Minnesota Fusion Center
Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy

Version: 02/03/2025	Document Number: INV-7047	Distribution: INV

Applicable CALEA Standards:

40.2.3

Policy Statement/Objective:

The Minnesota Fusion Center (MNFC) operates as the only Governor approved and U.S. Department of Homeland Security (DHS) recognized fusion center for the State of Minnesota. The objective of the MNFC is to serve as a mechanism through which government, law enforcement, public safety, and private sector entities can unite to protect the homeland through the efficient and appropriate sharing of information. The MNFC's mission is to collect, evaluate, analyze, and disseminate information regarding criminal, terrorist, and all-hazards activity in Minnesota, while complying with state and federal laws to ensure the rights and privacy of all.

Definitions:

All-hazards – An all-hazards approach refers to preparedness for terrorist attacks, major disasters, and other emergencies within the United States. Within the context of the fusion process, some fusion centers have defined their mission to include an all-hazards approach. While the application of the all-hazards approach varies, it generally means the fusion center has identified and prioritized types of major disasters and emergencies beyond terrorism and crime that could occur within their jurisdiction. For this approach, fusion centers also gather, analyze, and disseminate information that would assist the relevant responsible agencies (e.g., law enforcement, fire, public health, emergency management, critical infrastructure, etc.) with the prevention, protection, response, or recovery efforts of those incidents.

Participating agency personnel – Refers to individuals who provide on-going support to the fusion center, but are not employed by the Bureau of Criminal Apprehension.

Publicly available information – Information that is available to any member of the general public.

Information-originating agency – The department, agency, or entity that creates, develops, publishes, or issues information.

Personally identifiable information (PII) – Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number, or other identifying number or code, telephone number, email address, etc.); or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.) Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic, or other media.

Non-criminal identifying information – Information that does not meet the reasonable suspicion requirement but is relevant to the identification of the criminal subject or the criminal activity the subject is engaged.

National Network of Fusion Centers (NNFC) – The hub of much of the two-way intelligence and information flow between the federal government and our State, Local, Tribal, Territorial (SLTT) and private sector partners. The fusion centers represent a shared commitment between the federal government and the state and local governments who own and operate them. Individually, each is a vital resource for integrating information from national and local sources to prevent and respond to all threats and hazards.

Need-to-know – A determination by an information-originating agency that a prospective recipient requires access to specific information to carry out official duties or to assist in lawful and authorized governmental functions.

Policy:

The MNFC Privacy/Civil Rights and Civil Liberties (P/CRCL) Policy, herein referred to as the P/CRCL Policy, establishes authoritative guidelines which are applicable to all MNFC personnel and authorized participating agency personnel. The P/CRCL policy will outline the authoritative guidelines and legal requirements regarding the collection, handling, storage, access, dissemination, retention, archiving, and purging of information. Furthermore, the policy will also address the guidelines regarding the disclosure of information in response to requests under the Freedom of Information Act (FOIA) and the Minnesota Government Data Practices Act (MGDPA).

The P/CRCL policy is provided to new MNFC employees to review and acknowledge via the Department of Public Safety policy management application during their first two weeks of employment. Employment is contingent on the acceptance of the policy. Participating agency personnel are provided a digital version of the P/CRCL policy following their initial assignment to the MNFC and required to review and acknowledge the policy. An annual review of the P/CRCL policy will occur.

Roles and Responsibilities:

I. POLICY APPLICABILITY AND LEGAL COMPLIANCE

MNFC and authorized participating agency personnel with direct access to modify MNFC records are required to abide by this P/CRCL Policy. These individuals and any other recipient of MNFC information must also follow all applicable laws which govern the treatment of the information, the MNFC collects, receives, maintains, archives, accesses, discloses, or disseminates.

The MNFC operates within the following statutory codes:

- 28 CFR Part 23: Criminal Intelligence Systems Operating Policies
- Executive Order 22-20: Directing State Agencies to Implement Cybersecurity Measures to Protect Critical Infrastructure in Minnesota
- Information Sharing Environment Functional Standard - Suspicious Activity Reporting (SAR) 1.5.5
- Federal Resource Allocation Criteria (RAC) policy
- 6 U.S.C. 482: Facilitating homeland security information sharing procedures

II. GOVERNANCE AND OVERSIGHT

The MNFC is a unit within the Criminal Information Operations Section (CIOS) of the Investigative Services Division of the Minnesota Bureau of Criminal Apprehension (BCA). Administrative and operational oversight of the CIOS is administered by the identified Special Agent in Charge (SAIC). This individual is also designated as the Director of the Minnesota Fusion Center (Director). The Director may be supported by a designated Deputy Director of the Minnesota Fusion Center. Oversight of the

Investigative Services Division is provided by the Deputy Superintendent of Investigations who reports directly to the Superintendent of the BCA.

The Director will designate an individual to serve as the MNFC Privacy Officer. As of this version of the P/CRCL Policy, the Director has designated the MNFC operations manager as the P/CRCL Officer. The P/CRCL Officer will adhere to the P/CRCL best practices as identified by the DHS Privacy Office and the Office for Civil Rights and Civil Liberties. The statutory and regulatory standards addressed in this training include but may not be limited to 28 Code of Federal Regulations (CFR) Part 23 and Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5. The MNFC Privacy Officer is responsible for information privacy issues, including implementation of P/CRCL Policy requirements.

The MNFC Privacy Officer manages inquiries alleging information errors, complaints, or privacy policy violations. The MNFC Privacy Officer will coordinate conflict resolution under MNFC's redress policy and enforcement and sanctions.

The Privacy Officer can be contacted at: MNFC.PrivacyOfficer@state.mn.us.

The MNFC Director, Deputy Director, and Privacy Officer, will designate a privacy oversight committee comprised of BCA and MNFC personnel. This committee will conduct an annual review and, if needed, update the privacy policy. The annual legislative audit will include confirmation of the annual P/CRCL policy review.

III. INFORMATION

A. Collection Requirements

The MNFC handles public safety and all-hazards information originating from international law enforcement agencies, U.S. Federal, State, Local, Tribal, and Territorial (F-SLTT) agencies, critical infrastructure sector agencies, and publicly available information. Additionally, the MNFC may receive information directly from the public via publicly available reporting methods.

All information handled by the MNFC:

1. **Is relevant to a lawful investigation or prosecution of an individual(s) or organization suspected of being involved in the support, planning, or commission of criminal- or terrorism-related conduct or activity**

   OR

2. Meets the ISE-SAR Functional Standards identifying pre-operational behaviors that are criminal in nature and have historically been associated with terrorism

   OR

3. Is lawfully obtained and will develop or further the understanding and analysis of threats posed to Minnesota

   AND

4. Meets the standards of Information Quality (*refer to Section V*) or limitations to such have been identified

   AND

5. Was obtained in accordance to F-SLTT laws and regulations

The MNFC and authorized participating agency personnel will not directly or indirectly research, collect, request, 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 noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations. It is also assumed that information-originating agencies will agree not to submit information based solely on the aforementioned criteria. Such information will only be sought, collected, and retained if it is:

1. Relevant to whether an individual or organization has engaged in, is engaging in, or is planning criminal or terrorist activity

   OR

2. Relevant to ongoing law enforcement investigations or all-hazards related situations

   OR

3. Needed by the MNFC or partner agencies to identify an individual or to provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

B. Categorization of Information within a Records Management System (RMS)

The MNFC routinely receives requests for information, threat to life reports, or submissions of suspicious activity, from international law enforcement agencies, U.S. F-SLTT agencies, critical infrastructure agencies, and the public. Upon receipt of this information, MNFC personnel will determine if it is a lawful request and/or submission. If the submission is determined to be lawful, MNFC personnel will categorize the information as a Request for Information (RFI), Threat to Life (TTL), Terrorist Screening Center Alert (TSC), or a Suspicious Activity Report (SAR).

1. RFIs must meet criteria i., iii., iv., and v. as outlined in Section III, Part A. Additionally, the originating agency must also:
   - Name the original requestor and requesting agency;
   - Clearly define the criminal predicate; and
   - Clearly articulate what exactly is being asked.
2. TTL notifications refer to an initiative created by the Federal Bureau of Investigation (FBI) to provide a mechanism through which imminent or potential threats involving the risk of death or serious physical injury to any person can be shared. TTLs involve:
   - A threat to kill or seriously injure others
   - A threat to kill or seriously injure oneself
3. TSC alerts originate from the FBI's Terrorist Screen Center (TSC), which maintains the U.S. government's consolidated Terrorist Watchlist. This is a single database of personally identifying information (PII) about individuals known or reasonably suspected of being involved in terrorist or transnational criminal activity. MNFC personnel do not have access to the actual database.
4. Suspicious Activity Report (SAR)
   a. Must meet one of the criteria of the Nationwide Suspicious Activity Reporting Initiative standards.

      OR

   b. Meet an MNFC established SAR standard which may include non-criminal behavior.

      AND

   c. Adhere to the MNFC retention policy.

Information which is lawfully obtained and will develop or further the understanding and analysis of threats posed to Minnesota, may be stored in the same RMS. The information will also include the name of the submitting agency; 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. Retention of this information will follow the MNFC Retention Policy.

Information originally received as an RFI, TTL, TSC, or SAR may be re-evaluated and transitioned to analytical information if it is deemed by appropriate supervisory personnel that it will further the understanding and analysis of threats posed to Minnesota. The P/CRCL Officer will review this information and, when possible, remove all personally identifiable information (PII) and noncriminal identifying information (NCII) which is no longer required to maintain the relevance of the information.

Information storage and retention guidelines may change for records if/when new information is received. Additionally, record information may be used to support analytical products. In these instances all personally identifiable information shall be removed.

Access to the RMS is limited to MNFC personnel and only to those authorized participating agency personnel who have received additional training on the proper handling of criminal justice information and intelligence information.

IV. ACQUIRING AND RECEIVING INFORMATION

Any information gathered by MNFC or authorized participating agency personnel will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

- 28 CFR Part 23;
- The National Criminal Intelligence Sharing Plan (NCISP);
- The Constitution of the United States and the Minnesota Constitution Article I (Bill of Rights);
- Minnesota Government Data Practices Act (MGDPA), Minn. Stat. § 13.01 et seq.;
- Minnesota Health Records Act, Minn. Stat. § 144.293, subd. 2 (Release or Disclosure of Health Records);
- As well as any other regulations that apply to multijurisdictional intelligence and information databases.

MNFC and authorized participating agency personnel will only gather publicly available information or, when appropriate, information originating from a state or federally-approved criminal justice information system. Authorized participating agency personnel who are given access to modify MNFC records are required to adhere to the information gathering practices mentioned above. External agencies that receive any products disseminated by the MNFC are expected to understand and adhere to the applicable federal and state laws regarding receiving, sharing, and use of sensitive, criminal justice information.

The MNFC may contract with external third-party vendors to develop and maintain the technical infrastructure of record management, communication, or information dissemination platforms. These vendors are required to submit to a cybersecurity audit conducted by BCA's information technology section. The MNFC shall only utilize a third-party vendor if these standards are met.

The MNFC will only utilize third-party commercial vendors that aggregate publicly available information, which may include personally identifiable information (PII).

MNFC and authorized participating agency personnel will not employ any cyber-intrusion methodologies to obtain information. Additionally, MNFC personnel will not covertly interact or engage with any

individual, group, or organization.

V. INFORMATION QUALITY ASSURANCE

The MNFC is required by Minn. Stat. §13.05, subd. 5 to assure that data are accurate, complete, current, and secure. MNFC personnel will take all reasonable steps to ensure the information obtained is legally gathered. Information quality will also be assessed through database searches, cross-checks with other data systems and open source information. Additionally, these checks will utilize the least intrusive feasible means, taking into account the effect on individual privacy.

VI. COLLATION AND ANALYSIS

Information within the MNFC RMS may be used toward the production of analytical products only if PII is removed. Additionally, utilizing this information for analysis may only be done by MNFC personnel and participating agency personnel who have completed basic analytical tradecraft training provided by the FBI, DHS, National Fusion Center Association (NFCA), National White Collar Crime Center (NW3C), or similar nationally recognized program. Non-analytical products, such as officer safety alerts, may contain PII.

On occasion, other fusion centers operating within the National Network of Fusion Centers may request Minnesota-specific information to utilize in the production of their products. This information may be shared if the request is reviewed and approved by the MNFC Privacy Officer and appropriate supervisors. Shared information must have PII removed.

The MNFC requires that all analytical products be reviewed to ensure that the appropriate privacy, civil rights, and civil liberties protections are met prior to dissemination or sharing by the MNFC.

VII. MERGING RECORDS

During the record entry process, it may be determined that multiple entries for an individual exist. If multiple records are identified these may be merged when unique identifiers, such as Minnesota State ID number, driver's license number, social security number, etc., are matching.

VIII. SHARING AND DISSEMINATION: Use of Information by the MNFC

Information obtained from or through the MNFC can only be used for official and lawful purposes. A lawful purpose means the Request for Information (RFI) can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety.

Access to or disclosure of records retained by the MNFC will be provided only to persons authorized to have access, and only for legitimate law enforcement or public safety purposes necessary for the performance of official duties. Recipients of MNFC products will be vetted annually to verify their continued a need-to-know.

The MNFC reserves the right to deny access to any MNFC user who fails to comply with the applicable restrictions and limitations.

The MNFC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting process, as that is defined in this policy as an ISE- SAR.

IX. REDRESS: Disclosure of Information Outside of the MNFC

No briefs or assessments can be disseminated outside of the MNFC unless reviewed and approved for dissemination by the MNFC Operations Manager, the MNFC Director, or a designee. When reviewing

briefs and assessments, particular attention will be focused on content, classification, and compliance with this policy. All attached documents will have the permission of the originating agency for use prior to inclusion in the brief or assessment, and dissemination will be limited to individuals with a verified need-to-know.

- *Disclosure to a Data Subject:*

  An individual who is the subject of data at the MNFC has a number of rights designated in Minn. Stat. §13.04, subd. 3. Those rights include the right to know data exists, to inspect the data at the MNFC, to have copies of the data, and to have the meaning of the data explained. When data is classified as private, the MNFC must verify the identity of the individual using one of the identification methods specified in the BCA's data practices policies and procedures. The MNFC must respond to an individual data subject within ten (10) working days of receipt of a data request for data about that individual. All data requests must be submitted to the BCA's Data Practices Division. More information can be found in BCA's Data Access Policy and Inventory.

- *Disclosure to the Public:*

  The public has the right to access public data maintained at the MNFC. See Minn. Stat. §13.03, subd. 3. The rights granted by section 13.03 include the right to inspect, to have copies, and to have the meaning of the data explained. The MNFC is required to respond in an amount of time that is appropriate, prompt, and reasonable. See Minn. Stat. §13.03, subd. 2(a) and Minn. Rules 1205.9300, subp. 3.

  All media requests shall be forwarded to the Director for referral to the BCA's Public Information Officer.

- *Corrections:*

  An individual data subject is authorized by Minn. Stat. §13.04, subd. 4 to challenge the accuracy and/or completeness of public or private data. The terms "accuracy" and "completeness" are defined in Minn. Rules 1205.1500, subp. 2. Section 13.04, subd. 4, requires any challenge to the accuracy or completeness of data to be made to the "responsible authority." MNFC's responsible authority is the Commissioner of the Department of Public Safety. Minn. Rules 1205.0200, subp. 13.

  The Commissioner of Public Safety has thirty (30) days to respond to a data challenge and either change the data or indicate that the data are accurate or complete. If the individual data subject does not agree with the Commissioner's determination, the individual has the right to appeal the determination to the Commissioner of Administration. The appeal process is described in Minn. Rules 1205.1600. A record will be kept of all requests for corrections and the resulting action, if any.

Information gathered or collected and records retained by MNFC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed without prior notice to the originating agency unless disclosure is required by law.
- Disclosed to persons not authorized to access or use the information.

The MNFC 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.

X. SECURITY SAFEGUARDS

The MNFC is located within a secure area of the BCA, a public safety agency with appropriate physical safety measure and access restrictions. This provides adequate physical security safeguards for

information managed by the MNFC. The record management system utilized by BCA meets the Criminal Justice Information data storage requirements.

The Superintendent, the MNFC Director, or their designee, will identify the technical resources to establish a secure facility for MNFC operations with restricted access, security cameras, and alarm systems to guard against an external breach of the facility. In addition, the Superintendent or their designee will identify the technological support for secure internal and external safeguards against network intrusion of MNFC information systems.

Access to the MNFC database from outside of the facility will only be allowed over secure network lines.

MNFC information will be maintained in so that it cannot be stored, modified, destroyed, accessed, or purged without prior authorization.

Access to MNFC 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.

Classified information will only be stored on electronic systems or in a safe explicitly approved for classified processing or storage by the U.S. Department of Homeland Security, the FBI, or DPS/BCA as appropriate to the system or information.

SAR information will be stored in the same system as that for all other data, but will be clearly labeled as to its record-type when disclosed. This system is compliant with 28 CFR Part 23 security requirements.

All MNFC documents or software will be stored on MNFC computer systems or storage devices and in compliance with DPS/BCA policies. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publically available information.

Minnesota law requires that if a breach of the security of private or confidential data occurs, the state agency that maintains the data must notify the individuals whose data were disclosed. Methods of notice are provided for in the statute along with the ability, in the appropriate circumstances, to delay notification to permit an active criminal investigation to occur without impediment. Minn. Stat. §13.055.

XI. INFORMATION RETENTION AND DESTRUCTION

The Minnesota Records Management Act, Minn. Stat. §138.17, requires that an approved records retention schedule be in place before records can be destroyed. An approved records retention schedule for MNFC records is in place and authorizes the destruction of certain records. The retention period varies by record series type. For any records series not on the approved records retention schedule, approval is required prior to destruction. That approval could be in the form of a new approved records retention schedule or a one-time permission. The MNFC will make its approved records retention schedule available for public review, including posting it on the BCA public website: https://s3.us-east-2.amazonaws.com/assets.dps.mn.gov/s3fs-public/Minnesota-Fusion-Center-Retension-Schedule.pdf.

A list of records disposed of pursuant to the approved records retention schedule shall be maintained by the MNFC. Minn. Stat. §138.17, subd. 7. When records containing non-public data as defined in the Minnesota Government Data Practices Act are being disposed of pursuant to the approved records retention schedule, the records must be destroyed in a way that prevents their contents from being determined. Minn. Stat. § 13.02, subd. 8a.

XII. ACCOUNTABILITY AND ENFORCEMENT

The MNFC will make this Privacy, Civil Rights, and Civil Liberties Policy available for public review, including posting it on the BCA public website: https://dps.mn.gov/divisions/bca/bca-

divisions/investigations/Pages/MNFC.aspx.

The MNFC Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system. The Privacy Officer can be contacted at the following address: MNFC.PrivacyOfficer@state.mn.us.

Individual users of MNFC information remain responsible for the appropriate use of MNFC information. Each user of the MNFC and each participating agency within the MNFC are required to abide by this Privacy, Civil Rights, and Civil Liberties Policy. Failure to abide by the restrictions for the use of the MNFC information may result in the suspension or termination of user privileges; discipline imposed by the user's employing agency, or criminal prosecution.

XIII. TRAINING

All staff members assigned to the MNFC from participating agencies are required to complete annual MNFC P/CRCL Policy training conducted or provided by the MNFC Privacy Officer.

The MNFC's Privacy Policy training program will cover:

- Purposes of the privacy policy
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR and ISE-SAR information maintained or submitted by the MNFC to the shared spaces
- How to implement the policy in the day-to-day work of a Participating Agency
- The impact of improper activities associated with violations of the policy
- Mechanisms for reporting violations of the policy
- The possible penalties for policy violations, including transfer, dismissal, and criminal liability, if any
- Special training to personnel authorized to share Protected Information through the ISE regarding the center's requirements and policies for collection, use, and disclosure of Protected Information

References:

LIST OF APPLICABLE STATUTES

The following is a list of legal provisions that affect the operations of the Minnesota Fusion Center (MNFC), the classification of data it holds, and how access and dissemination of that data occurs.

Federal Provisions

United States Constitution, including the **Bill of Rights**

Brady Handgun Violence Prevention Act, Public Law 103-159; 18 U.S.C. §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, Public Law 100-503; 5 U.S.C. § 552a, subd. (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

Crime Identification Technology, 34 U.S.C. § 40301

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, et seq.

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23

Criminal Justice Information Systems, 28 CFR Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682

Electronic Communications Privacy Act of 1986, Public Law 99-508; 18 U.S.C. §§ 2510–2522, 2701– 2709

Facilitating Homeland Security Information Sharing Procedures, 6 U.S.C. § 482

Fair Credit Reporting Act, 15 U.S.C. § 1681

Federal Civil Rights laws, including The Enforcement Act of 1871 (42 U.S.C. § 1983) and The Civil Rights Act of 1964

Federal Records Act, 44 U.S.C. § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552

Indian Civil Rights Act of 1968, 25 U.S.C. §ë 1301-1303

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, and as amended by the 9/11 Commission Act, Public Law 110-53

National Child Protection Act of 1993, Public Law 103-209, 42 U.S.C. § 5119 et seq.

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616

Privacy Act of 1974, 5 U.S.C. § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313

Protection of Human Subjects, 28 CFR Part 46

Safeguarding Customer Information, 16 CFR Part 314

Sarbanes-Oxley Act of 2002, Public Law 107-204, 15 U.S.C. § 7201

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

Minnesota Provisions

Minnesota Constitution

Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13, and enabling rules found in Minnesota Rules, Chapter 1205

Official Records Act, Minnesota Statutes § 15.17

Records Management Act, Minnesota Statutes §138.163, et seq.

Minnesota Health Records Act, Minnesota Statutes § 144.291, et seq.

Minnesota Statutes, Chapter 243 – Corrections

Minnesota Statutes, Chapter 260B – Delinquency

Minnesota Statutes, Chapter 299C – Bureau of Criminal Apprehension

Minnesota Statutes, Chapters 609-643 – Provisions related to crimes and offenses, rehabilitation, and incarceration