CS-214
Rev 11/2020

Position Code
1. INTCSPL3G53N

State of Michigan
Civil Service Commission
Capitol Commons Center, P.O. Box 30002
Lansing, MI 48909

POSITION DESCRIPTION

This position description serves as the official classification document of record for this position. Please complete this form as accurately as you can as the position description is used to determine the proper classification of the position.

2. Employee's Name (Last, First, M.I.)	**8. Department/Agency** Legislative Auditor General
3. Employee Identification Number	**9. Bureau (Institution, Board, or Commission)** **Executive**
4. Civil Service Position Code Description **Information Technology Specialist-4**	**10. Division**
5. Working Title (What the agency calls the position) **Information Technology Security Specialist**	**11. Section**
6. Name and Position Code Description of Direct Supervisor **Brian Piggott, Chief Security Officer**	**12. Unit**
7. Name and Position Code Description of Second Level Supervisor **Dorothy Smith, Chief Information Officer**	**13. Work Location (City and Address)/Hours of Work** **201 N. Washington Square, 6th Floor, Lansing, MI 48913** **8:00 a.m. - 5:00 p.m.**

14. General Summary of Function/Purpose of Position

This position will function as the IT security expert who will have office-wide responsibility for the OAG's IT security. The position will be responsible for being the IT security subject matter expert in all IT security matters related to OAG technologies and processes including IT governance, configuration, patch and change management, physical security, identity and access management administration, data integrity, network security, and disaster recovery concepts.

The position will provide security expertise and support for all OAG data systems, applications, infrastructure, operating systems, incident response support and related tasks to ensure they are in compliance with security requirements and applicable security standards.

The responsibilities of this position are of crucial importance to the department, are highly complex, and have substantial direct impact on the overall mission of the OAG.

15. Please describe the assigned duties, percent of time spent performing each duty, and what is done to complete each duty.

List the duties from most important to least important. The total percentage of all duties performed must equal 100 percent.

Duty 1

General Summary of Duty 1 **% of Time** 60____

Monitors, develops, and supports the activities/systems for the OAG Office of Information Technology (OIT) security programs.

Individual tasks related to the duty.

- Under the direction of the Chief Security Officer (CSO), coordinate internal security efforts with the Managed Security Services Program (MSSP) vendor.
- Coordinate with the Chief Information Officer (CIO), CSO, and the Chief Technology Officer (CTO) regarding all business and technical security matters.
- Analyzes and escalates issues on OAG technical environment and contractor hosted solutions.
- Develops and maintains, internal security reports. reviews, analyzes, and escalates issues or anomalies (e.g., AD, 0365 reports).
- Review and escalate, if necessary, the alleged violations of data security and privacy.
- Communicate as needed, with OAG management and staff, IT security and risk management topics.
- Leads all efforts for SEIM system implementation, maintenance, and use.
- Leads activities for vulnerability management activities that include developing standard processes for server scanning, code scanning, and server hardening.
- Work with OIT technical staff to develop and document a corrective action plans to mitigate vulnerabilities identified through by the organization's vulnerability management tools.
- Builds, maintains, and supports security test environment servers and Governance Risk and Compliance (GRC) tools.
- Backup for compliance staff by working on tasks that include risk assessments and change management.

Duty 2

General Summary of Duty 2 **% of Time** 25____

Technical expert for the incident response section in the OAG OIT Security Operations Center. Monitors, contains, and eradicates security events.

Individual tasks related to the duty.

- Provide technical expertise for cyber event detection, correlation, response, and recovery.
- Lead and coordinate with other technical resources in the overall incident response efforts across multiple platforms across multiple state agencies, and with multiple vendors.
- Develop strategic goals required to ensure that the OAG Incident Response processes and procedures are following the best practices.
- Monitor intrusion detection systems to identify potential threats and work with technical staff to mitigate the threats.
- Technology expert for cybersecurity tools that are used to collect and analyze event data to meet program reporting and evaluation requirements. Event data includes tickets serviced, requests sent through to the team, actions, and the results of investigations.
- Receives, analyzes, and interprets escalated requests from analyst staff, and provides consistent and timely responses.
- Analyze and apply lessons learned from information security events to improve event management processes and procedures.
- Ensure that appropriate changes and improvement actions are implemented as required in a timely fashion.
- Ensure and enforce the incident management policy, based on standards and procedures for the organization.
- Identify and implement areas for process improvement that the team will execute.
- Identify, create, and document the response to incidents in accordance with security policies and organizational objectives.

- Develop specific processes for collecting and protecting evidence during a security event and communicate with partners for information sharing and situational awareness.
- Develop and document procedures specific to cybersecurity practices and processes.

Duty 3

General Summary of Duty 3 **% of Time** 10

Facilitate the review of OAG business continuity and disaster recovery plans.

Individual tasks related to the duty.

- Ensure OAG business continuity and disaster recovery plans are prepared and current.
- Review and advise for possible improvement/completeness of office-wide disaster recovery and business continuity plans for comprehensive coverage in accordance with state standards, policies, and best practices.
- Plan for and participate in business continuity and disaster recovery exercises.

Duty 4

General Summary of Duty 4 **% of Time** 5

Other duties as assigned.

Individual tasks related to the duty.

- Participate in team meetings and workgroups to coordinate standards and methods, and to promote sharing of technical information.
- Take training to enhance job-related skills and abilities .
- Serve as a security expert and conducts trainings when needed.
- Provide IT Security presentations to executives and staff when required.
- All other duties as assigned.

16. Describe the types of decisions made independently in this position and tell who or what is affected by those decisions.

Based on professional judgment, makes decisions related to IT security responsibilities including all IT security matters for all OAG data systems, applications, infrastructure, operating systems, incident response support and related tasks.

Based on professional judgment, communicates with OAG and State personnel regarding IT security risks and risk mitigation strategies and measures.

17. Describe the types of decisions that require the supervisor's review.

Operates at the direction of and in consultation with the Information Security Manager. Supervisory review would adhere to the OAG reporting protocols to ensure the Information Security Manager is appropriately informed. Guidance is sought and approval required for:

- Situations that arise that may be deviations from the OAG's practices, standards, or written policies.
- Decisions or actions that could be construed as nonstandard for a professional in a similar position.

18. What kind of physical effort is used to perform this job? What environmental conditions is this position physically exposed to on the job? Indicate the amount of time and intensity of each activity and condition. Refer to instructions.

Standing, sitting, reaching, lifting, carrying, walking, bending and typical office activity including a significant amount of time utilizing the computer.

Participate in 24x7 support rotation for SOC.

19. List the names and position code descriptions of each classified employee whom this position immediately supervises or oversees on a full-time, on-going basis. (If more than 10, list only classification titles and the number of employees in each classification.)

NAME	CLASS TITLE	NAME	CLASS TITLE

20. This position's responsibilities for the above-listed employees includes the following (check as many as apply):

____Complete and sign service ratings.
____Provide formal written counseling.
____Approve leave requests.
____Approve time and attendance.
____Orally reprimand.

____Assign work.
____Approve work.
____Review work.
____Provide guidance on work methods.
____Train employees in the work.

21. Do you agree with the responses for Items 1 through 20? If not, which items do you disagree with and why?

Agree.

22. What are the essential functions of this position?

All duties are essential.

23. Indicate specifically how the position's duties and responsibilities have changed since the position was last reviewed.

N/A

24. What is the function of the work area and how does this position fit into that function?

The Office of the Auditor General conducts post audits of financial transactions and accounts of the State and of all branches, departments, offices, boards, commissions, agencies, authorities, and institutions of the State established by the Constitution or by law and performance audits thereof. The IT Specialist functions as an employee under the CSO, and the position will be responsible for all matters relating to IT security.

25. What are the minimum education and experience qualifications needed to perform the essential functions of this position?

EDUCATION:

Possession of a bachelor's degree with at least 21 semester (32 term) credits in one or a combination of the following: computer science, data processing, computer information systems, data communications, networking, systems analysis, computer programming, information assurance, IT project management or mathematics.

EXPERIENCE:

Three years of professional experience equivalent to an Information Technology Infrastructure or Programmer/Analyst P11 or one year equivalent to an Information Technology Infrastructure or Programmer/Analyst 12.

KNOWLEDGE, SKILLS, AND ABILITIES:

- Thorough understanding of advanced principles, concepts, techniques, and best practices of IT security including NIST and CIS frameworks.
- Knowledge of the disciplines of IT security. Ability to prepare and develop reports, document findings, and provide information.
- Knowledge of best practices for configuration, patch, and change management processes.
- Good knowledge of identity and access management administration methods, data integrity, security, high availability, and disaster recovery concepts.
- Experience in enterprise security design and security infrastructure design.
- Knowledge of operating systems, cloud services, firewalls, and intrusion detection/prevention systems e.g., Windows, VMWare, UNIX VM, CISCO, etc.
- Ability to quickly learn and implement new technologies and procedures.
- Ability to establish and maintain good rapport with office staff at all levels.
- Ability to set priorities and to collaborate and function as a security team leader.
- Ability to develop and conduct training sessions.
- Ability to troubleshoot security alerts or issues under pressure.
- Ability to be self-motivated and work independently.

CERTIFICATES, LICENSES, REGISTRATIONS:

- Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), CompTIA Security+ preferred.

NOTE: Civil Service approval of this position does not constitute agreement with or acceptance of the desirable qualifications for this position.

I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.

_______________________________ _______________________

Supervisor's Signature **Date**

TO BE FILLED OUT BY APPOINTING AUTHORITY

Indicate any exceptions or additions to statements of the employee(s) or supervisors.

I certify that the entries on these pages are accurate and complete.

______________________________	_______________________
Appointing Authority's Signature	**Date**

TO BE FILLED OUT BY EMPLOYEE

I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.

______________________________	_______________________
Employee's Signature	**Date**

NOTE: Make a copy of this form for your records.