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

Focal Document: **Illinois Biometric Information Privacy Act (BIPA) (2008)**
Focal Document URL: https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-il-bipa-2008.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
1	Short title	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5	Legislative findings; intent	The General Assembly finds all of the following:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(a)	Legislative findings; intent	The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(b)	Legislative findings; intent	Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(c)	Legislative findings; intent	Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(d)	Legislative findings; intent	An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(e)	Legislative findings; intent	Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(f)	Legislative findings; intent	The full ramifications of biometric technology are not fully known.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5(g)	Legislative findings; intent	The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15	Retention; collection; disclosure; destruction	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15(a)	Retention; collection; disclosure; destruction	A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
15(a)	Retention; collection; disclosure; destruction	A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.	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	
15(b)	Retention; collection; disclosure; destruction	No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15(b)(1)	Retention; collection; disclosure; destruction	informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
15(b)(2)	Retention; collection; disclosure; destruction	informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
15(b)(3)	Retention; collection; disclosure; destruction	receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
15(c)	Retention; collection; disclosure; destruction	No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.	Functional	Intersects With	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-03.3	Mechanisms exist to prevent the sale, processing and/or sharing of Personal Data (PD) when:(1) Instructed by the data subject; or(2) The data subject is a minor, where selling and/or sharing PD is legally prohibited.	5	
15(d)	Retention; collection; disclosure; destruction	No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
15(d)(1)	Retention; collection; disclosure; destruction	the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
15(d)(2)	Retention; collection; disclosure; destruction	the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
15(d)(3)	Retention; collection; disclosure; destruction	the disclosure or redisclosure is required by State or federal law or municipal ordinance; or	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
15(d)(4)	Retention; collection; disclosure; destruction	the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
15(e)	Retention; collection; disclosure; destruction	A private entity in possession of a biometric identifier or biometric information shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

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
15(e)(1)	Retention; collection; disclosure; destruction	store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
15(e)(1)	Retention; collection; disclosure; destruction	store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
15(e)(2)	Retention; collection; disclosure; destruction	store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
15(e)(2)	Retention; collection; disclosure; destruction	store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
20	Right of action	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(a)	Right of action	Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(a)(1)	Right of action	against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(a)(2)	Right of action	against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(a)(3)	Right of action	reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(a)(4)	Right of action	other relief, including an injunction, as the State or federal court may deem appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(b)	Right of action	For purposes of subsection (b) of Section 15, a private entity that, in more than one instance, collects, captures, purchases, receives through trade, or otherwise obtains the same biometric identifier or biometric information from the same person using the same method of collection in violation of subsection (b) of Section 15 has committed a single violation of subsection (b) of Section 15 for which the aggrieved person is entitled to, at most, one recovery under this Section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20(c)	Right of action	For purposes of subsection (d) of Section 15, a private entity that, in more than one instance, discloses, rediscloses, or otherwise disseminates the same biometric identifier or biometric information from the same person to the same recipient using the same method of collection in violation of subsection (d) of Section 15 has committed a single violation of subsection (d) of Section 15 for which the aggrieved person is entitled to, at most, one recovery under this Section regardless of the number of times the private entity disclosed, redisclosed, or otherwise disseminated the same biometric identifier or biometric information of the same person to the same recipient.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25	Construction	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25(a)	Construction	Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25(b)	Construction	Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25(c)	Construction	Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25(d)	Construction	Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25(e)	Construction	Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
30	(Repealed)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
99	Effective date	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control