cpl.thalesgroup.com

THALES
Building a future we can all trust

Data Security Compliance with the NAIC Data Security Law

How Thales solutions help with NAIC Compliance

What is the NAIC Data Security Law?

The National Association of Insurance Commissioners (NAIC) Data Security Law (Model Law) requires insurers and other entities licensed by state insurance departments to develop, implement, and maintain an information security program; investigate any cybersecurity events; and notify the state insurance commissioner of such events. The NAIC model law provides a blueprint for state-level laws regulating insurance companies. The main recommendations of the law include:

- Develop a written information security program
- Assign information security responsibility
- Perform periodic risk assessments
- Implement key cyber security safeguards
- Prepare incident response plans and procedures
- Regularly monitor and report on program status
- Implement Service Provider oversight
- Provide Board-level oversight

Which companies are subject to NAIC Data Security Law?

The law applies to licensees of each state insurance bureau. This includes (with some exceptions) insurance industry companies, agencies, agents, public adjusters, and brokers.

When did the NAIC Data Security Law go into effect?

The National Association of Insurance Commissioners officially adopted the Data Security Law in the fourth quarter of 2017. As of May 2023, 22 states have enacted versions of the law: Alabama, Alaska, Connecticut, Delaware, Hawaii, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, New Hampshire, North Dakota, Ohio, South Carolina, Tennessee, Vermont, Virginia, and Wisconsin.

What are the penalties for NAIC Data Security Law non-compliance?

The suggested penalties for non-compliance with the NAIC Data Security Law are up to $500 per violation (subject to a maximum of $10,000). If the insurer/producer violates the commissioner's cease and desist order, suggested penalties are up to $10,000 per violation (subject to a maximum of $50,000). Individuals at those institutions can be fined up to $10,000 for each violation and may also be sentenced to up to five years in prison.

How Thales can help with NAIC Data Security Law compliance?

Thales helps organizations comply with the NAIC Data Security Law by addressing essential requirements for risk management in an organization's NAIC-mandated Information Security Program.

NAIC Data Security Law Section 4. Information Security Program

Licensee shall develop, implement, and maintain an Information Security Program that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.

Thales helps organizations by:

- Reducing third party risk
- Controlling access to sensitive data and information systems
- Identifying and managing sensitive data
- Encrypting data at rest and in motion
- Securing the development of apps
- Implementing multi-factor authentication
- Securing the disposal of non-public information

NAIC	Requirement	Thales Solutions
D. 1	Design its Information Security Program to mitigate the identified risks ... including its use of **Third-Party Service Providers**	**CipherTrust Cloud Key Manager** can reduce third party risks by maintaining on-premises under the full control of the financial institution the keys that protect sensitive data hosted by third party cloud providers. This increases operational efficiency through harmonization and automation. **CipherTrust Transparent Encryption** provides complete separation of administrative roles, so only authorized users and processes can view unencrypted data. Sensitive data stored in a third-party cloud will not be accessible in cleartext to unauthorized users. These could include third party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. In addition, **Thales Portfolio of Data Security** solutions offer the most comprehensive range of data protection, such as **Thales Data Protection on Demand (DPoD)** that provides built in high availability and backup to its cloud-based **Luna Cloud HSM** and **CipherTrust Key Management** services, to the **HSE** network encryption appliances that provides options to zeroize.
Part D. 2, a	**"Place access controls on Information Systems,** ...protect against unauthorized acquisition of Nonpublic Information;"	**Thales OneWelcome** identity & access management products and solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensuring that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access. **Thales OneWelcome Consent & Preference Management** module enables organizations to gather consent of end consumers such that financial institutions may have clear visibility of consented data, thereby allowing them to manage access to data that they are allowed to utilize.

How can Thales help with NAIC compliance?

NAIC	Requirement	Thales Solutions
Part D. 2, a		**CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. The solution provides complete separation of roles where only authorized users and processes can view unencrypted data.
Part D. 2, b	**"Identify and manage the data**...that enable the organization to achieve business purposes..."	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
Part D. 2, d	**"Protect by encryption** or other appropriate means, all **Nonpublic Information while being transmitted** over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or **storage device or media;"**	**Protect Data at Rest:** **CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Tokenization** permits the pseudonymization (and consequently, de-identification) of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports. • **CipherTrust Enterprise Key Management** streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, our key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. **Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. • Generates and protects root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Signs application code to ensure software remains secure, unaltered, and authentic • Creates digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments **Protect Data in Motion:** **Thales High Speed Encryptors (HSEs)** provide network-independent data-in-motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps. Rigorously tested and certified to exacting standards such as FIPS 140-2 L3 and Common Criteria, Thales HSE network encryption solutions have been vetted by such organizations as the USA Department of Defense Information Network (DoDIN) and NATO.

How can Thales help with NAIC compliance?

NAIC	Requirement	Thales Solutions
Part D. 2, e	**"Adopt secure development practices for in-house developed applications..."**	**CipherTrust Platform Community Edition** makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications. The solution includes licenses for CipherTrust Manager Community Edition, Data Protection Gateway, and CipherTrust Transparent Encryption for Kubernetes. **CipherTrust Secrets Management** is a state-of-the-art secrets management solution, which protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens.
Part D. 2, g	"Utilize effective controls, which may include **Multi-Factor Authentication..."**	**SafeNet Trusted Access** provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. This allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies— all managed from one authentication back end delivered in the cloud or on-premises. **SafeNet IDPrime** smart cards can be leveraged for implementing physical access to sensitive facilities. These smart cards can also augment Passwordless authentication initiatives relying on PKI and FIDO technology.
Part D. 2, i	**Include audit trails** within the Information Security Program designed to detect and respond to Cybersecurity Events	The **Thales Data Security Solutions** all maintain extensive access logs and prevent unauthorized access. In particular, **CipherTrust Transparent Encryption** security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and external SIEM systems. In addition, **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** watches for abnormal I/O activity on files hosting business critical data on a per process basis. It allows administrators to alert/block suspicious activity before ransomware can take hold of your endpoints/servers. It defends against ransomware even when the ransomware is installed prior to CTE-RWP. **SafeNet Trusted Access** allows organizations to respond and mitigate the risk of data breach by providing an immediate, up to date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication. In addition, the service automatically streams logs to external SIEM systems.
Part D. 2, k	Develop, implement, and maintain procedures for the **secure disposal of Nonpublic Information in any format.**	**CipherTrust Data Security Platform** encryption and tokenization solutions rely on cryptographic keys to encrypt and decrypt data. This means you can selectively "destroy" data simply by destroying the encryption keys for that data.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us