Compliance Overview

This document provides an overview of the verticals that are the most regulated in terms of logical access security.

A general approach is discussed, followed by specific compliance regulations as follows:

1 Healthcare
2 Law Enforcement
3 Financial
4 Utilities
5 Manfucturing

General Approach

Emphasize:	**Easy add-on** IT admins at these organizations are so busy, they don't want to revamp the whole network system just to add logical access control. Sphinx Logon requires no change to their existing infrastructure - installs within minutes instead of days and is non-invasive. **Experience** Over the past 16 years, the Sphinx software has been continuously expanded and fine-tuned according to the needs of its customers. The result is that the standard software comes with the all the options and features these types of organizations need.
Differentiation from competitors:	• Many competitors have more complex infrastructure solutions, yet the security they provide is not better than Sphinx Logon. • Or, customers may think they need to go for the most secure solution, such as a full fledged Public Key Infrastructure (PKI). But this level of security is not a requirement of HIPAA, CJIS, or the other regulatory agencies listed here. Also the level of complexity and work required to manage such a solution causes many to give up and seek an easier solution. • Customers should be aware that many vendors sell their solutions in modules, meaning the customer must pay multiple fees. Sphinx Logon has only one license fee, based on the number of cardholders. Also, Sphinx licenses never expire.
Target:	• In all of these organizations, get the IT decision maker involved in the discussion as early as possible. • If there's no in-house IT admin - ie, for smaller organizations - ask to work with their IT integrator. This can also lead to additional sales through the IT integrator's contacts.

1 HEALTHCARE	
Compliance:	**HIPAA** (Health Insurance Portability and Accountability Act) Requires that all healthcare organizations, big and small, must have elevated logon security. * Must confirm that users are who they claim to be. * Trackable when users accessed the network. Sphinx Logon provides the two-factor authentication (card + PIN) and audit trail that meet this requirement.
Links:	HHS.gov overview: http://www.hhs.gov/hipaa/for-professionals/index.html Recent article: http://www.healthdatamanagement.com/opinion/hipaa-turns-20-why-its-an-effective-law-for-healthcare
Sphinx case study:	http://www.odsphinx.com/web/casestudies/CaseStudyRegionalHospital.pdf

2 LAW ENFORCEMENT	
Compliance:	**CJIS** (Criminal Justice Information Services) Security Policy Specifically 5.6.2.1.2 Personal Identification Number (PIN) and 5.6.2.2 Advanced Authentication. * Each individual's identity must be authenticated. * Advanced authentication required when individuals logon from outside of a physically secure location. Sphinx Logon provides the two-factor authentication (card + PIN) that meets this requirement.
Links:	FBI overview: http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view Recent article: http://www.policemag.com/channel/technology/articles/2016/03/what-is-the-fbi-cjis-security-policy.aspx
Sphinx case study:	http://www.odsphinx.com/web/casestudies/CaseStudyMidwestPolice.pdf

3 FINANCIAL	
Compliance:	**GLBA** (Gramm-Leach-Bliley Act) • "...requires financial institutions - companies that offer consumers financial products or services like loans, financial or investment advice, or insurance - to explain their information-sharing practices to their customers and to safeguard sensitive data". • "Under the Safeguards Rule, financial institutions must protect the consumer information they collect". • "Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs." • "Controlling access to sensitive information by requiring employees to use “strong” passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.)" Sphinx Logon provides the two-factor authentication (card + PIN), user group control, and password change updater that meets these requirement.
Links:	FTC overview: http://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act Compliance advice: http://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying#how
Sphinx case study:	http://www.odsphinx.com/web/casestudies/CaseStudyMortgageBroker.pdf

4 UTILITIES	
Compliance:	Municipals such as electric, gas and water companies are subject to accountability regarding their logical access controls. NIST (National Institute of Standards and Technology) is the organization that provides voluminous security standards documents. The NIST Cybersecurity Practice Guide Energy states: "They must authenticate authorized individuals to the devices and facilities to which they are giving access rights with a high degree of certainty." Another NIST special publication states: "...compliance necessitates organizations executing due diligence with

	regard to information security and risk management. In sum, when municipals use advanced authentication, they meet the government requirements. Sphinx Logon provides the two-factor authentication (card + PIN) that meets this requirement.
Links:	NIST Energy link: https://nccoe.nist.gov/sites/default/files/library/sp1800/es-idam-nist-sp1800-2b-draft.pdf Water departments overview: http://www.awwa.org/portals/0/files/legreg/documents/awwacybersecurityguide.pdf Article that provides links to public utilities industrial control security: http://www.nist.gov/el/isd/scada-021015.cfm Interesting article about an attack: http://www.tripwire.com/state-of-security/incident-detection/dhs-confirms-u-s-public-utilitys-control-system-was-hacked/

5 MANUFACTURING	
Compliance:	Although there is no official regulation in this vertical, many suppliers are required to protect the confidential data of the companies to which they deliver. They must document how they control access to sensitive information such as data that constitutes intellectual property and be able to show that only certain employees are allowed access to the information. Sphinx Logon provides the two-factor authentication (card + PIN) that ensures that only employees with proper rights can access confidential data. Note also that NIST (National Institute of Standards and Technology) is currently working on a Cybersecurity for Smart Manufacturing Systems project, so it will be interesting to see the results of this in the coming years.
Links:	NIST project status: http://www.nist.gov/el/isd/cs/csms.cfm Recent article: http://www.controleng.com/blogs/system-integration-and-process-control/single-blog/a-guide-to-industrial-control-system-security/fed7d7659ae1be7ec369aec20448b510.html
Sphinx case study:	http://www.odsphinx.com/web/casestudies/CaseStudyAutoPartsSupplier.pdf