State of Michigan
Civil Service Commission

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

Position Code
1. ITPRANEN84N

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)** MI Cybersecurity & Infrastructure Protection
4. Civil Service Position Code Description Info Tech Prgmr Analyst-E	**10. Division** Michigan Office of Cyber Security
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 BELONGA, NATHANIEL; INFO TECH MANAGER-3	**12. Unit**
7. Name and Position Code Description of Second Level Supervisor NEVAI, THOMAS L; STATE ADMINISTRATIVE MANAGER-1	**13. Work Location (City and Address)/Hours of Work** Lansing, MI / Shift and week-end work required, OT and On-call

14. General Summary of Function/Purpose of Position

This position assists in assuring the confidentiality, integrity, and availability of State of Michigan IT resources and data. It is part of a team responsible for identifying, notifying, and responding to security threats to the state of Michigan Enterprise. The position uses a broad range of security and forensic tools to enhance the response to, support of, and investigation into significant incidents in order to provide a clearer view of the exploits, vulnerabilities, tactics, techniques, and procedures (TTPs) used to cause the incident. This position may also work in the area of physical security for the data centers and perform functions as background checks on contractor's and employees and auditing of access logs.

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**

Participate in the development, implementation, and maintenance of statewide IT security program.

Individual tasks related to the duty:

- Assist in the development, implementation and documentation of IT security procedures.
- Using procedures and various cyber tools the analyst correlates events to identify and gather indicators of compromise for a cyber-incident. Process the incident according to standard operating procedures and escalates as appropriate.
- Creates trouble tickets documenting the incident according to standard operating procedures. Escalates as appropriate.
- Where procedure do not exist escalates cyber incident to ITPA12 for classification.
- Monitor for violations of data security and privacy breaches. Looking at logs, alerts, monitoring traffic of incidents, pull information together.
- Conduct security audits to ensure compliance with State security policies, standards, and procedures.
- Support Incident Response lead when working to resolve incidents
- Process security related tickets research and determine the actual problem.
- Configure, implement and maintain security hardware and software tools
- Assist and provide input to higher level staff in the development of specifications for security hardware and software configuration.
- Assist liaisons or other staff as needed in IT security risk assessments.
- Generate security reports and metrics and offer suggestions for new reports.
- Evaluate firewall change requests and assess organizational risk.

Duty 2

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

Maintain knowledge of “state of the art” IT security technologies and developments in new technologies and/or methodologies where feasible.

Individual tasks related to the duty:

- Conduct research and 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.
- Conduct research to determine best IT security practices.

Duty 3

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

Other duties as assigned

Individual tasks related to the duty:

- Utilize a set of security and forensic tools to identify and document cyber threats to the State of Michigan enterprise environment. Tools could include but are not limited to Content Management Systems, Vulnerability Management Systems, Intrusion Protection Systems, Intrusion Detection Systems, Log Management Systems, Camera Systems, and Physical Access Systems, Penetration Testing tools or Background Check tools.
- Analyze output from tools to provide a clearer view of exploits, vulnerabilities, tactics, techniques and procedures to cause a security incident.
- Be an active member of the State of Michigan's cyber security response team by responding to, trouble shooting, resolving and recommending methods for mitigating risks caused by cyber security incidents.
- Develop expertise in mitigating cyber threats by conducting research, documenting action taken on incidents and implementing changes in response to cyber incidents.
- Conduct security audits to ensure compliance with State security policies, standards and procedures.
- Assist in the development, implementation and documentation of IT security procedures.
- Assist in the development of specifications for security hardware and software configuration.

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 IT security systems. These decisions impact the confidentiality, integrity and availability of 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 needs.

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?

Security Analysts in the Risk Management and Compliance unit develop, maintain and utilize security and forensic tools to identify, document and remediate cyber threats to the State of Michigan enterprise environment. Tools include but are not limited to Content Management Systems, Vulnerability Management Systems, Intrusion Protection Systems, Intrusion Detection Systems, Log Management Systems, Camera Systems, Physical Access Systems, Penetration Testing tools or Background Check tools.

.

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

New position.

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 Cybersecurity (MCS) reports to the Chief Security Office 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 Risk Management and Compliance. This section is involved with Regulatory and Standards Compliance; Security Risk Management; Data Security, Digital Forensics; Incident Management; IT Security Systems development, design, operations and Maintenance; Network and Telecommunications Security; on an enterprise basis. This position is a security analyst in this section.

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 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.

Information Technology Programmer/Analyst P11/12

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 9

EXPERIENCE:

Information Technology Programmer/Analyst 9
No specific amount or type is required.

Information Technology Programmer/Analyst P11
No specific type or amount is required.

Alternate Education and Experience

Information Technology Programmer/Analyst 9
Educational level typically acquired through the completion of high school and two years of experience as an application programmer, computer operator, IT Technician, or two years (4,160 hours) of experience as an Information Technology Student Assistant may be substituted for the education requirement.

KNOWLEDGE, SKILLS, AND ABILITIES:

A minimum of one-year of IT security related work in a professional environment is preferred. Considerable knowledge of IT security technologies, including IDS, vulnerability scanning tools, anti-virus software and forensic techniques is needed. Knowledge of network technologies and familiarity with incident response policies and procedures 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.

CERTIFICATES, LICENSES, REGISTRATIONS:

- The duties require the use of a personal vehicle.
- The duties require working shifts and on 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.

CARRIE WILLIAMS 12/6/2017

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**