State of Michigan
Civil Service Commission

Capitol Commons Center, P.O. Box 30002
Lansing, MI 48909

Position Code
1. INTCSPL3G41N

POSITION DESCRIPTION

This position description serves as the official classification document of record for this position. Please complete the information 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** TECH, MGMT AND BUDGET - IT
3. Employee Identification Number	**9. Bureau (Institution, Board, or Commission)** Executive Bureau
4. Civil Service Position Code Description INFO TECH SPECIALIST-3	**10. Division** Cyber Security and Infrastructure Protection (CIP)
5. Working Title (What the agency calls the position) ITS-14 Security Operations Specialist	**11. Section** Michigan Cyber Security (MCS)
6. Name and Position Code Description of Direct Supervisor BELONGA, NATHANIEL T; INFO TECH MANAGER-3	**12. Unit** Michigan Security Operations Center (MiSOC)
7. Name and Position Code Description of Second Level Supervisor WAIER, BRENDA; STATE ADMINISTRATIVE MANAGER-1	**13. Work Location (City and Address)/Hours of Work** 7150 Harris Dr. Dimondale, MI / Monday – Friday, 8:00am-5:00pm

14. General Summary of Function/Purpose of Position

This position serves as the Security Operations (Sec Ops) expert for all security tools used in the Michigan Security Operations Center (MiSOC). This specialist will be responsible for leading and implementing best practices for supporting MiSOC security tools, concepts, regulatory requirements, standards, hardware, software, networking, operating systems, and automation.

The SO expert will make recommendations to management and executives on best practices and how security can be improved on a State-wide enterprise basis, as well as provide routine updates to leadership on the progress and status of active events. This position will function with significant autonomy and will maintain, advocate and advance the use of emerging data security technologies, develop standards and procedures, promote the usage of automated tools, develop strategies, and align practices with strategic initiatives. This position is responsible to research enterprise security technologies and make recommendations on future system changes and upgrades. Responsibilities include directing, evaluating and validating technical results and initiatives based on current industry research and best practice.

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: **Percentage:** **80**

Technical expert for the development, research, evaluation, recommendation, and planning of security operation tools for Department of Technology, Management and Budget, Office of Cybersecurity, Security Operations section.

Individual tasks related to the duty:

- Provide technical expertise, guidance, and oversight of security operations tool configurations for the following systems: ForcePoint, IBM QRADAR, FireEye Endpoint Protection, SourceFire, NetWitness, Tenable Security Center, Incident Response case management system, MiSOC Active Directory domain controllers, storage and utility servers, mailboxes and calendars used by the MiSOC.
- Lead and coordinate with other technical resources in the overall security operational efforts across multiple platforms, across multiple state agencies, and with multiple vendors.
- Develop strategic goals required to ensure operational compliance with applicable standards, procedures, directives, policies, regulations, and statutes, including the DTMB Strategic Plan and DTMB Security best practices.
- Receives, analyzes, and interprets escalated requests from analyst staff and provides technical expertise in a consistent and timely fashion.
- Provide expert technical guidance to the 18 agencies throughout the State of Michigan during the development, implementation and operation of complex technology systems, used by both the MiSOC internally and SOM agencies externally.
- Engage State of Michigan technology vendor representatives by establishing working partnerships. Stay current on industry security technology and standards. Understand the investment and support of industry security standards by our vendor partners.
- Ensure that IT security systems operations and maintenance remain available to enable critical day-to-day business functions.
- Provide expert technical guidance for the implementation of security applications, operating systems, hardware, network, and security controls. Work with other technical experts within the MiSOC and provide expert guidance in tool related issues.
- Evaluates and recommends continuous improvement plans and their effectiveness regarding the performance and reliability of the MiSOC's infrastructure.
- Direct the design, implementation, maintenance, and coordinate augmentation of the MiSOC's critical tools and infrastructure.
- Design and ensure the daily/weekly/monthly process of backing up security systems to ensure business continuity in case of disaster

Duty 2

General Summary: **Percentage:** **10**

Act as the Security Operations technical expert in the development of new policies, procedures and assessments within the Security Operations section of the MiSOC.

Individual tasks related to the duty:

- Develop advanced strategies for cybersecurity operations based on analysis, research, and industry best practices.
- Analyze and evaluate the effectiveness of enterprise data security policies, processes, procedures and controls against established standards, guidelines and requirements and identify improvement actions required to maintain the appropriate level of data protection and make recommendations to management where appropriate.
- Analyze and enforce security administration change management procedures to ensure that security polices, and controls remain effective following an enterprise change.
- Define and evaluate key performance indicators to measure the effectiveness of information technology security tools.

Duty 3

General Summary: **Percentage:** **10**

Act as a technical and business security expert in the development of new metrics within the Security Operations section of the MiSOC to review, document, and report agency security metrics and incidents to director level management and departmental Information Security Officers

Individual tasks related to the duty:

Actively seek training opportunities for professional development to identify and research new security technology trends

Plan and attend training, as required, to maintain work competencies and skills

Identify and share information related to security tools and technology to application development and technical support staff

Conduct team meetings and work groups to coordinate standards and methods, and to promote sharing of technical information

Ensuring the creation of reports based on audit requirements and standards metrics for management.

Develop and recommend solutions for work planning efforts.

Review and validate official documents such as requests for exceptions to security policies and configurations.

Assess the effectiveness of enterprise security policies, processes, procedures, and controls against established standards, guidelines, and requirements to identify actions required to maintain the appropriate level of cyber security protection and suggest changes where appropriate.

Evaluate metrics on the performance of security tools and direct creation of new reports for management related to security operations.

Act as technical security expert for MiSOC leadership engagements.

Work with management to specify staffing and training requirements.

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.

This level is responsible for assignments that have considerable impact enterprise wide. Independent judgment and decisions are based on the technical areas of security expertise specifically incident response.
• Decisions involved in technology used to implement security architectures.
• Decisions involved with the best approach to resolve technical and functional issues.
• Plan, develop and administer event related policies, procedures, and documentation.

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

Decisions that have a major budget or financial implication, have a resource impact, include setting work priorities, or have significant impact on staff. Problems that are taking a prolonged period of time and will need additional resources to resolve.

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

This job is performed in an ergonomically correct office environment. This position requires occasional bending and lifting up to 40 pounds of computer equipment.

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.

Additional Subordinates

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

N	Complete and sign service ratings.	N	Assign work.
N	Provide formal written counseling.	N	Approve work.
N	Approve leave requests.	N	Review work.
N	Approve time and attendance.	N	Provide guidance on work methods.
N	Orally reprimand.	N	Train employees in the work.

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

Yes

23. What are the essential functions of this position?

The Security Operations Specialist position serves as the expert in security tools, concepts, regulatory requirements, standards, and practices in tools, software, networking, operating systems, and hardware for State of Michigan. This expert will also make recommendations to management and executives on trending threats and how security can be improved on a State-wide basis as well as provide routine updates to management on the progress and status of active events.

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

PD update, this position has changed minimally from the previous review. The duties have just been more detailed in this version to better convey understanding of responsibilities. Tool names were replaced by tool functionality as some vendors have changed, and may change in the future but the functional tool will remain a responsibility.

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

This work area is responsible for maintaining the confidentiality, integrity, and availability of State of Michigan data. This includes the management, configuration and maintenance of security technologies for the State of Michigan, how they function, how they are maintained and the security controls to accomplish these tasks.

26. 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:

Information Technology Specialist 14 - 15
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:

Expert knowledge of security tools used for protecting an enterprise perimeter from cybersecurity threats.
Expert knowledge of concepts and operating principles of data communications and information systems hardware and software.
Expert skills to analyze multiple and highly complex security concepts, issues and opportunities as they relate to security.
Expert knowledge of security operations and the other security teams.
Expert knowledge of the operational and technical problems involved in the administration of a specialized program.
Expert knowledge of the assigned program specialty.
Ability to work collaboratively and establish and maintain good rapport with staff at all levels across the enterprise
Ability to adapt, integrate, and modify existing programs or vendor-supplied packaged programs for use with existing information systems.
Ability to use programming procedures and techniques in the implementation of computer programs.

CERTIFICATES, LICENSES, REGISTRATIONS:

Duties may involve use of a vehicle. Certified Information System Security Professional (CISSP) preferred.

NOTE: Civil Service approval does not constitute agreement with or acceptance of the desired qualifications of 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 | **Date**

TO BE FILLED OUT BY APPOINTING AUTHORITY

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

N/A

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

AMY MILLER | 7/7/2026

Appointing Authority | **Date**

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	Date