STATE OF SOUTH DAKOTA
CLASSIFICATION SPECIFICATION

Cybersecurity Series

In this series:

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Technician	808604	ITH 4	Covered	Non-exempt
Cybersecurity Analyst	808607	ITS 7	Covered	Exempt
Cybersecurity Engineer	808609	ITS 9	Covered	Exempt
Cybersecurity Architect	808610	ITS 10	Exempt	Exempt
Cybersecurity Manager I	808619	ITS 9	Exempt	Exempt
Cybersecurity Manager II	808621	ITS 11	Exempt	Exempt

Purpose of Series
This series captures the breadth and depth of work that establishes standards and policies that secure, defend, and preserve data, networks, systems, applications, users, vendors, third party partners and providers, contracts and other designated systems. Incumbents of classifications in this series ensure appropriate security controls and measures are in place and effective through monitoring and analysis of threat information from multiple sources, disciplines, and agencies.

STATE OF SOUTH DAKOTA
CLASSIFICATION SPECIFICATION

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Technician	808604	IT 4	Covered	Non-exempt

Role Description

This is a first-level security and compliance position that works within the framework of established security and compliance policies and procedures.

Example Functions

- Conducts monitoring of data security and implements controls as directed.
- Assists in firewall configuration.
- Guides data security remediation such as security patching.
- Reviews data logs and activities and notifies more senior staff of exceptions.
- Delivers security awareness training.
- Provides input to the preparation of disaster recovery plans.
- Prepares documentation for all actions taken.

Requisite Knowledge, Skills, and Experiences

- Knowledge of IT security issues and resolutions.
- Ability to learn and apply concepts.
- Ability to follow technical direction.
- Ability to problem-solve and apply analytical skill in resolving issues.

STATE OF SOUTH DAKOTA
CLASSIFICATION SPECIFICATION

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Analyst	808607	IT 7	Covered	Exempt

Role Description
Under general supervision, incumbents typically perform a variety of tasks requiring problem-solving, data review, and analysis. Cybersecurity Analysts are responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Example Functions
- Assisting with the development and delivery of end user cybersecurity training.
- Collaborating with Managed Service Providers and clients to respond to inbound requests for information from the SOC.
- Collecting, analyzing, and evaluating information for reliability, validity, and relevance to create effective intelligence products.
- Conducting regular vulnerability scans and penetration testing to identify vulnerabilities and potential for exploitation.
- Documenting all systems security operations and maintenance activities
- Escalating alerts for investigation based on their severity including prioritization of the alerts for follow-on incident response activities.
- Identifying and assessing intelligence gaps between the state and the capabilities and activities of cybersecurity adversaries.
- Interpreting malicious network activity in traffic.
- Participating in cybersecurity planning and review processes including tabletop exercises, cybersecurity audits, assessments, hardening review, baseline standards.
- Participating in threat hunting process.
- Producing findings to help initialize or support law enforcement and counterintelligence investigations or activities.
- Responding to security incidents including system breach or loss of data.

Requisite Knowledge, Skills, and Experiences
- Knowledge and skill in cybersecurity fundamentals such as incident management, forensic analyses, obfuscation techniques, vulnerability scans, threat intelligence, encryption, and decryption.
- Broad understanding and knowledge of client and server architectures and Webserver architectures and systems.
- Broad understanding and knowledge of networking technologies, architectures, and tools
- Knowledge of Internet network addressing.
- Broad understanding and knowledge of programming languages and methodologies.
- Broad understanding and knowledge of data management, retrieval systems and technologies, transfer technologies, and backup systems.

STATE OF SOUTH DAKOTA
CLASSIFICATION SPECIFICATION

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Engineer	808609	IT 9	Covered	Exempt

Role Description
Under administrative supervision, Cybersecurity Engineers apply a depth of knowledge and skill in complex and varied work situations with limited need for direction. Incumbents design, develop, test, and evaluate information system security throughout the systems development life cycle and serve as a subject matter expert in the cybersecurity field and/or are leads of teams and projects.

Example Functions
- Analyzing user needs and requirements to plan and conduct system security development.
- Applying security policies to applications that interface between information systems, physical systems, and/or embedded technologies.
- Creating solutions and tools that help organizations manage disruption of operations.
- Designing or integrating appropriate data backup capabilities into overall system designs.
- Developing Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.
- Developing security risk profiles and mitigation strategies to resolve vulnerabilities
- Engages in ethical hacking and penetration testing to break-in and exploit vulnerabilities of state assets for purpose of reporting of risks.
- Identifying and directing the remediation of technical problems encountered during testing and implementation of new systems.
- Implementing and integrating system development life cycle (SDLC) methodologies into development environment.
- Incorporating cybersecurity vulnerability solutions into system.
- Performing risk analyses and security reviews by assessing threats to and vulnerabilities of computer system.
- Providing input to the Risk Management Framework process activities and related documentation.
- Recommending security changes to system or system components.
- Storing, retrieving, and manipulating data for analysis of system capabilities and requirements.

Requisite Knowledge, Skills, and Experiences
- Understanding of cybersecurity industry standards.
- Knowledge and skill to continually improve standard processes for networking, software development, systems engineering, financial and risk analysis, and security intelligence

STATE OF SOUTH DAKOTA
CLASSIFICATION SPECIFICATION

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Architect	808610	IT 10	Exempt	Exempt

Role Description
Incumbents in this role ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Cybersecurity Architects apply advanced knowledge and skills in complex, difficult, or novel work situations.

Example Functions
- Defining and documenting how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
- Determining the security controls for the information systems and networks and documenting appropriately.
- Developing a system security context, a preliminary system security Concept of Operations (CONOPS), and baseline system security requirements in accordance with applicable cybersecurity requirements.
- Documenting and addressing the state's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
- Ensuring that acquired or developed systems and architectures are consistent with organization's cybersecurity architecture guidelines.
- Evaluating security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.
- Identifies critical infrastructure systems with information communication technology that were designed without system security considerations.
- Identifying and prioritizing critical business functions in collaboration with organizational stakeholders.
- Mentoring the Security Operations Center team and creating development plans for team members.
- Performing security reviews, identifying gaps in security architecture, and developing a security risk management plan.

Requisite Knowledge, Skills, and Experiences
- Knowledge and skill to integrate the organization's goals and objectives into the architecture.
- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of organization's enterprise information security architecture.

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Manager I	808619	IT 9	Exempt	Exempt

Supervises and manages cybersecurity staff who establish standards and policies that secure, defend, and preserve data, networks, systems, applications, users, vendors, third party partners and providers, contracts and other designated systems.

Classification	Class Code	Pay Grade	Civil Service	FLSA
Cybersecurity Manager II	808621	IT 11	Exempt	Exempt

Supervises multiple teams of cybersecurity staff who establish standards and policies that secure, defend, and preserve data, networks, systems, applications, users, vendors, third party partners and providers, contracts and other designated systems.