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: **California SB327 (2018)**
Focal Document URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-ca-sb327-2018.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
SECTION 1	N/A	Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
TITLE 1.81.26	Security of Connected Devices	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1798.91.04	Security of Connected Devices	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1798.91.04(a)	Security of Connected Devices	A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(a)(1)	Security of Connected Devices	Appropriate to the nature and function of the device.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(a)(2)	Security of Connected Devices	Appropriate to the information it may collect, contain, or transmit.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(a)(3)	Security of Connected Devices	Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(b)	Security of Connected Devices	Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(b)(1)	Security of Connected Devices	The preprogrammed password is unique to each device manufactured.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(b)(1)	Security of Connected Devices	The preprogrammed password is unique to each device manufactured.	Functional	Intersects With	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers:(1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and(2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.	8	
1798.91.04(b)(2)	Security of Connected Devices	The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
1798.91.04(b)(2)	Security of Connected Devices	The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	8	
1798.91.05	Security of Connected Devices	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1798.91.06	Security of Connected Devices	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SEC. 2	N/A	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control