State of Michigan
Civil Service Commission

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

Position Code
1. ITPRANAN05N

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)** Cyber Security and Infrastructure Protection
4. Civil Service Position Code Description INFO TECH PRGMR ANALYST-A	**10. Division** Michigan Cyber Security (MCS)
5. Working Title (What the agency calls the position) IT Security Analyst	**11. Section** Michigan Security Operations Center (MiSOC)
6. Name and Position Code Description of Direct Supervisor NEVAI, THOMAS L; INFO TECH MANAGER-3	**12. Unit**
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** Hybrid Remote Work Environment, Dimondale, MI – MSP HQ - / 8:00 a.m. – 5:00 p.m. Occasional on-call or overti

14. General Summary of Function/Purpose of Position

The Security Analyst position works as a member of the Security Operations Team. The Senior Security Analyst position reviews and remediates cyber incidents and vulnerabilities found by IT level analysts to IT security specialists and managers to maintain the confidentiality, integrity, and availability of State of Michigan data.

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:** **55**

Technical security analyst completing cyber investigations involving the security of the State of Michigan network.

Individual tasks related to the duty:

• Reviews and validates security procedures to ensure adequate security procedures have been developed to identify and classify cyber events.
• Ensures that all identified incidents are promptly and thoroughly investigated. Documents standard operating procedures for undocumented incidents, and documents lessons learned.
• Reviews correlated information compiled by an ITPA11 and creates a security plan to mitigate the incident.
• Reviews security incidents for actual or potential breaches or non-compliances and ensures that all identified events are promptly and thoroughly investigated, as needed.
• Reviews, assesses risks and scope for high level security incidents.
• Reviews and validates specifications and implementation of security hardware and software. Implements corrective action as needed.
• Reviews and informs management on security risk assessment results and recommends corrective actions as necessary.
• Reviews metrics on the performance of security responsibilities, controls, and design. Develops new reports for management based on those collected metrics across multiple agencies: conducts trend analysis.
• Train incoming analysts in roles and responsibilities.
• Generates end-of-shift reports for documentation and knowledge transfer to subsequent analysts and other staff on duty.
• Reviews audit results and identifies remediation if necessary and implements corrective action to ensure the effectiveness of enterprise security controls.
• Escalates as necessary.
• Other duties as assigned.

Duty 2

General Summary: **Percentage:** **40**

Technical Security Analyst performing duties related to the Incident Response team.

Individual tasks related to the duty:

• Leads mid to high-level Incident Responses when working to resolve incidents.
• Serves as the Incident response specialist for cyber event detection, correlation, response, and recovery.
• Operates Incident Response tools and determines configuration for tools that are used to collect and analyze data to meet program reporting and evaluation requirements. Incident data includes incident tickets serviced, requests sent through to the IR team, IR actions, and the results of IR investigations.
• Coordinates security responses and root-cause for all cyber security related events for the State of Michigan.
• Evaluate/deconstruct malware (e.g. obfuscated code) through open-source and vendor provided tools.
• Advocates and advances the use of emerging data security technologies, develops standards and procedures, promotes the usage of automated tools, and aligns practices with strategic initiatives.
• Analyzes / Provides 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.
• Interfaces with other agencies to assist and make recommendations on how to improve the security posture and reduce the number of security related events.
• Participates in On-Call rotation.
• Escalates as appropriate to specialists and/or management.

Duty 3

General Summary: **Percentage:** **5**

Maintain knowledge of “state of the art” IT security technologies and developments in new technologies and/or methodologies where feasible.
Executes / Develops security policies and procedures.
Make recommendations for continuous security improvements within the MiSOC.

Individual tasks related to the duty:

- Attend training classes, seminars, and conferences to keep abreast of “state of the art” IT security technology.
- Keep abreast of IT security developments and activities through interface with IT security groups such as the Computer Emergency Response Team (CERT).
- Implement new security methodologies and make recommendations to management regarding the purchase of new security technologies.
- Continuous learning to determine best IT security practices.
- Other duties assigned by management.

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

Decisions involving the development of the IT security systems. These decisions impact the confidentiality, integrity and availability of the sensitive data on the entire State of Michigan network.

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

Decisions regarding the acquisition of new security technologies, as well as system changes affecting enterprise-wide operational tools.

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.

• The position operates in a normal office environment, performing duties within the assigned workspace.
• Tasks can be completed routinely seated at a desk, visiting others at their desks, in the context of meetings and meeting rooms.
• Work requires extensive use of personal computers including keyboards and monitors.
• This position is subject to stress and pressure to resolve problems quickly and effectively.
• There are frequent deadlines that are imposed by external forces; heavy workloads are possible and overtime during development projects may be required.
• Duties may involve lifting of 25 pounds or less.

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?

Prepared by management.

23. What are the essential functions of this position?

• Senior Security Analysts in the Michigan Security Operations Center review and validate security procedures to ensure adequate security procedures have been developed to identify and classify cyber events.
• Ensures that all identified events are promptly and thoroughly investigated.
• Reviews correlated information and builds a security plan to mitigate and identifies a response.
• Reviews security incidents for actual or potential breaches or non-compliances and ensures that all identified events are promptly and thoroughly investigated.

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

Requesting to update the MiSOC ITPA 12 Security Analyst PD shifts the role from a broad security operations position to a more focused Incident Response (IR) role. System administration duties (servers, SIEM, EDR, IPS, vulnerability tools) present in the older PD were removed, and replaced with tasks such as leading cyber incident investigations, malware analysis, coordinating root-cause actions, reporting to management, and participating in on-call rotations. Duty 1 increased from 50% to 55%, emphasizing incident review and documentation. The overall structure, qualifications, and workplace requirements remain largely the same.

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

In their efforts to serve the citizens of the State of Michigan, state agencies are using information technology to deliver and support many of their programs and initiatives. DTMB through the Chief Information Officer (CIO) is responsible for providing the IT services that support the agencies' business goals and objects. The Bureau of Cybersecurity and Information Protection is responsible for cybersecurity and physical security. The Office of Michigan Cyber Security (MCS) reports to the Chief Security Officer who reports to the CIO. MCS was created to provide leadership for an enterprise wide information security program. One of the sections of this information security program is the Michigan Security Operations Center (MiSOC). This section is involved with Regulatory and Standards Compliance; Security Risk Management; Data Security, Digital Forensics; Incident Management; Threat Analytics; IT Security Systems development, design, operations and Maintenance; Network and Telecommunications Security; on an enterprise basis. This position is a senior security analyst in this section.

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

EDUCATION:

Information Technology Programmer/Analyst 9

Possession of an Associate's degree with 16 semester (24 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.

Information Technology Programmer/Analyst P11/12

Possession of a Bachelor's degree with 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 Programmer/Analyst 12
Two years of professional experience equivalent to an Information Technology Infrastructure or Programmer/Analyst P11.

Alternate Education and Experience

Information Technology Programmer/Analyst P11 - 12
Possession of an associate's degree with 16 semester (24 term) credits in computer science, information assurance, data processing, computer information, data communications, networking, systems analysis, computer programming, IT project management, or mathematics and two years of experience as an application programmer, computer operator, or information technology technician; or two years (4,160 hours) of experience as an Information Technology Student Assistant may be substituted for the education requirement.

OR

Educational level typically acquired through completion of high school and four years of experience as an application programmer, computer operator, information technology technician, or four years (8,320 hours) of experience as an Information Technology Student Assistant may be substituted for the education requirement.

KNOWLEDGE, SKILLS, AND ABILITIES:

Two years or more of professional IT experience is preferred. Considerable knowledge of IT security technologies is preferred. Broad knowledge of server administration, network technologies, asset management, databases, is helpful. Must possess excellent communication skills, both verbal and written, and be able to work well in a team environment and handle multiple tasks.
Maintains knowledge of the security tools, concepts, regulatory requirements, standards, and practices in tools, software, networking and operating systems, hardware tools.

CERTIFICATES, LICENSES, REGISTRATIONS:

- The duties require the use of a personal vehicle.
- The position may work overtime, different shift schedules and/or weekends.
- Employment requires passing a drug test and background check.
- The position also requires the passing a LEIN background investigation.

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.

MARCELINA BREWER	3/3/2026
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**