CERTES
CERTESNETWORKS.COM

WHITE PAPER |

CERTES NETWORKS – COMPLIANCE SOLUTIONS

New York Department of Financial Services

The New York Department of Financial Services' (NYDFS) introduction of 'first-in-the-nation' cybersecurity rules require banks, insurers, and other NYDFS-regulated financial services companies to adhere to stringent cybersecurity requirements. The new cyber security requirements (23 NYCRR 500) came into effect on March 1st, 2017. The new rules mandate firms to test their computer systems. Firms need to establish plans to respond to cybersecurity events. Finally, firms need to annually certify compliance with the cybersecurity requirements.

Firms operating within the jurisdiction of the State of New York will have to prepare and submit a Certification of Compliance from February 15th, 2018. It is common opinion that other States will follow suit and implement their own regulations based on the New York requirements. Therefore, the impact of the regulations are of relevance and interest not only to organizations in New York but to the whole of the United States. They can also impact any third party wishing to do business with financial services firms in New York, as explained below.

NYDFS Requirements

Given the current regulatory environment, many of the demands of NYDFS will have already been met. From appointing a CISO to adopting a written cybersecurity policy, good security practices will address a large part of the NYDFS demands. However, there are a number of specific technical requirements that are brand new and which firms need to be aware of. This includes the need to enforce encryption for all Nonpublic information both in transit and at rest (this must be in place by September 2018). In addition, firms must impose stronger access privileges for all Nonpublic information. Furthermore, firms must implement written policies and procedures regarding how data accessed by third parties is secured. These policies should address how those third parties use encryption to protect data in transit. Therefore, third parties may be forced into deploying encryption as a security measure (otherwise they risk losing business to competitors that do).

How does Certes Networks help you comply with NYDFS?

Certes Networks' patented Layer 4 stealth encryption is quick to deploy and easy to manage. Certes Next Gen Encryptors are multi-layer encryption appliances that provide data protection and application segmentation. The Next Gen Encryptors integrate easily into any existing network. They operate transparently to the network infrastructure. They ensure that all data is encrypted without impacting overall network performance.

- **Confidentiality:** Packet level encryption protects data in motion across any network.
- **Integrity:** Per packet authentication prevents the injection of rogue packets into your network.
- **Ease of Deployment:** 100% Software-Defined security overlay eliminates the need to re-architect the network or replace legacy applications.
- **Scale:** Supports your national or global infrastructure across multiple provider networks.
- **Control:** Patented, centralized, and automated control of keys and policies at enterprise scale.
- **Third Party Protection:** Lower risk use of third-party resources, including Cloud, WAN, or MPLS.

NYDFS Requirement	Resolution	How Certes Networks Helps
Access Privileges 500.07	Limit user access privileges to Information Systems that provide access to Nonpublic information and periodically review such access privileges	• We enable you to define roles and set permissions to enable role based access to Nonpublic information. • Our fine grained role based access enables essential separation of duties for secure management of access control - ensuring no one individual is responsible for both setting and implementing security policy. • Ease the management process by using prebuilt roles; or create your own to meet the organization's security structure.
Encryption of Network Information 500.15 (a)	Implement controls, including encryption, to protect Nonpublic information held or transmitted by the Covered Entity both in transit over external networks and at rest.	• Certes Next Gen Encryptors are multi-layer encryption devices offering Layer 2, Layer 3 or Layer 4 encryption. They can provide protection for any type of private network. • Integrating easily into any existing network, Certes Networks' overlay solution requires no rearchitecting of the network, enabling encryption to be rapidly deployed. • Operating transparently within the network infrastructure, there is no performance degradation. • Works with existing networks with no impact on existing failover, redundancy and load-sharing.
Third Party Service Provider Security 500.11	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. (Includes the use of encryption as required by Section 500.15)	• Certes Zero Trust WAN extends trust across the network. • We encrypt data as it traverses a third party service provider network or the Internet. • Our 'drop-in' solution works with existing network and applications. • By encrypting all data an organization can minimize challenges arising from third party security shortfalls. This can reduce the burden of time-consuming or expensive audits of business partners. • Avoids the business constraint associated with changing third party providers as organizations are not limited by security provisions.
Audit Trail 500.06	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.	• Certes provides a full audit trail for logging and auditing to support all compliance and audit reviews. • Complete record of key changes, policy changes and device configuration changes.

About Certes Networks

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you “Encryption without Compromise”.

For more information visit **CertesNetworks.com**

Global Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
Tel: +1(888) 833-1142
Fax: +1(412)262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East & Africa Sales
emea@certesnetworks.com

V1-06-01-2017