STATE OF OHIO (DAS) CLASSIFICATION SPECIFICATION	**CLASSIFICATION SERIES**: Enterprise Information Security	**SERIES NO**.: 6998
	MAJOR AGENCIES: Administrative Services only	**EFFECTIVE DATE**: 08/05/2018

SERIES PURPOSE:
The purpose of the enterprise information security occupation is to provide for the security and privacy of computer networks and data by planning, implementing, upgrading and monitoring security measures.

At the first level, employees deploy & support enterprise security tools.

At the second level, employees collect & analyze intrusion artifacts to enable mitigation of potential incidents & determine best methods for identifying perpetrator(s) of a network intrusion using an array of specialized computer investigative techniques & programs or develop & enforce all security policies & procedures for personal computers & local area networks.

At the supervisory level, employees supervise data security analysts assigned to one work unit in the development, implementation & monitoring of enterprise policies & procedures to ensure data security and privacy of systems and data.

At the managerial level, employees manage enterprise risk management, security operations, &/or privacy programs to ensure the security and privacy of systems and data & supervise assigned staff.

JOB TITLE	**JOB CODE**	**PAY GRADE**	**EFFECTIVE**
Enterprise Information Security Professional 1	69981	35	08/05/2018

CLASS CONCEPT:
The full performance level class works under general supervision & requires considerable knowledge of electronic data processing, computer science & systems analysis in order to deploy & support enterprise security tools such as endpoint protection, Security Information & Event Management (SIEM), Intrusion Detection Systems (IDS) to safeguard State assets against malicious activity, characterize & monitor network traffic to identify anomalous activity & potential threats to network resources & analyze identified malicious activity to determine weaknesses exploited, exploitation methods & effects on system & information or evaluate & support documentation, validation & accreditation processes necessary to assure that new IT systems meet organization's information assurance & security requirements and/or support security audit activites and review security logs to validate access levels and activity.

JOB TITLE	**JOB CODE**	**PAY GRADE**	**EFFECTIVE**
Enterprise Information Security Professional 2	69982	36	08/05/2018

CLASS CONCEPT:
The advanced level class works under general supervision & requires thorough knowledge of electronic data processing, computer science & systems analysis in order to collect & analyze intrusion artifacts to enable mitigation of potential incidents & determine best methods for identifying perpetrator(s) of a network intrusion using an array of specialized computer investigative techniques & programs &/or develop & enforce all security policies & procedures for personal computers & local area networks & applications.

JOB TITLE	**JOB CODE**	**PAY GRADE**	**EFFECTIVE**
Enterprise Information Security Supervisor	69985	16	08/05/2018

CLASS CONCEPT:
The supervisory level class works under general direction & requires thorough knowledge of electronic data processing, computer science & systems analysis in order to supervise security analysts assigned to one work unit.

JOB TITLE	**JOB CODE**	**PAY GRADE**	**EFFECTIVE**
Enterprise Information Security Manager	69986	17	08/05/2018

CLASS CONCEPT:
The managerial level class works under general direction & requires thorough knowledge of electronic data processing, computer science & systems analysis in order to manage enterprise risk management program through planning,

developing, coordinating & implementing information technology disaster recovery & business continuity planning & oversee ongoing development & implementation of statewide information & cybersecurity policies, standards, guidelines & procedures to ensure information security capabilities cover current threat capabilities or act as agency information security officer &, in addition to each preceding option, supervise assigned staff if applicable.

JOB TITLE	JOB CODE	B. U.	EFFECTIVE	PAY GRADE
Enterprise Information Security Professional 1	69981	14	08/05/2018	35

JOB DUTIES IN ORDER OF IMPORTANCE: (These duties are illustrative only. Incumbents may perform some or all of these duties or other job-related duties as assigned.)

Deploys & supports enterprise security tools such as endpoint protection, Security Information & Event Management (SIEM), Intrusion Detection Systems (IDS) to safeguard State assets against malicious activity, Characterizes & monitors network traffic to identify anomalous activity & potential threats to network resources & analyzes identified malicious activity to determine weaknesses exploited, exploitation methods & effects on system & information, tests information assurance safeguards in accordance with established test plans & procedures, determines appropriate course of action in response to identified & analyzed anomalous network activity, determines tactics techniques & procedures for intrusion sets, performs event correlation using information gathered to gain situational awareness & determine effectiveness of observed attack, or works with systems development groups to define & implement security controls for personal computers & local area networks (i.e., analyzes new & existing computer systems to determine appropriate access levels for resources & data files requiring protection by automated data security systems & formulates appropriate access profiles for each application, implements security controls for new & existing systems, monitors system performance & coordinates changes to security software hierarchy with systems development staff & works closely with project & systems development staff to ensure data security is addressed in system design).

Triages malware; uses computer network defense tools for continual monitoring & analysis of system activity to identify malicious activity; implements data security principles, participates in development of archive policies for database elements, provides input & subject matter expertise regarding security practices & automates security tasks using a scripting language (e.g., Power Shell, WMI).

Coordinates responses to IT audit requests; maintains repository of audit information; develops reporting methodology to ensure accurate tracking of audit responses; utilizes subject matter expertise to correctly identify appropriate sources for each type of information requested.

MAJOR WORKER CHARACTERISTICS:

Knowledge of computer science; systems analysis & design; data security practices & implementation; common adversary tactics, techniques & procedures; data backup, types of backups & recovery concepts & tools; cryptology; encryption methodologies; incident response & handling methodologies; network traffic analysis methods; scripting language programs (e.g., Power Shell, WMI)*. Skill in operation of personal computer & associated hardware & software; utilization of network analysis tools to identify vulnerabilities. Ability to define problems, collect data, establish facts & draw valid conclusions; read & understand variety of technical material; write program specifications & system documentation; communicate verbally & in writing on technical & non-technical matters; maintain confidentiality of sensitive information; cooperate with co-workers on group projects.

(*)Developed after employment.

MINIMUM CLASS QUALIFICATIONS FOR EMPLOYMENT:

Completion of undergraduate core coursework in computer science; 12 mos. trg. or 12 mos. exp. in computer data security either through monitoring system/network traffic for anomalous activity, systems development or controlling accessibility of data.

-Or 12 mos. exp. as Information Technology Apprentice, 69910; successful completion of Ohio Cyber Apprenticeship program; additional 12 mos. trg. or exp. in Information Systems/Information Technology with a focus in one of the following areas: Software Engineering/Development, Data Analytics/Business Intelligence, Database Administration, Network, IT Security, and Help Desk/Customer Support.

-Or equivalent of Minimum Class Qualifications for Employment noted above.

Note: The Ohio Cyber Apprenticeship program is a program offered by the Department Administrative Services. 2000 hrs. of on the job experience and 200 certified instructional credits must be earned in order to complete this program.

TRAINING AND DEVELOPMENT REQUIRED TO REMAIN IN THE CLASSIFICATION AFTER EMPLOYMENT:
Not applicable.

UNUSUAL WORKING CONDITIONS:
Work involves operation of computer terminal for long periods of time; overtime may be required.

JOB TITLE	JOB CODE	B. U.	EFFECTIVE	PAY GRADE
Enterprise Information Security Professional 2	69982	14	08/05/2018	36

JOB DUTIES IN ORDER OF IMPORTANCE: (These duties are illustrative only. Incumbents may perform some or all of these duties or other job-related duties as assigned.)

Collects & analyzes intrusion artifacts (e.g., source code, malware, trojans) to enable mitigation of potential incidents & determines best methods for identifying perpetrator(s) of network intrusion using an array of specialized computer investigative techniques & programs (e.g., analyzes log files & other evidence; confirms what is known about intrusion via dynamic analysis; decrypts seized data using technical means; documents original condition of digital &/or associated evidence; ensures chain of custody is followed; utilizes variety of investigative analyses such as signature analysis, static analysis, static malware & media analysis; timeline analysis), performs incident triage to include determining scope, urgency & potential impact & provides technical summary of findings in accordance with established reporting procedures or performs risk assessments to ensure systems are in compliance with applicable standards and frameworks.

&/OR

Develops & enforces all security policies & procedures for personal computers & local area networks & applications.

Serves as technical expert & liaison to law enforcement personnel to explain incident details; provides testimony as needed; uses specialized equipment & techniques to catalog, document extract, collect, package & preserve digital evidence; assists lower-level data security personnel in analysis of new systems & identifying security requirement of new system; coordinates state & federal data processing audits; conducts & administers information security tests; participates in information security risk assessments; reviews authorization & assurance documents to confirm level of risk is within acceptable limits for each software application, system & network.

Deploys and maintains enterprise security systems (e.g., Endpoint protection, IDS, SIEM); supports agencies in the use of these tools; establishment of access levels & monitoring of system performance; serves as liaison with users in & outside of agency.

MAJOR WORKER CHARACTERISTICS:

Knowledge of computer science; systems analysis & design; data security practices & implementation; common adversary tactics, techniques & procedures; data backup, types of backups & recovery concepts & tools; cryptology; encryption methodologies; incident response & handling methodologies; network traffic analysis methods; scripting language programs (e.g., Power Shell, WMI)*; employee training & development*. Skill in operation of personal computer & associated hardware & software; utilization of network analysis tools to identify vulnerabilities. Ability to define problems, collect data, establish facts & draw valid conclusions; read & understand variety of technical material; write program specifications & system documentation; communicate verbally & in writing on technical & non-technical matters; maintain confidentiality of sensitive information; cooperate with co-workers on group projects.

(*)Developed after employment.

MINIMUM CLASS QUALIFICATIONS FOR EMPLOYMENT:

Completion of undergraduate core coursework in computer science; 24 mos. trg. or 24 mos. exp. in computer data security either through monitoring system/network traffic for anomalous activity, systems development or controlling accessibility of data.

-Or 12 mos. exp. as Enterprise Information Security Professional 1, 69981.

-Or equivalent of Minimum Class Qualifications For Employment noted above.

TRAINING AND DEVELOPMENT REQUIRED TO REMAIN IN THE CLASSIFICATION AFTER EMPLOYMENT:

Not applicable.

UNUSUAL WORKING CONDITIONS:

Work involves operation of computer terminal for long periods of time; overtime may be required.

JOB TITLE	JOB CODE	B. U.	EFFECTIVE	PAY GRADE
Enterprise Information Security Supervisor	69985	EX	08/05/2018	16

JOB DUTIES IN ORDER OF IMPORTANCE: (These duties are illustrative only. Incumbents may perform some or all of these duties or other job-related duties as assigned.)
Supervises data security analysts assigned to one work unit, recommends staffing needs & selects personnel, assigns & reviews work, trains staff, establishes work priorities, develops & enforces unit policies & procedures & develops forms, charts &/or, tables for recording & reporting units activities.

Oversees response to identified malicious activity & determines appropriate course of action in response to identified & analyzed anomalous network activity; directs analysis of security issues for new & existing systems to determine appropriate security controls; participates in planning security enhancements; participates in the development of security policies & procedures; oversees the deployment and maintenance or enterprise security tools; evaluates agency's security needs & recommends ways to improve security; prepares written & oral reports for management on technical evaluations; oversees coordination of state & federal data processing audits.

MAJOR WORKER CHARACTERISTICS:
Knowledge of computer science; systems analysis & design; data security practices & implementation; common adversary tactics, techniques & procedures; data backup, types of backups & recovery concepts & tools; cryptology; encryption methodologies; incident response & handling methodologies; network traffic analysis methods; scripting language programs (e.g., Power Shell, WMI)*; supervisory principles & techniques*; employee training & development. Skill in operation of personal computer & associated hardware & software; utilization of network analysis tools to identify vulnerabilities. Ability to define problems, collect data, establish facts & draw valid conclusions; read & understand variety of technical material; write program specifications & system documentation; communicate verbally & in writing on technical & non-technical matters; maintain confidentiality of sensitive information; cooperate with co-workers on group projects.

(*)Developed after employment.

MINIMUM CLASS QUALIFICATIONS FOR EMPLOYMENT:
Completion undergraduate core coursework in computer science; 24 mos. trg. or 24 mos. exp. in computer systems analysis, design & operations or data security involving determination of appropriate access levels for resources & & formulating appropriate access profiles for each application; 12 mos. trg. or 12 mos. exp. in computer project/program management or providing work direction & training to computer personnel engaged in data security or program analysis &/or design.

-Or 12 mos. exp. as Enterprise Information Security Professional 2, 69982.

-Or equivalent of Minimum Class Qualifications For Employment noted above.

TRAINING AND DEVELOPMENT REQUIRED TO REMAIN IN THE CLASSIFICATION AFTER EMPLOYMENT:
Not applicable.

UNUSUAL WORKING CONDITIONS:
Not applicable.

JOB TITLE	JOB CODE	B. U.	EFFECTIVE	PAY GRADE
Enterprise Information Security Manager	69986	EX	08/05/2018	17

JOB DUTIES IN ORDER OF IMPORTANCE: (These duties are illustrative only. Incumbents may perform some or all of these duties or other job-related duties as assigned.)

Manages enterprise risk management, security operation, or privacy program through planning, developing, coordinating & oversees ongoing development & implementation of statewide information & cybersecurity policies, standards, guidelines & procedures to ensure information security capabilities cover current threat capabilities or acts as agency information security officer &, in addition to each preceding option, supervises assigned staff.

Recommends staffing needs & selects personnel, assigns & reviews work, trains staff, establishes work priorities, develops & enforces policies & procedures & develops forms, charts &/or, tables for recording & reporting staff activities, & directs analysis of security issues for new & existing systems to determine appropriate security controls, participates in planning security enhancements, oversees development of security policies & procedures, evaluates agency's security needs & recommends ways to improve security, prepares written & oral reports for management on technical evaluations, & oversees coordination of state & federal data processing audits. Provides technical assistance to systems users & supervisory personnel regarding security procedures; contacts or meets with vendors regarding hardware/software security products or problems.

MAJOR WORKER CHARACTERISTICS:

Knowledge of computer science; systems analysis & design; data security practices & implementation; common adversary tactics, techniques & procedures; data backup, types of backups & recovery concepts & tools; cryptology; encryption methodologies; incident response & handling methodologies; network traffic analysis methods; scripting language programs (e.g., Power Shell, WMI)*; supervisory principles & techniques; employee training & development. Skill in operation of personal computer & associated hardware & software; utilization of network analysis tools to identify vulnerabilties. Ability to define problems, collect data, establish facts & draw valid conclusions; read & understand variety of technical material; write program specifications & system documentationcommunicate verbally & in writing on technical & non-technical matters; maintain confidentiality of sensitive information; cooperate with co-workers on group projects.

(*)Developed after employment.

MINIMUM CLASS QUALIFICATIONS FOR EMPLOYMENT:

Completion of undergraduate core coursework in computer science; 36 mos. trg. or 36 mos. exp. in computer systems analysis, design & operations or data security involving determination of appropriate access levels for resources & & formulating appropriate access profiles for each application; 12 mos. trg. or 12 mos. exp. in computer project/program management or providing work direction & training to computer personnel engaged in data security or program analysis &/or design.

-Or 12 mos. exp. as Enterprise Information Security Supervisor, 69985.

-Or equivalent of Minimum Class Qualifications For Employment noted above.

TRAINING AND DEVELOPMENT REQUIRED TO REMAIN IN THE CLASSIFICATION AFTER EMPLOYMENT:

Not applicable.

UNUSUAL WORKING CONDITIONS:

Not applicable.