

**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**  
 Reference document: Secure Controls Framework (SCF) version 2026.1  
 STRM Guidance: <https://securecontrolsframework.com/set-theory-relationship-mapping-strm/>

**Focal Document: Criminal Justice Information Services (CJIS) Security Policy (v6.0)**  
 Focal Document URL: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>  
 Published STRM URL: <https://content.securecontrolsframework.com/strmscf-strm-usa-federal-fbi-cjis-6-0.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.1	Criminal Justice Information (CJ)	Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric identity history, biographic, property, and case/incident history data. The following categories of CJ describe the various data sets housed by the FBI CJIS architecture: 1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data. 2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual. 3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. 4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII). 5. Case/Incident History—information about the history of criminal incidents. The following type of data are exempt from the protection levels required for CJ: transaction control type numbers (e.g., ORI, NIC, JCN, etc.) when not accompanied by information that reveals CJ or PI. The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJ until the information is released to the public via authorized dissemination (e.g., within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJ introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1.1	Criminal History Record Information (CHRI)	Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJ. Due to its comparatively sensitive nature, additional controls are required for the access, use, and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
4.1.1	Criminal History Record Information (CHRI)	Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJ. Due to its comparatively sensitive nature, additional controls are required for the access, use, and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
4.2	Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information	This section describes the requirements for the access, use, and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.2.1	Proper Access, Use, and Dissemination of CHRI	Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
4.2.1	Proper Access, Use, and Dissemination of CHRI	Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows: 1. Gang Files 2. Threat Screening Center Files 3. Supervised Release Files 4. National Sex Offender Registry Files 5. Historical Protection Order Files of the NCIC 6. Identity Theft Files 7. Protective Interest Files 8. Person With Information (PWI) data in the Missing Person Files 9. Violent Person File 10. NICS Denied Transactions File The remaining NCIC files are considered non-restricted files.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows: 1. Gang Files 2. Threat Screening Center Files 3. Supervised Release Files 4. National Sex Offender Registry Files 5. Historical Protection Order Files of the NCIC 6. Identity Theft Files 7. Protective Interest Files 8. Person With Information (PWI) data in the Missing Person Files 9. Violent Person File 10. NICS Denied Transactions File The remaining NCIC files are considered non-restricted files.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows: 1. Gang Files 2. Threat Screening Center Files 3. Supervised Release Files 4. National Sex Offender Registry Files 5. Historical Protection Order Files of the NCIC 6. Identity Theft Files 7. Protective Interest Files 8. Person With Information (PWI) data in the Missing Person Files 9. Violent Person File 10. NICS Denied Transactions File The remaining NCIC files are considered non-restricted files.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows: 1. Gang Files 2. Threat Screening Center Files 3. Supervised Release Files 4. National Sex Offender Registry Files 5. Historical Protection Order Files of the NCIC 6. Identity Theft Files 7. Protective Interest Files 8. Person With Information (PWI) data in the Missing Person Files 9. Violent Person File 10. NICS Denied Transactions File The remaining NCIC files are considered non-restricted files.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 30, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows: 1. Gang Files 2. Threat Screening Center Files 3. Supervised Release Files 4. National Sex Offender Registry Files 5. Historical Protection Order Files of the NCIC 6. Identity Theft Files 7. Protective Interest Files 8. Person With Information (PWI) data in the Missing Person Files 9. Violent Person File 10. NICS Denied Transactions File The remaining NCIC files are considered non-restricted files.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	5	
4.2.3	Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.2.3.1	For Official Purposes	NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
4.2.3.1	For Official Purposes	NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
4.2.3.1	For Official Purposes	NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
4.2.3.1	For Official Purposes	NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	5	
4.2.3.2	For Other Authorized Purposes	NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially. A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
4.2.3.2	For Other Authorized Purposes	NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially. A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
4.2.3.2	For Other Authorized Purposes	NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially. A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	5	
4.2.3.3	CSO Authority in Other Circumstances	If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted files information.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
4.2.3.3	CSO Authority in Other Circumstances	If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted files information.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	5	
4.2.4	Storage	When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key evidence for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
4.2.5	Justification and Penalties	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.2.5.1	Justification	In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.2.5.2	Penalties	Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.3	Personally Identifiable Information (PI)	For the purposes of this document, PI is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PI. A criminal history record for example inherently contains PI as would a Law Enforcement National Data Exchange (N-DEX) case file. PI shall be extracted from CJ for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PI extracted from CJ. Due to the expansive nature of PI, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PI.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
4.3	Personally Identifiable Information (PI)	For the purposes of this document, PI is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PI. A criminal history record for example inherently contains PI as would a Law Enforcement National Data Exchange (N-DEX) case file. PI shall be extracted from CJ for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PI extracted from CJ. Due to the expansive nature of PI, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PI.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.3	Personally Identifiable Information (PII)	For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEX) case file. PII shall be extracted from CJ for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJ. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
4.3	Personally Identifiable Information (PII)	For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEX) case file. PII shall be extracted from CJ for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJ. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
4.3	Personally Identifiable Information (PII)	For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEX) case file. PII shall be extracted from CJ for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJ. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	5	
5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRPR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1.1	Information Exchange	Before exchanging CJ, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJ. Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJ data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document. Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
5.1.1	Information Exchange	Before exchanging CJ, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJ. Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJ data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document. Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRPR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1.2	Monitoring, Review, and Delivery of Services	As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	