THALES

www.thalesesecurity.com

## THALES eSECURITY HELPS FINANCIAL INSTITUTIONS COMPLY WITH THE NY DFS CYBERSECURITY REGULATIONS (23 NYCRR PART 500)

- Access control ensure only credentialed users can retrieve sensitive data
- Security intelligence logs help establish an audit trail of access attempts
- Strong encryption and key management renders sensitive data useless to unauthorized users
- Data protection that addresses third-party security risks

‹Thales eSecurity›

# COMPLY WITH THE NY DFS CYBERSECURITY REGULATIONS

## (23 NYCRR PART 500)

Thales eSecurity's data security solutions provide the tools you need to align with key elements of the NY DFS cybersecurity regulations (23 NYCRR Part 500).

### ABOUT THE NY DFS CYBERSECURITY REGULATIONS

New York's cybersecurity regulations, which became effective in March 2017, exemplify the continuing trend toward regulatory oversight of organizations' cybersecurity protections. As governments seek to address the threats to citizens' data, specific requirements around cybersecurity are becoming more commonplace, as is the risk of financial and reputational damage for organizations found to be non-compliant.

Enforcement of the regulations is expected to occur pursuant to the NY DFS' authority under the New York Banking Law, which authorizes the assignment of penalties based on violations of any regulation promulgated under the DFS' jurisdiction – which would include the cybersecurity regulations. The New York Banking Law allows for penalties of up to $2,500 per day for any violation; up to $15,000 per day for reckless or unsound practices; and up to $75,000 per day for a willful violation.[1]

1 http://codes.findlaw.com/ny/banking-law/bnk-sect-44.html

‹Thales eSecurity›

# COMPLY WITH THE NY DFS CYBERSECURITY REGULATIONS

## KEY DATES

Mar 1, 2017: 23 NYCRR Part 500 becomes effective.

Aug 28, 2017: 180 day transitional period ends.

Feb 15, 2018: First certifications required (23 NYCRR 500.17(b)).

Mar 1, 2018: Compliance with sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b).

Sep 3, 2018: Compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15. [Encryption and monitoring of authorized users goes into force.]

| 23 NYCRR 500 | Summary | Thales Coverage |
|---|---|---|
| Section 500.06 audit trail | Include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | Thales eSecurity's Vormetric Data Security Platform includes Security Intelligence Logs that generate audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the enterprise. |
| Section 500.07 access privileges | Limit user access privileges to Information Systems that provide access to Nonpublic Information and periodically review such access privileges. | Thales eSecurity's Vormetric Data Security Manager enables the organization to limit user access privileges to Information Systems that provide access to Nonpublic Information. |
| Section 500.08 application security | Write procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity. | With Thales eSecurity's Vormetric Application Encryption your organization can encrypt specific files or columns in databases, big data nodes, and platform-as-a-service (PaaS) environments. The application encryption solution features a set of documented, standards-based APIs that can be used to perform cryptographic and key management operations in your technology ecosystem. |
| Section 500.11 third party service provider security policy | Implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. | Thales eSecurity will help you ensure your third-party service providers, security meets your own rigorous standards. Thales also offers multi-cloud encryption with centralized key and access control management for enterprises using the Cloud, SaaS and other third-party services. |
| Section 500.14 training and monitoring | Implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | The Vormetric Platform's Security Intelligence Logs let your organization identify unauthorized access attempts and to build baselines of authorized user access patterns. Vormetric Security Intelligence completes the picture with pre-built integration to leading security information and event management (SIEM) systems that make this information actionable. The solution allows immediate automated escalation and response to unauthorized access attempts, and all the data needed to build behavioral patterns required for identification of suspicious use by authorized users, as well as training opportunities. |
| Section 500.15 encryption of nonpublic information | Implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | Thales eSecurity's Vormetric Transparent Encryption solution protects data with file and volume level data-at-rest encryption, access controls, and data access audit logging without re-engineering applications, databases or infrastructure. Deployment of the transparent file encryption software is simple, scalable and fast, with agents installed above the file system on servers or virtual machines to enforce data security and compliance policies. Policy and encryption key management are provided by the Vormetric Data Security Manager.<br><br>In addition, Thales eSecurity's Datacryptor 5000 network data encryption solution uses high-assurance encryption methods and state of the art key management techniques to provide robust security, low latency and high performance in Layer 2 and IP networks. |

Follow us on:

**Americas –** Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
**Asia Pacific –** Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
**Europe, Middle East, Africa –** Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com