CSBS SINCE 1902

CONFERENCE OF STATE BANK SUPERVISORS

Conference of State Bank Supervisors (CSBS)
Job Description

Job Title	**Chief Information Security Officer**
Reports To	**Chief Information Officer**
Department	**SRR**
FLSA Status	**Exempt**
Date	**June 2015**
Position Number	**200**

Job Summary

This position is responsible for providing vision, leadership, oversight and management of CSBS physical and cyber security policies, procedures and practices. The CISO is responsible for ensuring that CSBS and its subcontractors implement industry best practice policies, procedures and practices that address physical security, cyber security, data privacy and protection, as well as compliance with relevant laws and regulations. The CISO also provides thought leadership in conjunction with his/her engagement in industry and government forums, and collaboration with state and federal cyber security experts and practitioners.

Essential Functions

To perform this job successfully, an individual must be able to perform each essential duty and responsibility satisfactorily. Reasonable accommodations may be made to enable an individual with disabilities to perform the essential functions. Other duties may be assigned to meet business needs.

- Develop and maintain the CSBS strategic security program and plan, taking into consideration business and legal requirements, risk (likelihood and impact), and criticality; and building consensus among stakeholders.
- Develop, maintain and enforce CSBS physical and cyber security policies and practices designed to protect sensitive corporate assets, ensure data privacy, and comply with laws and regulations, including the Federal Information Security Management Act (FISMA), Payment Card Industry (PCI) and the Criminal Justice Information System (CJIS) and other applicable privacy laws. Familiarity with Service Auditor Reports such as SSAE16 Service Organization Controls [SOC] reports.
- Manage contractors and outsourcers providing technology services to CSBS, including managed security services, infrastructure engineering, operations, desktop support, and software development. Ensure compliance with the appropriate laws and regulations.
- Develop, maintain and enforce CSBS security policies and procedures, for example:
    - Identification of sensitive data and policies/practices regarding the identification of sensitive data as well as practices for information labeling, handling and storage.

  - Personnel security, including role-appropriate pre-employment background checks; and Security Awareness Training, ensuring necessary and appropriate content and compliance with requirements for each SRR employee to take the training as well as the frequency of updated training.
  - Network, infrastructure and application security.

- Ensure technology solutions adhere to best practices and meet security requirements, including Software-as-a Service (SaaS) contracts, Infrastructure-as-a-Service (IaaS) contracts, Platform-as-a-Service (PaaS) contracts and customized software development solutions.
- Provide guidance and make recommendations to CSBS management and Board of Directors with regards to the security characteristics (i.e., advantages and disadvantages) of various technologies and business practices.
- Ensure contracts with 3rd parties contain appropriate security language, including data privacy and protection language required by state and federal laws. Develop, maintain and manage a third party security assessment program for key vendor relationship and third party providers.
- Manage the CSBS Incident Response Plan. Perform incident response planning, including developing, maintaining and enforcing the CSBS Incident Response Plan in addition to managing security incidents if/when they occur. This would include coordinating incidents, if applicable, with associated third party providers and, if applicable, multiple regulatory organizations and stakeholders.
- Coordinate, provide leadership and management for security related audits and inspections. Interface as the primary contact with state and federal regulators and third party contractors with regards to CSBS' security posture and practices.

Additional Responsibilities:

- Provide thought leadership to industry and government forums related to cyber security practices, issues and challenges in the financial services industry, such as the Executive Leadership of Cybersecurity. Collaborate with industry and government security officials on security-related issues and initiatives, including national security issues impacting the financial services sector.
- Monitor industry trends for changes in physical and cyber security challenges and implement planning, policy and procedure changes in response.
- Contribute to industry and government forums that develop industry guidance and regulations regarding security practices.
- Prepare and present security related briefings for senior CSBS and industry executives as well as state and government regulators.

CSBS SINCE 1902

CONFERENCE OF STATE BANK SUPERVISORS

Minimum Qualifications

To perform this job successfully, an individual should possess the knowledge, skills, and abilities listed and meet the amount of education, training and/or work experience required.

Education and Experience

- Master's degree in technology related discipline or a Bachelor's degree with Master's equivalent work experience in information security, privacy or compliance.
- Industry Security Certification such as a valid and current CISSP, CISA or CISM certification is mandatory. Additional certification in CAP (FISMA), PCI QSA, ITIL, CSA CCSK (Cloud) or ISO 27001 is desired, but is optional
- Minimum of 15 years of experience in security is required. Ideally this would include some experience in the role of a Chief Information Security Officer (CISO)/Chief Security Officer (CSO) of an organization with a significant "footprint" in the financial services industry.
- At least 7 years of experience in managing information security programs in accordance with the Federal Information Security Management Act (44 U.S.C. 3544), guidance and standards from the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS).
- The candidate should possess a Top Secret security clearance, or be reasonably confident of his/her ability to obtain one (e.g., by already possessing a Secret level security clearance) in order to participate in classified briefings.

Knowledge, Skills, and Abilities

- Knowledge of, and experience with current physical and logical security issues and best practices in datacenter infrastructure, networks, end user computing and applications.
- Knowledge of the cloud computing industry, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), including the security and privacy issues associated with using cloud infrastructure.
- Ability to work calmly during stressful circumstances.
- Strong interpersonal skills and communication skills. Ability to communicate at the executive level, including CXO level personnel as well as the CSBS Board of Directors and the SRR Board of Managers.
- Strong planning and task management skills. Management experience.
- Strong vendor management skills. Ability to manage and assure successful delivery from outsourced third party security and infrastructure providers.
- Ability to work in collaboration with a variety of stakeholders to identify and discuss issues.
- Ability to work in fast paced environment managing multiple projects driven by multiple deadlines.

CSBS SINCE 1902

CONFERENCE OF STATE BANK SUPERVISORS

Working Conditions

- Office work environment
- Some travel required

This job description should not be construed to imply that these requirements are the only standards for the position. Incumbents will follow any other instructions and perform any other related duties as may be required. CSBS has the right to revise this job description at any time. CSBS is an "at will" employer and as such, neither this job description nor your signature constitutes any form of contractual arrangement between you and CSBS.

Employee's Signature:	Date:
Manager's Signature:	Date: