Position Description
Information Technology Manager
Working Title: State of Wisconsin Chief Information Security Officer (CISO)

Department of Administration
Division of Enterprise Technology

Position Summary

The Chief Security Information Officer (CISO), Director for the Bureau of Security, reports to the Division's Deputy Division Administrator and is responsible for the statewide security (i.e. cybersecurity) program while representing the State of Wisconsin among its peer state CISOs across the nation as the State of Wisconsin CISO. The CISO's role is to provide vision and leadership for developing and supporting security initiatives as a component of the department's oversight responsibilities for all state agencies. The CISO directs the planning and implementation of enterprise Information Technology (IT) security solutions in support of associated business operations and general defenses against security vulnerabilities.

The CISO is responsible for providing regulatory oversight of IT security. This oversight includes the development of enterprise-wide policy, standards, and procedures as guidance for compliance with federal laws, regulations, and sound security, data, and privacy practices. Additionally, the CISO is responsible for developing security program strategy and plans to ensure compliance and further enhance security practices across all state agencies, while aligning to the Wisconsin's Strategic IT Plan.

The CISO is responsible for security technologies in support of statewide operations on-premises and in the private and public cloud. The CISO is responsible for maintaining collaboration and coordination within the department, with the state agencies we support, local units of governments, Wisconsin tribes and educational entities. The CISO is also responsible for identifying and assessing internal and external threats, vulnerabilities and risks as well as ensuring for robust monitoring, timely detection, containment, and incident response necessary to mitigate any possible exposure.

The CISO is responsible for ensuring that technologies and associated projects are appropriately monitored for security risks with risk mitigation requirements being efficiently set and appropriately designed and delivered with any technological implementation. Policies, standards, and technical procedures will need to be regularly reviewed and updated to provide direction as to prevent unauthorized access to State of Wisconsin systems.

Goals and Worker Activities

30% A. Manage the bureau's programs and staff. Provide leadership, management expertise and direction to bureau staff.

1. Plan, direct, manage and evaluate the operations of the bureau.
2. Direct the development of bureau plans to respond to the goals established by the department and division. Develop work plans to ensure efficient use of staff resources.

3. Establish annual objectives for the bureau. Analyze resources in terms of overall goals and objectives of the bureau to ensure proper allocation. Work with your leadership to refine.
4. Organize the resources and activities of the bureau for maximum effectiveness and efficiency in achieving Bureau, Division, Department and Enterprise responsibilities, objectives, and strategic plans.
5. Establish workload priorities, assign tasks, and instruct and direct employees in completing their assigned duties.
6. Counsel and motivate staff to provide them a leader to openly communicate with.
7. Develop performance standards to maximize productivity, conduct periodic performance evaluations, and recommend training to meet performance standards and enhance career development. Develop training plans for staff to ensure the necessary level of staff competency.
8. Recommend/initiate personnel actions (hiring, reclassification, etc.) as needed to ensure appropriate and effective allocation of staff resources and compensation of employees.
9. Maintain channels of communication with all staff to ensure that employees are informed of division and project objectives, activities, and plans and encourage input from employees.
10. Maintain professional, effective communications with subordinates, peers, and leadership across the enterprise to encourage and ensure a comprehensive cyber response organization based on trust and cooperation.

20% B. Develop organizational strategy to ensure that security is continually considered. Ensure that the technology and data resources of the organization are secure.

1. Ensure the confidentiality of sensitive information processed by, stored in, and moved through information systems and applications, while following the guidelines enforced by national standards and compliance organizations such as NIST, the IRS, and the FBI.
2. Ensure the integrity of the information such that decisions and actions taken based upon the data processed by, stored in, and moved through information systems can be made with the assurance that the information has not been manipulated.
3. Develop a security strategy, associated roadmaps, and supporting documentation to effectively communicate to leadership and those the division supports. Align that strategy to industry standards, ensuring a multi-facetted defense model that best utilizes state dollars.
4. Identify and assess internal and external threats, vulnerabilities and risks as well as ensuring robust monitoring, timely detection, containment, and incident response necessary to mitigate the exposure caused by an incident is in place.
5. Manage audits conducted by state and federal compliance organizations and report results to leadership within the impacted agencies.
6. Manage regular reviews of access to all systems and develop risk analysis and rating of all current and future systems and platforms.
7. Organize vulnerability assessments and security reviews. Investigate security violations and report policy violations to management.
8. Develops and coordinates remediation plans to address security vulnerabilities.

9. Develop and administer an effective security awareness program.
10. Oversee the development and maintenance of incident response plans.
11. Develop and maintain budgets associated with security and business continuity related expenses.

20% C. Develop and manage security policies, standards, procedures, which meet the goals and objectives of the enterprise strategic plan. Ensure on-going oversight and security requirements for project initiatives are planned and implemented appropriately.

1. Develop a comprehensive program for planning, design, implementation, and monitoring of security measures.
2. Represent the State of Wisconsin with Federal Agencies, other State Governments, Private Industry and the Education Sector.
3. Be a security reference for all Wisconsin government entities, able to coordinate security efforts across the state.
2. Manage the development and publication of enterprise-wide information security policies, standards, and procedures to ensure compliance for federal and state audit organizations.
3. Recommend tools for the implementation of security best practices; work closely with systems, network, and application development personnel to ensure the integrity of information security procedures.
4. Oversee efforts to protect enterprise-wide computing and information assets through the use of security best practices.
5. Oversee staff and vendors who safeguard the state's assets, intellectual property, and computer systems.
6. Ensure that technologies and associated projects are appropriately monitored for security risks with risk mitigation requirements being efficiently set and appropriately designed and delivered with newly developed technologies.

10% D. Identify protection goals and objectives consistent with enterprise strategic plan.

1. Ensure that business requirements are reflected in security policy, thus ensuring that the policy enables rather than restricts business operations.
2. Participate closely in related areas such as business continuity planning and data and privacy initiatives.
3. Initiate ad hoc projects to investigate the advantages, disadvantages, risks, and cost of common security initiatives, and advise the CIO with appropriate recommendations.
4. Act as custodian of enterprise-wide strategic security processes (e.g., role analysis, data classification) by validating process ownership, responsibilities, and stakeholders.
5. Respond to enterprise-level audit exceptions (i.e., those audit exceptions where a specific individual cannot be found to be responsible).
6. Infuse a security culture throughout the enterprise.

7. Ensure that security considerations are engineered into the infrastructure (e.g., network architecture, middleware design, application-level authorization).
8. Work closely with enterprise architecture to facilitate this infusion by ensuring the currency and applicability of the security principles and standards.
9. Actively participate in the ongoing efforts to establish and manage enterprise architecture.
10. Routinely review enterprise architecture guidance documents to ensure compliance with current security laws, regulations, guidelines, and best practices. Maintain a common and uniform architecture for security protection to maximize interoperability of component agency information systems.
11. Maintain a common and uniform architecture for security protection to maximize interoperability of component agency information systems.
12. Participate in government-wide initiatives to share lessons learned and ensure compliance with the security policies, guidelines, and best practices.

10% E. Oversee the investigation of security incidents and assist with disciplinary or legal matters associated with such incidents as necessary.

1. Proactively monitor federal and commercial computer incident response and homeland security groups (MS0ISAC, US-CERT, etc.) to determine potential threats to systems.
2. Coordinate establishment of Computer Incidents Response Team with Legal and HR to combat threats and disruptions associated with phishing, identity theft, government investigations, and potential lawsuits.
3. Provide appropriate notification to security officers in agencies and as required, collect feedback on the mitigation of new vulnerabilities and threats.
4. Coordinate anomaly reporting to determine if potential threat activity is directed against one component agency or across all the enterprise, achieving Bureau, Division, Department and Enterprise responsibilities, objectives and strategic plans.
5. Coordinate incident reporting to outside organizations, including law enforcement and government-wide incident response.
7. Interact with the CIO to ensure that the fiscal decisions related to IT across the department maintain and enhance our information security posture.

10% F. Work with outside consultants as appropriate for independent security and compliance audits and perform other duties as requested by the CIO or other leaders.

1. Work closely with Technology, Legal, Human Resources, Privacy, Risk Management, Business Leaders, as well as internal and external audit departments, regulators, and vendors.
2. Develop strategic partnerships with service providers and outsourcing partners to produce "win-win" results.

3. Participate in the regular reviews on the progress of projects and initiatives in progress and ensure continued compliance with security requirements, best practices, and efficient use of bureau resources.
4. Ensure DevSecOps is effectively utilized in the development of applications.
5. Make formal presentations to CIO, business executives, senior managers and clients/partners on strategic security directions and architectural recommendations to gain commitment and funding.
6. Facilitate third party security testing and verification such as penetration tests and audits to enhance customer's trust.
7. Provide risk assessment services to business units in support of their operations.

Knowledge and Skills

General

1. Strong oral and written communication skills including the ability to communicate business and technical concepts and information effectively to a wide range of audiences including the public.
2. Strong inter-personal skills including the ability to work independently, with high-level government officials, business and IS managers, and staff in federal, state and local agencies, and with division and department managers in a decentralized environment.
3. Strong project management skills.
4. Proven ability to plan and organize work, requiring an in-depth understanding of security issues and ability to integrate into the work of others.
5. Ability to defend and explain difficult issues with respect to key decisions and positions to staff and senior officials.
6. Experience in analyzing enterprise business and technology issues in a large corporation or government organization.
7. Ability to establish credibility as to garner support for recommendations.
8. Ability to identify appropriate members and develop effective teams with specific knowledge and skills needed to develop solutions and make recommendations.
9. Resourceful in identifying and obtaining information from sources needed to perform responsibilities effectively.

Technological/ Specific

10. Must be an articulate and persuasive leader who can serve as an effective member of the senior management team and who is able to communicate security-related concepts to a broad range of technical and non-technical staff.
11. A strong cybersecurity background and experience in business management.
12. Knowledge of secure software development.
13. Computer/network investigation skills and forensics knowledge.
14. Extensive knowledge of networks, system, database, and applications security.
15. Demonstrated ability to work with management and staff at various levels of the organization to implement sound security practices.
16. Ability to provide technical direction to security architects and project consultants to ensure appropriate security requirements are set forth on new development efforts.

17. Knowledge of standards-based architectures, with an understanding of how to get there, including compliance monitoring and enforceability.
18. Demonstrated understanding of legacy system security issues and their interface with present-day successor architecture.
19. Experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
20. Strong working knowledge of security principles (such as authentication, vulnerability testing, penetration testing, auditing, and risk management) and security elements (perimeter controls, VPNs, and firewalls).
21. The ability to develop and effectively document strategy, supporting road maps, and work with teams and leadership to communicate them.