NSSIC in complying with the ISE Privacy Guidelines requirements and the DHS/DOJ *Fusion Center Privacy Policy Development Template* (April 2010).**
5	**November 9, 2010**	**K. Rivera, O. Morales**	**Addition of POC's e-mail addresses and law citations related to information access**
6	**June 2014**	**S. Lebrón**	**POC e-mail updated. Corrected the name of the center: The National Security State Information Center.**

Contents

IV. Policy Provisions

This *Privacy Policy* embraces the eight Privacy Design Principles developed by the Organization of Economic Cooperation and Development's *Fair Information Practices* while following appropriate privacy and civil liberties safeguards as outlined in the principles and shall be used to guide the policy wherever applicable. The eight Privacy Design Principles are:

A. **Purpose Specification —** Define agency purposes for information to help ensure agency uses of information are appropriate.
B. **Collection Limitation** — Limit the collection of personal information to that required for the purposes intended.
C. **Data Quality** — Ensure data accuracy.
D. **Use Limitation** — Ensure appropriate limits on agency use of personal information.
E. **Security Safeguards** — Maintain effective security over personal information.
F. **Openness** — Promote a general policy of openness about agency practices and policies regarding personal information.
G. **Individual Participation** — Allow individuals with reasonable access and opportunity to correct errors in their personal information held by the agency.
H. **Accountability** — Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

All these principles have, as common end results, an increase in local public safety and national security, thus minimizing the threat and risk of injury to first responder personnel, the public in general, and all property involved. This task, always taking into consideration the individual privacy, civil rights, civil liberties, and other protected interests will support the integrity of the criminal investigation and the justice system we believe in.

We at the NSSIC will strive to promote our capabilities thus minimizing reluctance of individuals or groups to use or cooperate with the system by creating an atmosphere of governmental legitimacy and accountability which will make the most effective use of our public resources allocated to the public's safety.

A. Purpose

The Puerto Rico State Information Center or Centro de Información del Estado as defined in Spanish is a Fusion Center (herein referenced to as "Center") as defined below:

A Fusion Center is a collaborative effort of two or more agencies who provide resources, expertise, and/or information to the Center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorism activity. It will also be able to maintain critical communication before, during and after any natural disasters affecting Puerto Rico and the rest of the Nation.

The Center project began to take shape in response to the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of the Center focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated. Another key component of the Fusion Center will also address communications between all agencies that, directly or indirectly, are related to any man-made or natural disasters, thus making the Center an All-Threats/All-Hazards Fusion Center.

The Center's intelligence products and services will be available to law enforcement agencies, other criminal justice entities, and all agencies, and private sector operations based on their need-to-know classification. All agencies participating in the Center will be subject to a Memorandum of Understanding and will be required to adhere to all Center policies and security requirements. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information while information analysis and intelligence are developed and exchanged.

The Center will develop databases by using existing data sources from participating entities to integrate data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity, and other crimes for investigative leads as well as trends and patterns related to All-Hazards. Examples of such information will be that related to any terrorist activities that might have any tie-ins or include words such as Puerto Rico, local gangs or terrorist groups. Crimes that could be related to organizations within Puerto Rico will also be monitored for evidence of large scale or interstate crime that could or could not be related to terrorist cells. Cyber terrorism or identity theft focused on Puerto Rican citizens living in the mainland will be monitored for origins that could be in Puerto Rico or international origins. All-Hazards will include information relating to spills, fires, accidents or events at Critical Infrastructures or National Monuments, etc. This capability will facilitate integration and exchange of information between the participating agencies.

B. Collection Limitation

The Center is founded and maintained to analyze information and intelligence by agencies participating in the project. The decision of the agencies to participate in the Center and about which databases to provide is voluntary and will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal and state laws.

Because the laws, rules, or policies governing information and intelligence that can be collected and released on private individuals varies from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information is to abide by the collection limitations applicable to it by reason of law, the Center's and their own policies and

procedures. This will include the proper labeling of information aligned with the Center and all other participating Agencies. Information contributed/generated by the Center will be aligned throughout the program and will be collected in conformance with agreed upon policies and procedures.

C. Data Quality

The agencies participating in the Center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the Center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated *before* any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

D. Use Limitation

Information obtained from or through the Center is exclusively for lawful purposes. A lawful purpose means the request for data is directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act. This includes any terrorist acts or threats within our island or Nationwide and which might have a connection to Puerto Rico in any way.

The **Commander-of-Center (CoC)** will take necessary measures to make certain that access to the Center's information and intelligence resources is secure and will prevent any unauthorized access or use. The Board reserves the right to restrict the qualifications and number of personnel who will be accessing the Center and to suspend or withhold service to any individual violating this *Privacy Policy*. The **Center's Executive Committee (CEC)**, or persons acting on behalf of the CEC, further reserves the right to conduct inspections concerning the proper use and security of the information received from the Center.

Security for information derived from the Center will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to Center data and/or sensitive information will be trained as to those requirements. All personnel having access to the Center's data agree to abide by the following rules:

1. The Center's data will be used only to perform official investigative-related duties related to All-Threats/All Hazards in a manner authorized by the user's employer.

2. Individual passwords will not be disclosed to any other person except as authorized by agency management.
3. If authorized personnel of any of the participating agencies or members of the Center suspect their passwords were disclosed or compromised, said passwords will be changed.
4. Background checks will be completed on personnel who will have direct access to the Center.
5. Use of the Center's data in an unauthorized or illegal manner will subject the user to denial of further use of the Center; discipline by the user's employing agency, and/or criminal prosecution.

All NSSIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the center's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

All NSSIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the list of applicable state and federal privacy, civil rights, and civil liberties laws referenced in Appendices B and C of this policy.

The NSSIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the listing of applicable state and federal privacy, civil rights, and civil liberties laws referenced in Appendices B and C of this policy.

Each authorized user understands that access to the Center can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

E. Security Safeguards

1. Information obtained from or through the Center will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign.

2. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes, (2) disclosed or published without prior approval of the contributing agency, or (3) disseminated to unauthorized persons.

3. Use of the Center's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the

Center will be granted only to law enforcement and all participating agencies' personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Fusion Center Governance Board.

4. Each individual user will be provided with an electronic copy of this privacy policy and must complete and sign a hard copy of an Individual User Agreement Form after having read the policy acknowledging receipt of the policy and confirming agreement to comply with the policy and provisions here contained. This form will be supplied upon arrival to the Fusion Center and kept in records for 5 years or while the individual maintains connections with the Fusion Center. New Privacy Policy updates will be distributed and Letters of Assignment will be supplied to the Individuals for their signatures. These documents will be kept with the User Agreement Forms initially signed by each Individual. The individual's key information will be stored in a database for future reference as well as to tie-in with the log files. In addition, to confirm each Individual's skills, the Center will be doing a skills review test before granting access. The Center will ask the individual to make a formal request and will deny him access if the skills are not up to requirements defined in the CONOPS.

5. Access to the Center's databases from outside of the Center will only be allowed over secure network lines and with the approval of the Fusion Center Governance Board. A logging system will be implemented to maintain records of the information sought and collected, by whom and when it was collected. This will allow full traceability of queries and their purposes.

F. Openness

The Center will allow access to the Privacy Policy to all personnel working at the Center's database and analysis desks as well as participating agencies that require the support of the Center. The access will be direct for all users that have an actualized user name and password. Only the CoC will have authorization to edit the Policy and only after a review and approval of the NSSIC Privacy Oversight Committee. All participating agencies either will have a representative at the Center or a connection through a secure line, allowing the review of the policy at any time. In addition, the Privacy Policy will be available on the NSSIC's website for the public's review and comments in both English and Spanish.

G. Individual Participation

The data maintained by the Center is provided, on a voluntary basis, by the participating agencies or is information obtained from other sources by the Center. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination,

and use of any information that results from the search process. The individual will also be responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the Center's applications. Persons wishing to access data pertaining to themselves will make a formal request to the Center but the data will not identify the originating agency. The Center will communicate directly with the agency or entity that is the source of the data in question and will supply them with the new data supplied by the member of the public requesting the review. If the information is correct, the originating agency will correct their data, will inform the Center, who will inform the inquirer about the correction done.

Participating agencies agree that they will only attend requests related to their agencies.

H. Accountability

Any query request made to the Center's data applications is automatically logged by the system identifying the user initiating the query. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement investigative purpose or to other agencies as provided by law. The agency *from* which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:

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

The Governance Board will be responsible for conducting or coordinating audits and investigating misuse of the Center's data or information. The Center's CoC or Privacy Officer (when assigned) shall report all violations and/or exceptions to the Board and will serve as the liaison for the Information Sharing Environment. Individual users of the Center's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use limitations for the use of the Center's data may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the Center is required to abide by this *Privacy Policy* in the use of information obtained by and through the Center.

V. Governance

1. Primary responsibility for the operation of the Center, its information systems, operations, personnel coordination; the receiving, and the enforcement of this policy is assigned to the Commander-of-Center (CoC). This will include all operations such as: seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information.

2. The Center is guided by three separate but crucial Committees: 1) The Center's Executive Committee, who is the decision-making group as well as manages budgets and key-decisions affecting the Center, and acts as ambassadors of the program, 2) the Center Privacy Oversight Committee, that monitors the Center's Privacy Policy, its proper application and any infringements of this policy and its related Federal and state laws, and 3) the NSSIC Committee, composed of representatives from all the stakeholders involved one way or another, in the NSSIC. This last Committee is basically composed of the suppliers as well as customers of the NSSIC.

    a. The NSSIC's Executive Committee (EC) is comprised, but not restricted to nine members. These will represent the State's Public Safety agencies as well as the Governor's representatives in matters related to Homeland Security. They have direct authority and ownership in the decision-making and goal setting processes of the Center. The Committee **is** comprised of the following:

        - Homeland Security Advisor for Puerto Rico
        - Superintendent of the Puerto Rico Police Department
        - Director Puerto Rico Homeland Security Office
        - Director Puerto Rico Emergency Management Agency
        - Director Emergency Medical Service
        - Director Puerto Rico National Guard
        - Secretary Puerto Rico Department of Justice
        - Director, Puerto Rico Fire Department
        - Director HIDTA (honorary)
        - Any other member appointed by the Governor

    b. The NSSIC Privacy Oversight Committee (NSSIC-POC) shall be comprised, but not restricted to five members. These members have knowledge of State and/or federal laws relating to privacy policies and would be composed of at least the following:

        - A trained Privacy Officer (PO) from the Center or the CoC if no PO has been assigned.
        - A legal counsel representative (Attorney at Law or DOJ)

- ❖ A Law Enforcement Official (Local Law Enforcement or FBI Official)
- ❖ A representative of the Governor, House of Representatives or the Senate
- ❖ A representative of Civil, Human Rights Advocates

3. An appointed and trained Center PO (or COC until a PO is appointed) will receive all reports regarding alleged errors and violations of the provisions of the Privacy Policy, receive and coordinate complaint resolution under the center's redress policy, guide the CPOC, act as the liaison between the Information Sharing Environment, the NSSIC-POC, the stakeholders and the Community to ensure the Center adheres to the Provisions for the ISE privacy guidelines as well as all Guidelines defined herewith. The Privacy Officer can be contacted at the following e-mail address: nssic@policia.gov

   In addition, the Privacy Oversight committee liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the center's information collection, retention, and dissemination processes and procedures.

   The NSSIC Committee composed of representatives or Fusion Liaison Officers (FLO's) from all the stakeholders involved in the NSSIC bring forth concerns, needs and/or requests from their agencies or groups. In addition, they can submit changes in policies, procedures, and protocols that should be addressed by the NSSIC. All this information is consolidated and brought to the attention of the NSSIC -EC by the CoC during their routine meetings. The Committee is comprised of FLO's from State and Federal Agencies involved in Law enforcement, Public Safety or support both of first responders and Critical Infrastructure. It will, at a later date, include representatives from the Sector Specific Security Groups of Critical Infrastructure within the Territory as well as a representative of the Region Fusion Centers as they become available.

4. When the operation becomes too complex to be handled only by the Commander of Center (increased facility size, data volume handled or personnel attached), a Center Security Officer (CSO) will be hired. The CSO will be responsible for security policy-making, development of security awareness among the staff and stakeholders, risk assessment of information assets, conduct periodic vulnerability assessment and recommend controls in light of the value vs. threat vs. vulnerability vs. cost. Furthermore, he will analyze all logs to initiate preventive measures such as modification of access privileges, deletion of user id's, and review of access privileges on a need-to-know basis.

VI. Information Procedures, Processes and Guidelines

A. Information Collection

1. The Center will seek or retain information that:
   - Is based upon a criminal predicate or threat to public safety, or
   - Is based upon reasonable suspicion that an identifiable individual or organization has committed a criminal offense or 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, or
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
   - Is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches);or
   - Is based on a level of suspicion that is less than reasonable suspicion, such as tips and leads or suspicious activity reports (SARs) and ISE-SARs; and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, when appropriate.

2. The Center will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. Labels will be applied by participating agencies and to center-originated information to indicate to the accessing authorized user that:

   - The information pertains to protected information, to include “personal data” on any individual (as defined in Appendix A of this policy), and, to the extent expressly provided in this policy, includes organizational entities.
   - The information is subject to laws, in Appendices B and C, restricting access, use, or disclosure.

4. The Center personnel will, upon receipt of information, assess the information to determine its nature and purpose and will assign categories to the information (or ensure that the originating agency has assigned categories to the information). Personnel will assign information to categories to indicate the result of the assessment, such as:
   - Whether the information is general data, tips and leads data, suspicious activity reports(SAR’s or ISE-SAR’s), or criminal intelligence information;

- The nature of the source (for example, anonymous tip, interview, public records, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the NSSIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
    - Protect confidential sources and police undercover techniques and methods.
    - Not interfere with or compromise pending criminal investigations.
    - Protect an individual's right of privacy or their civil rights and civil liberties.
    - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, participant in a witness protection program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information within this section will be reevaluated whenever:
    - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
    - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. NSSIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:
    - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.
    - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
    - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for three years in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The NSSIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (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 information privacy, civil rights, and civil liberties.

9. The labels will also define accessibility and sensitivity of disclosure of said information based on the state and Federal laws regarded in this Policy. All analysts, their supervisors and the Commander of Center will have access to all information gathered in the Center. Liaisons at the participating agencies will have access to information requested, conditioned to the type of information and how it relates to either them or their agencies. The Center's Concept of Operations Manual (NSSIC -CONOPS) defines these same labels and their proper use policy, as well as all other policies and procedures related to the Center. All personnel will be required to adhere to the practices, such as collection, use, analysis, retention, destruction, sharing, and disclosure of information, defined by the CONOPS procedures. These procedures are defined to abide strictly by all state and Federal laws that protect privacy, civil rights, and civil liberties herewith in defined. The primary laws being the U.S. Constitution (First, Fourth, and Sixth Amendments), the Constitution of the Commonwealth of Puerto Rico (Sections 1-20), and the Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983. All other laws and regulations applied to this center, its participants and the information herewith collected are outlined in the Appendixes B and C.

10. The PRISC will identify and review protected information originating from the center prior to sharing that information in the ISE. Further, the Center will provide notice mechanisms, including, but not limited to, metadata or data fields that will enable ISE authorized users to determine the nature of the protected information. This will allow them to handle effectively the information in accordance with applicable legal

requirements. Prior to the implementation of this Privacy Policy, the CONOPS will be released, defining all policies, including SAR Submittal Form and information handling policy, with exact methodology and procedures. They will be defined by type of participating agency and dissemination procedures. One key dissemination policy will be that no information related to on-going or past criminal investigations will be disseminated to non-law enforcement agencies unless specified in writing by the Center's Commander of Center. This is aligned with the 28 CFR Part 23.

11. The NSSIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    - The name of the originating 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 who questions regarding the information should be directed.

12. The NSSIC 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.

13. The NSSIC will keep an electronic record of the source of all information sought and collected by the center.

14. All information gathered through any method of investigative techniques used by the Center and affiliated agencies and handled in any way (collection, use, analysis, retention, destruction, sharing, and disclosure of information) will strictly comply and adhere to the following regulations and guidelines:

    - 28 CFR Part 23
    - Organisation for Economic Co-operation and Development's (OECD) *Fair Information Practices* (except under conditions defined by the Federal Privacy Act; state, local, or agency policy).
    - To criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
    - ISE-SAR Functional Standard (Version 1.5)
    - Local, state and federal laws as defined in Appendix B & C.

15. The NSSIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and

participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

16. The NSSIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals and/or organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

17. The Center will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, and federal laws and which is not based on misleading information collection practices.

18. The Center will not directly or indirectly receive, seek, accept, or retain information from any individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy; or if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information.

19. If, at any time, the Center develops information gathering and investigative functions, the techniques used will be the least intrusive necessary in the particular circumstance to gather legally authorized information. These procedures will be defined in the NSSIC CONOPS prior to the Center's implementation.

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

.

B. Information Quality Assurance

1. The Center will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete. It will also include the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [Refer to Section C: Collation and Analysis] has been met. One method is the labeling of said information based on its level of quality (accurate, complete, current, verifiable, and reliable).

2. The Center will investigate, during its analysis and if part of the program, its investigative phase, in a timely manner, alleged errors and deficiencies and will

correct, delete, or refrain from using protected information found to be erroneous or deficient. The Center will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the Center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable. All methodologies used are defined in the Center's Concept of Operations Manual (NSSIC -CONOPS).

3. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the center's confidence (validity and reliability) in retained information or when there is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

4. The Center will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be corrected at the source agency, deleted from the system, or not used when the Center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable.

5. SLT agencies, including agencies participating in the ISE, are responsible for the quality and accuracy of the data accessed by or shared with the Center. Originating agencies providing data remain the owners of the data contributed. The Center will advise the appropriate data owner, in writing, if its data is found to be inaccurate, incomplete, out of date, or unverifiable. This also includes incorrectly merged information, or information that lacks adequate context such that the rights of the individual may be affected.

6. The Center will use written or documented electronic notification to inform recipient agencies when information previously provided by the Center is deleted or changed by the center (for example, it is determined to be inaccurate or includes incorrectly merged information).

C. Collation, Analysis and Merging

1. Information acquired by the Center or accessed (Collation) from other sources will only be analyzed by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly as per procedures outlined in the NSSIC -CONOPS.

2. The information these analysts will evaluate is information as defined in Section VI, A. Information Collection of this policy.

3. This information will be related to any information which might shed light unto a possible criminal or terrorist act to occur or which might have occurred. This includes ties to any known criminal or terrorist organizations, events in which they were/are involved and which might be related to criminal or terrorist acts, etc.

4. Information acquired by the Center or accessed from other sources is analyzed (**Analysis**) according to priorities and needs and will only be analyzed to:
   - Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the Center
   - 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.
   - Grant support to agencies during an All-Hazard situation while analyzing any information which could be connected to a terrorist act, group or individual

5. Records about an individual or organization from two or more sources will not be merged (**Merging**) during a routine analysis unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match. The set of identifying information can be, but is not limited to:
   - name (full; partial if there is more evidence supporting the merge)
   - date of birth
   - law enforcement or corrections system identification number
   - Individual identifiers, such as fingerprints, photographs, clearly defined tattoos, or scars; social security number; driver's license number; or other biometrics.

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

D. Sharing and Disclosure

1. The Center will assign clearly defined, credentialed, access to certain individuals as defined in the NSSIC -CONOPS. Each user category or classification will have access to specific types of information. Within the Center, only the CoC, the analysts and their supervisors, will have full access to all information lines available to the Center. They will be the personnel who looks for tendencies, detect threats, or supports criminal investigations for the PRPD, Fire or other law enforcement agencies not only in Puerto Rico but within the Nation's Public Safety Community. This includes other State and Regional Fusion Centers, FBI, and DHS personnel on a need-to-know basis. Other categories of personnel, such as IT, the PIO, or any support staff, do not require access to said information and will be defined so in the NSSIC -CONOPS. The Commander of Center, the PIO and the analyst supervisors will be the only personnel assigned to Information sharing. **No individual within the Center will be capable of editing collected data from participating agencies.** If the Center detects external information requiring editing, the supplying agency will be informed as they have the exclusively right to change it. The Center

will then receive the updated information and share it with any other agency that might be using said information. This will maintain accuracy throughout the system.

2. The NSSIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. Use of the Center's data is limited to those individuals who have been selected, approved, and trained accordingly. This means that any Fusion Liaison Officer wishing to have access to the Center and its databases will need to follow the same requirements of the Centers analysts. Access to information contained within the Center will be granted only to the Fusion Liaison Officers of law enforcement and participating agencies' personnel which will have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Fusion Center Governance Board. They will also receive training in Privacy Policy, Civil Liberties and Rights in accord with the DHS Privacy Office guidelines.

4. The Center personnel who will have access to all information collected, analyzed and merged will be the Intelligence Analysts, their Supervisors, the CSO, and the Commander of Center. The Public Information Officer (PIO) will not have access to this information as well nor will have full privileges. The PIO will be oriented by the CoC or the CSO on what information can be made public.

5. Access to or disclosure of records retained by the Center will be provided to persons within the Center 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. An audit trail will be kept of access by or dissemination of information to such persons as defined in the NSSIC -CONOPS. Participating agencies may not disseminate information received from the Center without approval from the originator of the information, be it the Center itself or any other originating agency as agreed upon signing the Center's MOU.

6. Records retained by the NSSIC 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. 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.

7. Information gathered or collected and records retained by the NSSIC 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. 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 for a minimum of three years by the center.

8. Information gathered and records retained by the Center may be accessed or disclosed to **a member of the public** only if the information is defined by law to be a public record or otherwise appropriate for release to further the agency mission and is not excepted from disclosure by law. Such information may only be disclosed in accordance with the law and procedures applicable to the Center for this type of information or when there is a legitimate need. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

9. Information gathered and records retained by the Center ***will not*** be:
   - Sold, published, exchanged, or disclosed for commercial purposes
   - Disclosed or published without prior notice to the contributing agency that such information is subject to re-disclosure or publication
   - Disseminated to unauthorized persons.

10. There are several categories of records that will ordinarily ***not be provided*** to the public:

    - Some public records are required to be kept confidential by Federal or Puerto Rico law as they have been deemed exempted from disclosure. Records exempt from disclosure under the Puerto Rico Public Information Law, include:
      - Investigatory records of law enforcement agencies are exempted from disclosure requirements due to the nature of the information and their possible use in criminal investigations. However, certain law enforcement records must be made available for inspection and copying **as long as there availability status does not interfere with a criminal or terrorist related investigation**.
      - Intelligence information, including information subject to 28 CFR Part 23.
      - Protected federal, state, or local records, which may include records owned or controlled by another agency.
      - A violation of the nondisclosure agreement.
      - Puerto Rico court decisions that address exemptions under the Puerto Rico Public Information Law include the following: Colón Cabrera vs. Caribbean Petroleum Corp., 2007 TSPR 48/170 DPR 582 (Hernández Denton); Santiago vs. Bobb, 117 DPR 153,159, and Angueira Navarro vs. Junta de Libertad 2000 TSPR 2, 150 DPR 10 (Negrón García)

    - 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 the Critical Infrastructure Information Act of 2002. This includes a record assembled,

prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

- 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 accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

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

The above exceptions can be better defined through the following citations from the case of Colón vs. Caribbean Petroleum, 170 DPR 582, (2007). In which it is stated that:

We consider, first of all, if the information which is the object of the request, can be catalogued as public information. It is necessary to do this preliminary determination due to the fact that, once a document is catalogued as public, any citizen has the right to request access to it subject to determined exceptions.

Article 1(b) of the Law of Public Documents, 3 L.P.R.A. 1001(b), defines a public document as "any document which originates, or is kept or received in any dependency of the Commonwealth of Puerto Rico according to the law or in relation to the management of public affairs and that pursuant to the provisions of § 1002 of this title is required to be permanently or temporarily preserved

In our System of law we do not have a special legislation that disposes the exceptions in which the Government of Puerto Rico can maintain certain documents out of the public scrutiny. However, this Court has affirmed the supposed occasions in which the Government can claim confidentiality validly, as: (1) when a law declares so; (2) when the communication is protected by any of the evidentiary privileges that citizens can invoke; (3) when revealing the information can damage fundamental rights of third parties; (4) when it involves the identity of a confidant, and (5) when it is official information according to the Rules 414 and 415 of Evidence. (citations omitted) To maintain the confidentiality, the Government has the responsibility to prove that it satisfies any of the exceptions before mentioned.

In synthesis, all law that pretends to hide information to a citizen under the cloak of confidentiality has to justify itself to plenitude. This is satisfied if the legislation (1) falls within the constitutional power of the government; (2) promotes an important or substantial governmental interest;
Page 593
(3) the governmental interest is not related with the suppression of freedom of expression; and (4) the concomitant restriction of the right to freedom of expression is not larger than the essential to promote said interest. (citations omitted) Thereby, the State can invoke the mantle of secretiveness in cases of imperative public interest. Id

Colón vs. Caribbean Petroleum, 170 DPR 582, (2007).

E. Redress

1. Disclosure

1. An individual is entitled to know the existence of and to review the information about him or her, up to a certain degree, which has been gathered and retained by the Center and only upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity. The disclosure of said information is subject to the conditions specified below. The individual may obtain a copy of the information to challenge the accuracy or completeness of the information. The Center'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. All requests and what information is disclosed will be kept on file.

2. The existence, content, and source of the information will not be made available to an individual under Federal or Puerto Rico Public Information Law as defined in section VI.D (Sharing and Disclosure) when:

   - 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
   - The information is in a criminal intelligence system
   - The information relates to issues related to investigations addressing any criminal or terrorist related incident.
   - The information source does not reside with the Center
   - The Center did not originate or does not own or have a right to disclose the information.

   If the information does not originate with the center, the requestor will be referred to the originating agency, if appropriate or required, or 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.

3. Types of information which ordinarily will not be disclosed to members of the public upon their request for review are ownership of a gun which might have been involved in an violent incident, any possible ties relating directly or

indirectly with organized crime, money laundering, or terrorist acts and similar situations. This will be based on a case-by-case situation but will be based on the proper use of both State and Federal laws.

2. Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information retained about him or her ***within a system under the Center's control***, the Center 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. The procedure submittal will be made in writing and the individual will sign an understanding on his obligation to follow the procedure step-by-step.

2. If an individual has complaints or objections to the accuracy or completeness of information about him or her that ***originates with another agency***, the Privacy Office (or CoC while there is no CSO appointed) will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must consent to the correction, remove the record, or assert a basis for denial. A record will be kept of all complaints and correction requests.

3. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
   (a) Is exempt from disclosure,
   (b) Has been or may be shared through the ISE,
   (c)(i) Is held by the Center and
   (ii) Allegedly has resulted in demonstrable harm to the complainant,

   The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following e-mail address: nssic@policia.gov. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 working 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, 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. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

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

5. If any correction request is denied, to an individual he or she will be given reasons for the rejection. The individual will then be informed of the procedure for appeal when the center or originating agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

6. If records that have not been disclosed to a complainant require redressing procedures, the Center will address the issue under applicable law.

F. Security Safeguards

1. The Center Security Officer CSO (or CoC while there is no CSO appointed) will be designated and trained to serve as the center's security officer. The CSO be responsible for all security issues asked of the Center as well as stakeholders and users privileges. He will monitor access privileges; deletion of user id's and reviews of access privileges on a need-to-know basis.

2. The Center will operate in a secure facility protecting the facility from external intrusion, using secure internal and external safeguards against network intrusions. Access to Center databases from outside the facility will only be allowed over secure networks, as the Center 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.

3. The NSSIC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

4. As previously pointed out, access to the Center's information will only be granted to Center personnel whose position and job duties require such access. These individuals have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly. Queries made to the Center data applications will be logged into the data system identifying the user initiating the query. The Center will utilize watch logs to maintain audit trails of requested and disseminated information.

5. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

6. The Center will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical, reputational, 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. The Center will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

G. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. The decision to retain or destroy will be based on whether the information has no further value to the Center's products/Analysts, has not been reviewed in the last five years or meets the criteria for removal according to the Center's retention and destruction policy. If the Center decides information will be removed, it will be purged, destroyed, and deleted or returned to the submitting source. Notification of proposed destruction or return of records will be provided to the contributor, based on agreement with the providing agency. No approval will be required from the originating agency before information held by the Center is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

2. If information collected by the FC will be destroyed, any agency which has received said information will be informed 30 days in advance, in case they want the Center to retain the information as source evidence for an on-going investigation. In that case, an extension of one (1) year will be assigned to the information for future review. If no written notice is received during those 30 days, the information will be automatically destroyed.

3. A record of all these steps will be kept within the Center electronic archives, setting a marker on the date for future review.

H. Information System Transparency, Accountability and Enforcement

1. The Center will be open with the public in regard to information and intelligence collection practices. The Center's privacy policy will be provided to the public for review, will be made available upon request, and will be posted online at Homeland Security Information Network page (HSIN). The Privacy Officer (or COC until Privacy Officer is assigned) will be responsible for receiving and responding to

inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). The Privacy Officer can be contacted at nssic@policia.gov

2.

3. Queries made to the Center data applications will be logged into the data system identifying the user initiating the query. The Center's watch log will be utilized to maintain an audit trail of requested or disseminated information for three years.

4. The Center will provide a CD copy of this policy to all agency and non-agency personnel who provide services and will require written acknowledgement of receipt of this policy and agreement of compliance to this policy and the provisions it contains (MOU). The Center 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. This will include logging access of these systems and periodic auditing of these systems, as to not establish a pattern of the audits. These audits will be mandated at least quarterly, and a record of the audit will be maintained by the commander (or designee) of the Center.

5. The Center's personnel or other authorized users shall report violations or suspected violations of Center policies relating to protected information to the Center's privacy officer. The Center will annually conduct internal audits and inspections of the information contained in its criminal intelligence system. In addition, the CEC and CPOC will have the authority to or assign a panel to conduct random audits. This third-party panel has the option of conducting a random audit, without announcement, at any time and without prior notice to the Center. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system.

6. The CPOC (or Privacy Officer) will annually review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

7. The Center will notify an individual about whom sensitive personally identifiable information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical, reputation, 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.

8. The Privacy Officer (or COC until Privacy Officer is assigned) ensures that enforcement procedures and sanctions outlined in Section VI, H Information System Transparency, Accountability, and Enforcement are adequate and enforced.

9. Any authorized user found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information will be submitted to any of the following by the Privacy Officer (or COC until Privacy Officer is assigned):
   - Suspension and/or discontinue access to information by the user
   - Suspension, demotion, transfer, or termination of the person, as permitted by applicable personnel policies
   - The application of administrative actions or sanctions as provided by the Center's rules and regulations or as provided in agency personnel policies
   - If the user is from an agency external to the center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions
   - And/or refer the matter to appropriate authorities for criminal prosecution, as necessary, to effect the purposes of the policy.

10. The NSSIC 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.

I. Training

1. The Center 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:
   - All assigned personnel of the center
   - Personnel providing information technology service to the Center
   - Staff in other public agencies or private contractors providing services to the agency,
   - Users who are not employed by the agency or a contractor.

2. The Center will provide special training to personnel authorized to receive, handle, access or share protected information in the Information Sharing Environment regarding the center's requirements and policies for collection, use, and disclosure of protected information.

3. The Center'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 information retained by the Center

- How to implement the policy in the day-to-day work of the user, whether a paper or systems user
- The impact of improper activities associated with infarction accessible within or through the agency
- Mechanisms for reporting violations of center privacy-protection policies
- The nature and possible penalties for policy violations, including suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution
- Originating and participating agency responsibilities and obligations under applicable law and policy.

Appendix A – Terms and Definitions

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

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

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

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

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

Agency/Center — Agency/Center refers to the Center and all participating state agencies of the Center.

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

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

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

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

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

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

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

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

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

Credentials — Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per
28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per
28 CFR Part 23.

Data—Inert symbols, signs, or measures.

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

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

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

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

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

The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

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

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

Homeland Security Information— As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

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

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

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

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

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

ISE-Suspicious Activity Report (ISE-SAR) – An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

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

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

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

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

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

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

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

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

Non-repudiation— A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides

undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

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

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

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

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

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

Privacy — Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy — A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information

relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection — This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Protected Information —

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

Public — Public includes:

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

Public does not include:

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

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

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

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

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

Retention — Refer to "Storage."

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

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

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

Security — Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

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

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

   Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Sunshine Laws – U.S. federal and state laws requiring regulatory authorities' meetings, decisions and records to be made available to the public.

Suspicious Activity —Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR) — Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) 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.

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

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

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

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

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

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

Appendix B - Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Excerpt from U.S. Department of Justice's (DOJ) *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*

The following is a brief listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

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

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

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

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

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

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

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

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

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

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301
Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

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

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

IRTPA, as amended by the 9/11 Commission Act

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

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

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

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

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

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

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

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

Appendix C - State Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Collected from the Lex Juris

The following is a brief listing of state laws that one way or another protects individuals' *privacy, civil rights, and civil liberties* of Individuals under the Commonwealth of Puerto Rico. The list is arranged in alphabetical order by popular name.

Constitution of the Commonwealth of Puerto Rico, Sections 1-20

Letter of Rights of Carriers of the HIV Virus in Puerto Rico, C.C.P.R. § 523, P. de la C. 2980), Law 349, 2000

Record Inspections - Information Access, **Department of Justice, Special Investigations Bureau Law, C.C.P.R. § 138 l. Title 3 – Executive Power**

Protection and Safety of Infants in Hospital Facilities, **C.C.P.R. § 322 Public Policy Declaration, Title 24 – Health and Hygiene**

Organized Crime and Money Laundering Law, **C.C.P.R. § 971q, Judicial Authorization for recording non-telephone conversations, Title 25 – Internal Security**

Civil Rights**, C.C.P.R., Law No. 131 de 13 de mayo de 1943, as amended; sections 1-6**

Elderly Rights Act, C.C.P.R. § 343, Bill of Rights, Title 8 - Public Well Being and Charity Institutions

Well-being and Integral Protection for Childhood Law, Responsibilities and coordination with other agencies, **C.C.P.R. § 444c**

Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2158, Title 33 – Penal Code

Prohibition of Interception of telephone Communications - Inadmissible in Evidence**, Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2161, Title 33 – Penal Code**

Prohibition of Interception of telephone Communications - Penalties**, Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2162, Title 33 – Penal Code**

Illegal Use of Telecommunications - Prohibitions**, Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2163, Title 33 – Penal Code**

Illegal Use of Telecommunications – Manufacture, Possession or Equipment Transfer**, Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2164, Title 33 – Penal Code**

Illegal Use of Telecommunications – Inapplicability of Public Service and Emergency Communications**, Puerto**

Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2165, Title 33 – Penal Code

Prohibition of Reproduction, Transfer, Copying, Printing, Banner Use, Publicity and Sale, of Sound Recordings and Live Shows**, Puerto Rico Penal Code of 1937 and miscellaneous Penal Laws, C.C.P.R. § 2168, Title 33 – Penal Code**

Illegal Collection of Personal Information**, Penal Code of 1974, C.C.P.R. § 4182, Title 33 - Penal Code**

Written Communication Privacy Violation**, Penal Code of 1974, C.C.P.R. § 4184, Title 33- Penal Code**

Interception of Verbal Private Communication**, Penal Code of 1974, C.C.P.R. § 4185, Title 33 - Penal Code**

Recording, **Penal Code of 1974, C.C.P.R. § 4186, Title 33- Penal Code**

Disclosure of Private Conversation**, Penal Code of 1974, C.C.P.R. § 4187, Title 33 - Penal Code**

Private Conversation Publishing**, Penal Code of 1974, C.C.P.R. § 4188, Title 33 - Penal Code**

Message Alteration**, Penal Code of 1974, C.C.P.R. § 4189, Title 33 - Penal Code**

Improper Private Communication Usage**, Penal Code of 1974, C.C.P.R. § 4190, Title 33 - Penal Code**

Serious crimes**, Penal Code of 1974, C.C.P.R. § 4191, Title 33 - Penal Code**

Disclosure of Professional Secrets, **Penal Code of 1974, C.C.P.R. § 4192, Title 33 – Penal Code**

Personal Tranquility Intrusion, **Penal Code of 1974, C.C.P.R. § 4193, Title 33 – Penal Code**

Fraudulent Interference with counters or communication equipment**, Penal Code of 1974, C.C.P.R. § 4275**, **Title 33 – Penal code**

Wired communication Fraud**, Penal Code of 1974, C.C.P.R. § 4275b, Title 33 – Penal Code**

Alteration, Damage or Destruction of Computers, **Penal Code of 1974, C.C.P.R. § 4275c, Title 33 – Penal Code**