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 Identity Protection Act (IPA) (2009)**
Focal Document URL: https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3174&ChapterID=2
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-il-ipa-2009.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	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10	Prohibited activities	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10(a)	Prohibited activities	Beginning July 1, 2010, no person or State or local government agency may do any of the following:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10(a)(1)	Prohibited activities	Publicly post or publicly display in any manner an individual's social security number.	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(a)(2)	Prohibited activities	Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity.	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(a)(3)	Prohibited activities	Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.	Functional	Subset Of	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.	10	
10(a)(4)	Prohibited activities	print an individual's social security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act pursuant to the limitations and requirements of that Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(b)	Prohibited activities	Except as otherwise provided in this Act, beginning July 1, 2010, no person or State or local government agency may do any of the following:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10(b)(1)	Prohibited activities	Collect, use, or disclose a social security number from an individual, unless (i) required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the social security number is documented before collection of the social security number; and (iii) the social security number collected is relevant to the documented need and purpose.	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
10(b)(1)	Prohibited activities	Collect, use, or disclose a social security number from an individual, unless (i) required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the social security number is documented before collection of the social security number; and (iii) the social security number collected is relevant to the documented need and purpose.	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
10(b)(1)	Prohibited activities	Collect, use, or disclose a social security number from an individual, unless (i) required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the social security number is documented before collection of the social security number; and (iii) the social security number collected is relevant to the documented need and purpose.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	5	
10(b)(2)	Prohibited activities	Require an individual to use his or her social security number to access an Internet website.	Functional	Subset Of	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.	10	
10(b)(3)	Prohibited activities	Use the social security number for any purpose other than the purpose for which it was collected.	Functional	Subset Of	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.	10	
10(c)	Prohibited activities	The prohibitions in subsection (b) do not apply in the following circumstances:	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(c)(1)	Prohibited activities	The disclosure of social security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's social security number will be achieved.	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(c)(2)	Prohibited activities	The disclosure of social security numbers pursuant to a court order, warrant, or subpoena.	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(c)(3)	Prohibited activities	The collection, use, or disclosure of social security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; youth in care as defined in Section 4d of the Children and Family Services Act, and all persons working in or visiting a State or local government agency facility.	Functional	Subset Of	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.	10	
10(c)(4)	Prohibited activities	The collection, use, or disclosure of social security numbers for internal verification or administrative purposes.	Functional	Subset Of	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.	10	
10(c)(5)	Prohibited activities	The disclosure of social security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
10(c)(6)	Prohibited activities	The collection or use of social security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm-Leach-Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.	Functional	Subset Of	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.	10	
10(d)	Prohibited activities	If any State or local government agency has adopted standards for the collection, use, or disclosure of social security numbers that are stricter than the standards under this Act with respect to the protection of those social security numbers, then, in the event of any conflict with the provisions of this Act, the stricter standards adopted by the State or local government agency shall control.	Functional	Subset Of	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.	10	
15	Public inspection and copying of documents	Notwithstanding any other provision of this Act to the contrary, a person or State or local government agency must comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's social security number. A person or State or local government agency must redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.	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	
20	Applicability	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25	Compliance with federal law	If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, any State or local government agency that complies with the federal law shall be deemed to be in compliance with this Act.	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	
30	Embedded social security numbers	Beginning December 31, 2009, no person or State or local government agency may encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology, or other technology, in place of removing the social security number as required by this Act.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
35	Identity-protection policy; local government	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
35(a)	Identity-protection policy; local government	Each local government agency must draft and approve an identity-protection policy within 12 months after the effective date of this Act. The policy must do all of the following:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
35(a)(1)	Identity-protection policy; local government	Identify this Act.	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	
35(a)(2)	Identity-protection policy; local government	Require all employees of the local government agency identified as having access to social security numbers in the course of performing their duties to be trained to protect the confidentiality of social security numbers. Training should include instructions on the proper handling of information that contains social security numbers from the time of collection through the destruction of the information.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
35(a)(3)	Identity-protection policy; local government	Direct that only employees who are required to use or handle information or documents that contain social security numbers have access to such information or documents.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
35(a)(4)	Identity-protection policy; local government	Require that social security numbers requested from an individual be provided in a manner that makes the social security number easily redacted if required to be released as part of a public records request.	Functional	Intersects With	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive/regulated information that is displayed or printed.	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
35(a)(5)	Identity-protection policy; local government	Require that, when collecting a social security number or upon request by the individual, a statement of the purpose or purposes for which the agency is collecting and using the social security number be provided.	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	
35(b)	Identity-protection policy; local government	Each local government agency must file a written copy of its privacy policy with the governing board of the unit of local government within 30 days after approval of the policy. Each local government agency must advise its employees of the existence of the policy and make a copy of the policy available to each of its employees, and must also make its privacy policy available to any member of the public, upon request. If a local government agency amends its privacy policy, then that agency must file a written copy of the amended policy with the appropriate entity and must also advise its employees of the existence of the amended policy and make a copy of the amended policy available to each of its employees.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3	
35(c)	Identity-protection policy; local government	Each local government agency must implement the components of its identity-protection policy that are necessary to meet the requirements of this Act within 12 months after the date the identity-protection policy is approved. This subsection (c) shall not affect the requirements of Section 10 of this Act.	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
37	Identity-protection policy; State	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
37(a)	Identity-protection policy; State	Each State agency must draft and approve an identity-protection policy within 12 months after the effective date of this Act. The policy must do all of the following:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
37(a)(1)	Identity-protection policy; State	Identify this Act.	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	
37(a)(2)	Identity-protection policy; State	Require all employees of the State agency identified as having access to social security numbers in the course of performing their duties to be trained to protect the confidentiality of social security numbers. Training should include instructions on proper handling of information that contains social security numbers from the time of collection through the destruction of the information.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
37(a)(3)	Identity-protection policy; State	Direct that only employees who are required to use or handle information or documents that contain social security numbers have access to such information or documents.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
37(a)(4)	Identity-protection policy; State	Require that social security numbers requested from an individual be placed in a manner that makes the social security number easily redacted if required to be released as part of a public records request.	Functional	Intersects With	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive/regulated information that is displayed or printed.	5	
37(a)(5)	Identity-protection policy; State	Require that, when collecting a social security number or upon request by the individual, a statement of the purpose or purposes for which the agency is collecting and using the social security number be provided.	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	
37(b)	Identity-protection policy; State	Each State agency must provide a copy of its identity-protection policy to the Social Security Number Protection Task Force within 30 days after the approval of the policy.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5	
37(c)	Identity-protection policy; State	Each State agency must implement the components of its identity-protection policy that are necessary to meet the requirements of this Act within 12 months after the date the identity-protection policy is approved. This subsection (c) shall not affect the requirements of Section 10 of this Act.	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
40	Judicial branch and clerks of courts	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
45	Violation	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
50	Home rule	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
55	N/A	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
90	(Amendatory provisions; text omitted)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control