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 Helps with NAIC Compliance

Thales' solutions can help insurance providers comply with NAIC Data Security Law by simplifying compliance and automating security, reducing the burden on security and compliance teams. We help address essential requirements for risk management in an organization's NAIC-mandated Information Security Program.

We provide comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

NAIC	Thales Capabilities	Thales Solutions
Part D. 1 **"Mitigate risks … of Third-Party Service Providers"**	• Reduce third party risk by maintaining on-premises control over encryption keys protecting data hosted by in the cloud. • Enforce separation of roles between cloud provider admins and your organization, restrict access to sensitive data. • Monitor and alert anomalies to detect and prevent unwanted activities from disrupting supply chain activities. • Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using relationship-based fine-grained authorization.	**Data Security** Cloud Key Management Transparent Encryption Data Activity Monitoring User Rights Management Discovery and Classification **Identity & Access Management** Workforce Access Management Third-party Access Control Delegated User Management Externalized Authorization
Part D. 2, a "Place access controls on Information Systems"	• Limit access to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Centralize access policies and enforcement to multiple hybrid environments in a single pane of glass. • Provide customers secure access to their information in company's systems.	**Identity & Access Management** Workforce Access Management Customer Identity & Access Management **Data Security** Transparent Encryption

NAIC	Thales Capabilities	Thales Solutions
Part D. 2. b "Identify and manage data and systems..."	• Identify structured and unstructured sensitive data at risk across Hybrid IT. • Identify current state of compliance and documenting gaps. • Discover and classify potential risk for all public, private and shadow APIs.	**Application Security** API Security **Data Security** Data Discovery & Classification Data Risk Analytics Vulnerability Management
Part D. 2, d "Protect by encryption ... all Nonpublic Information while being transmitted ... or stored on a laptop computer or other portable computing or storage device or media."	• Encrypt data at rest on-premises, across clouds, and in big data or container environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment. • Pseudonymize sensitive information in databases. • Protect data in motion with high-speed encryption. • Protect data in use by leveraging confidential computing. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document. • Security products designed for post-quantum upgrade to maintain crypto-agility.	**Data Security** Transparent Encryption Tokenization Key & Secrets Management High Speed Encryption Hardware Security Modules Confidential Computing Data Governance Data Activity Monitoring
Part D. 2, e "Adopt secure development practices for in-house developed applications..."	• Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Deploy data protection controls in hybrid and multi-cloud applications to protect DevSecOps. • Protect and automate access to secrets across DevOps tools. • Easily access data security solutions through online marketplaces.	**Application Security** Runtime Protection Web Application Firewall DDoS Protection Bot Protection API Security **Data Security** Community Edition Secrets Management DPOD Marketplace
Part D. 2, g "Utilize effective controls, which may include **Multi-Factor Authentication..."**	• Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies based on the sensitivity of the data/application. • Protect against phishing and man-in-the-middle attacks.	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
Part D. 2, i "Include audit trails within the Information Security Program **designed to detect and respond to Cybersecurity Events"**	• Detect and prevent cyber threats with web application firewall. • Monitor ICT network and protect from DDoS attacks and Bad Bots. • Monitor API activity, track usage, detect anomalies, and identify potential unauthorized access attempts. • Data activity monitoring for structured and unstructured data on Hybrid IT. • Produce audit trail and reports of all access events to all systems, stream logs to SIEM.	**Application Security** Web Application Firewall DDoS Protection Bot Protection API Security **Data Security** Data Activity Monitoring Transparent Encryption **Identity & Access Management** Multi-Factor Authentication
Part D. 2, k Dispose of non-public information in any format	• Locate structured and unstructured regulated data across hybrid IT and prioritize remediation. • Remove keys from CipherTrust Manager can ensure secure deletion, digitally shredding all instances of the data.	**Data Security** Data Discovery & Classification Encryption & Key Management

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