Mariana Regional Fusion Center- Privacy Policy

September 2019

Table of Contents

A. Purpose Statement

The mission of the Mariana Regional Fusion Center is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the Marianas while protecting privacy, civil rights, civil liberties, and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected This policy has the express purpose of fulfilling that mission by ensuring strict adherence to all applicable federal and state constitutional rights, statutory, and regulatory protections while:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice systems processes and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals and damage to real or personal property.
- Minimizing reluctance of individuals or groups to use or cooperate with the justice systems.
- Making the most effective use of public resources allocated to public safety agencies.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening the ongoing business of the justice system.

B. Policy Applicability and Legal Compliance

1. All participating MRFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the MRFC'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 private contractors, private entities, and the general public.

2. The MRFC will provide a printed copy of its Privacy Policy to all MRFC personnel, none agency personnel who provide services to the MRFC, and to each source agency and CPIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

3. All MRFC personnel, participating agency personnel, personnel providing information technology services to the MRFC, Stakeholders, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, civil liberties, and other applicable protected interests including but not limited to the United States Constitution, 28 Code of Federal Regulation, Organic Act of Guam Bill of Rights, and Applicable Laws in the Guam Code Annotated.

4. The MRFC adopts internal operating procedures and policies that are compliant with applicable local, state and federal laws protecting privacy, civil rights and civil liberties. Procedures that are consistent with the provisions of this privacy policy, as well as all applicable state and federal constitutional rights and statutes and regulations, including 28 CFR Part 23.

C. Governance- and Oversight

1. Primary responsibility for the operation of the MRFC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the MRFC Director.

2. The MRFC is guided by a designated privacy oversight committee that liaises with the community to ensure that privacy, civil rights, and civil liberties are protected as provided in this policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures

The committee will annually review and update the P/CRCL policy in response to changes in law and implementation experience, including the results of audits and inspections, and will solicit input from stakeholders on the development of or proposed updates to the policy.

3. The MRFC's privacy committee is guided by a trained Privacy Officer who is appointed by the Director of the center. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the center (and for the Information Sharing Environment), ensuring that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: 221-B CHALAN PALASYO AGANA HEIGHTS GUAM 96910

4. The MRFC's Privacy Officer ensures that enforcement procedures and sanctions outlined in the enforcement section are adequate and enforced. (See Enforcement Section for details)

D. Definitions

- For examples of primary terms and definitions please refer to Appendix- A- Terms and Conditions

The remainder of this page was intentionally left blank

E. Information

1. They will seek or retain information (including "protected attributes," subject to conditions articulated in Section E.2., that:

- Is based on a possible threat to public safety or the enforcement of criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that 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 crime analysis or in the administration of criminal justice and public safety (including topical searches), 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, if appropriate. The center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads (including suspicious activity report [SAR] information) subject to the policies and procedures specified in this policy.

2. In accordance with applicable laws, guidance, and regulations, the MRFC not seek or retain and will inform information-originating agencies not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.

When participating on a federal law enforcement task force or when documenting a SAR or an ISESAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

3. The MRFC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is subject to all applicable Guam and Federal Law that restricts access, use or disclosure.
- The information is protected information as defined by the ISE Privacy Guidelines and guidelines established by 5 GCA 260-20611 Record Management Act, and to the extent expressly provided in this policy, that includes organizational entities

4. The MRFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads (including SAR data), criminal history, intelligence

information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the MRFC 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 and his or her 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, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under section 5 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. The MRFC 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 (including 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 which 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 PII).
- 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 five (5) years in order to work an unvalidated tip or lead 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 MRFC 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 MRFC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels, to enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The MRFC 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, when feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

11. The MRFC 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.

12. The MRFC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

1. Information-gathering and access and investigative techniques used by the MRFC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

- 28 CFR Part 23 regarding "criminal intelligence information," as applicable.
- The FIPPs; Fair Information Practice Principles, but note that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP) (Ver. 2).
- Constitutional provisions; Organic Act of Guam 141b Bill of Rights: 5 GCA Chapter 10 Sunshine Reform act of 1999; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

2. The MRFC's SAR process provides for human review and vetting to ensure that information is both gathered in an authorized and lawful manner and, when applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff members will be trained to recognize those behaviors and incidents that are indicative of criminal activity associated with terrorism.

3. The MRFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals 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, ethnicity, national origin, religion, etc.) and civil liberties (speech, assembly, association, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared

4. Information-gathering and investigative techniques used by MRFC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access the MRFC'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.

6. The MRFC will contract only with commercial database entities that provide an assurance that their methods for gathering PII comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

7. The MRFC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity that may receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
- • An individual who or information provider that is legally prohibited from obtaining or disclosing the information

G. Data Quality Assurance

1. The MRFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable has been met.

2. The MRFC will put in place a process for additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. The MRFC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

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

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

5. The labeling of retained information will be reevaluated by the MRFC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

6. The MRFC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

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

8. The MRFC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. Collation and Analysis

1. Information acquired or received by the MRFC or accessed from other sources will be analyzed only by qualified and properly trained individuals who have successfully completed a background check and possess the appropriate security clearance.

2. Information subject to collation and analysis is information as defined and identified in Section E (Information)

3. Information acquired or received by the MRFC] or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

- Further crime prevention (including terrorism), law enforcement, public safety, 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.

The MRFC requires that all analytical products be reviewed [and approved] by the Privacy Officer [or privacy oversight committee] to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

1. Information will be merged only by qualified individuals who have successfully completed a background check and possess the appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

2.The set of identifying information sufficient to allow merging by the MRFC may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

3. If the matching requirements are not fully met but there is reason to believe the records are about the same individual, the information may be associated by the MRFC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosures

1. Credentialed, role-based access criteria will be used by the MRFC as appropriate, to control:
   - The information to which a particular group or class of users can have access based on the group or class.
   - The information a class of users can add, change, delete, or print.
   - To whom, individually, the information can be disclosed and under what circumstances.

2. The MRFC 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 associated with terrorism.

3. Access to or disclosure of records retained by the MRFC] will be provided only 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 which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.

4. Agencies external to the MRFC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

5. Records retained by the MRFC 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.

6. Information gathered or collected, and records retained by the MRFC 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 Five (5) years by the MRFC.

7. Information gathered or collected and records retained by the MRFC may be accessed or disclosed to a member of the public only if the information is defined by law [citation to applicable law] to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

8. Information gathered or collected, and records retained by the MRFC will not be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior notice to the originating agency that such information is subject to

disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency or specifically authorized by the originating agency.
- Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will ordinarily not be provided to the public:
   - Records required to be kept confidential by law are exempted from disclosure requirements under 5 GCA CH 10 Sunshine Reform Act of 1999, and the Organic Act of Guam Bill of Rights ss1412b
   - Information determined by the federal government to meet the definition of "classified information" as defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
   - Investigatory records of law enforcement agencies that are exempted from disclosure requirements under GCA CH 10 Sunshine Reform Act of 1999, and the Organic Act of Guam Bill of Rights ss1412b. However, certain law enforcement records must be made available for inspection and copying under [cite public records act and applicable section].
   - 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 GCA CH 10 Sunshine Reform Act of 1999, and the Organic Act of Guam Bill of Rights ss1412b. By way of example, this may include a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under GCA CH 10 Sunshine Reform Act of 1999, and the Organic Act of Guam Bill of Rights ss1412b] or an act of agricultural terrorism under GCA CH 10 Sunshine Reform Act of 1999, and the Organic Act of Guam Bill of Rights ss1412b vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
   - Protected federal, state, local, tribal, or territorial records, which may include records originated and controlled by another agency that cannot, under 28 CFR Part 23 be shared without permission.
   - A record, or part of a record that constitutes trade secrets or information that is commercial, financial, or otherwise subject to a nondisclosure agreement that was obtained from a person and is privileged and confidential 28 CFR Part 23

10. The [name of center] shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

K. Redress

K.1 Disclosure

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2., below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the MRFC . The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). 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. A record will be kept of all requests and of what information is disclosed to an individual.

2. The existence, content, and source of the information will not be made available by the MRFC to an Individual 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 information system subject to 28 CFR
- Part 23 [see 28 CFR § 23.20(e)].
- The information relates to local laws 1421b Bill of Rights Organic Act of Guam, 5 GCA CH 10 Sunshine Reform Act of 1999
- The information source does not reside with the center.
- The center did not originate and does not have a right to disclose the information. • Other authorized basis for denial.

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.

K.2 Corrections

1. If an individual requests correction of information originating with the MRFC that has been disclosed, the center's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

K.3 Appeals

1. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the MRFC or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.4 Complaints

1. 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 or directors designee at the following

address: 221-b Chalan Palasayo Agana Heights Guam 96910 The Privacy Officer or directors designee 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 or **directors designee** will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

Sample Best Practice Language:

This complaint procedure is applicable to all requests for information and intelligence held by the center. 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) . (b) Has been or may be shared through the ISE.

a. (1) Is held by the MRFC and

b. (2) Allegedly has resulted in demonstrable harm to the complainant.

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

L. Security Safeguards

1. The MRFC's security officer is designated and trained to serve as the center's security officer.

2. The center will comply with generally accepted industry or other applicable standards for security, in accordance with MRFC Security Plan. Security safeguards will cover any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related MRFC activity.

The MRFC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.

3. The MRFC ill 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. The MRFC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

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

6. Queries made to the MRFC's data applications will be logged into the data system identifying the user initiating the query.

7. The MRFC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

9. All individuals with access to MRFC's information or information systems will report a suspected or confirmed breach to the Privacy Officer as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

The MRFC adheres to Title 9 GCA SS48.30 and SS 48.40 in the event of a date breach The MRFC will protect all government and private records consistent with the Records Management T- 5 GCA SS2060-20611

M. Information and Retention and Destruction

1. All criminal intelligence information, as that term is defined in 28 CFR § 23.3, will be reviewed for record retention (validation or purge) by MRFC at least every five (5) years, in accordance with 28 CFR Part 23. For other information or intelligence, the record retention will be established by state law or local ordinance, or in accordance with a retention schedule established by the MRFC (Refer to the Records Management Act 5 GCA SS 2060-20611

2. When information has no further value or meets the criteria for removal according to the MRFC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

3. The MRFC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

4. The procedure contained in Records Management Act 5 GCA SS2060-20611will be followed by MRFC for notification of appropriate parties, including the originating agency, before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

5. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the MRFC depending on the relevance of the information and any agreement with the originating agency.

6. A record of information to be reviewed for retention will be maintained by the [name of center] and, for an appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

7. A printed or electronic confirmation of the deletion will be provided to the originating agency when required under law or if pursuant to the terms of a pre-established agreement with the agency.

N. Accountability and Enforcement

Information System Transparency

1. The MRFC will be open with the public regarding information and intelligence collection practices. The center's P/CRCL policy will be provided to the public for review, made available upon request, and posted on the center's website ghs.guam.gov or hsin.dhs.gov

2. The MRFC's privacy officer and or the director's designee will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer or the directors designee can be reached at the following 221-b Chalan Palasayo Agana Heights 96910 or via phone 671-475-0400

Accountability

1. The audit log of queries made to the MRFC will identify the user initiating the query.

2. The MRFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of Five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. The annually will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, to not establish a pattern of the audits. These audits will be mandated at least semiannually, and a record of the audits will be maintained by the [Privacy Officer or title of designee] of the center. Audits may be completed by an independent third party or a designated representative of the [name of entity].

Optional: The MRFC will provide an overview of audit findings to the public to enhance transparency with respect to privacy, civil rights, and civil liberties protections built into the [name of center]'s operations.

4. The MRFC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer

5. The MRFC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s) and may include any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related MRFC activity.

The audit will be conducted by the center's director, the privacy office and or their designee. This center's director, the privacy office and or their designee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

6. The MRFC's privacy committee, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

Enforcement

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the MRFC Director will:

- Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
- Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.
- Apply administrative actions or sanctions as provided by MRFC rules and regulations or as provided in agency/center personnel policies.
- If the authorized user is from an agency external to the agency/center, request that the user's employer enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The MRFC 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 P/CRCL policy.

O. Training

1. The MRFC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy

- All center personnel.
- Participating agency personnel
- Personnel providing information technology services to the center.
- Staff members in other public agencies or private contractors providing services to the center.
- Authorized users who are not employed by the center or a contractor.

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

3. The MRFC's P/CRCL policy training program will cover:

- Purposes of the P/CRCL 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.
- Originating and participating agency responsibilities and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user
- . • The potential impact of violations of the agency's P/CRCL policy.
- Mechanisms for reporting violations of center P/CRCL protection policies and procedures.
- How to identify, report, and respond to a suspected or confirmed breach of PII.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.
- Updates to the P/CRCL policy, if any, in response to changes in law and implementation experience. (Refer to Governance and Oversight section for details)
- ISE Core Awareness Training, available at ise.gov.

Best Practice Sample Language:

Subject to course availability, the Privacy Officer of the MRFC will also take courses offered by the U.S. Department of Homeland Security addressing:

- P/CRCL training of trainers.
- Derivative classification marking.