STATE OF OREGON
POSITION DESCRIPTION

Position Revised Date:
July 1st, 2025

Agency: The Department of Administrative Services

Division: Office of the State Chief Information Officer

☐ New ☒ Revised

This position is:
☒ Classified
☐ Unclassified
☐ Executive Service
☐ Mgmt Svc – Supervisory
☐ Mgmt Svc – Managerial
☐ Mgmt Svc - Confidential

SECTION 1. POSITION INFORMATION

a. Classification Title:	Information Systems Spec. 7	**b.** Classification No:	C1487
c. Effective Date:		**d.** Position No:	1914876
e. Working Title:	Sr Vulnerability Management Engineer	**f.** Agency No:	10700
g. Section Title:	Cyber Security Services / SOC	**h.** Budget Auth No:	1300730
i. Employee Name:		**j.** Repr. Code:	OAS

k. Work Location (City – County): Salem / Marion

l. Supervisor Name: Leslie DeFoor

m. Position: ☒ Permanent ☐ Seasonal ☐ Limited Duration ☐ Academic Year
☒ Full-Time ☐ Part-Time ☐ Intermittent ☐ Job Share

n. FLSA: ☒ Exempt ☐ Non-Exempt

If Exempt: ☐ Executive ☐ Professional ☒ Administrative

o. Eligible for Overtime: ☐ Yes ☒ No

SECTION 2. PROGRAM AND POSITION INFORMATION

a. Describe the program in which this position exists. Include program purpose, who's affected, size, and scope. Include relationship to agency mission.

The Department of Administrative Services ("DAS") is the central administrative agency that leads state government to implement the policy and budget decisions of the Governor and Oregon Legislature. Employing an enterprise-wide perspective, DAS serves state government by developing and upholding accountability standards to ensure productive and efficient use of state government's financial, human and information resources.

DAS provides a stable management infrastructure and essential business services including technology, financial, procurement, publishing/distribution, human resources and facility asset management. These services support and enable state and local government agencies to carry out their missions, benefiting all Oregonians.

The Office of the Oregon State CIO ("EIS") is a state government-wide information technology (IT) program led by Oregon's Chief Information Officer (CIO). The CIO is a statutory position appointed by the Governor and works closely with the COO and state leadership on adoption of statewide IT policies, standards and governance. EIS has independent statutory authority and is aligned with the DAS budget.

The office is funded by assessment and rates charged for the services provided.

EIS provides centralized oversight for enterprise-wide IT resource management, planning, policy, program development, project delivery and the setting of statewide IT standards. EIS provides training, and direction to ensure IT integrity, security and consistency across state agencies by working closely with elected officials, political subdivisions, state agencies and IT leadership. EIS team is built on collaboration and support. We work together to ensure our customer agencies receive the highest quality of service. We take pride in our work and look for ways to innovate. EIS is committed to hiring highly-skilled, diverse and dedicated employees who will bring a unique skill set to the team. The Office is comprised of the following sections: Data Center Services (DCS), Strategic IT Governance, Cyber Security Services (CSS), and Enterprise Shared Services.

The Cyber Security Services ("CSS") is an information security management section within EIS. It acts as a shared information security resource for the state of Oregon. CSS's mission: Leading Oregon Government to safeguard the State's information resources. CSS is comprised of the following units: Governance Risk and Compliance, Enterprise Security Architecture, Network Security, and Security Operations Center (SOC).

b. Describe the primary purpose of this position, and how it functions within this program. Complete this statement. The primary purpose of this position is to:

advise the CSS SOC Manager and Director on varying levels of cyber security services which the CSS SOC provides to the State of Oregon Executive Agencies, Boards and Commissions.

Through ongoing communications, work with leadership on program development and provide guidance on front line customer support.

Through minimizing complexity and focusing on results, this position will assist in maintaining the enterprise cyber security posture by supporting and maintaining current and future SOC Services.

SECTION 3. DESCRIPTION OF DUTIES

List the major duties of the position. State the percentage of time for each duty. Mark "N" for new duties, "R" for revised duties or "NC" for no change in duties. Indicate whether the duty is an "Essential" (E) or "Non-Essential" (NE) function.

% of Time	N/R/NC	E/NE	DUTIES
25%	R	E	**Customer Assistance** **Software 20%** • Serve as a senior technical resource for Tenable Solution - related support. • Resolve high-impact issues with no established solutions. • Provide training and mentoring to state agency staff on platform usage and best practices. • Guide users with creation of meaningful reports to include Tenable dashboards. • Communicate to the agency support staff for upgrades, maintenance and other outages. **Data 5%** • Provide advanced support to agencies on generating, exporting, and interpreting Tenable vulnerability data and compliance

Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*

			reports. Review and answer data discrepancies between scan results and exported reports • Train users how to create custom reports or dashboards. • Train agency staff on best practices for accessing and utilizing Tenable vulnerability data.
35%	R	E	**Operations** **Software 25%** • Maintain and administer Tenable platforms in the Enterprise production environment. • Troubleshoot complex issues impacting multiple agencies or critical systems, which may not have a known solution. • Coordinate version upgrades, patches, and configuration updates. • Perform tuning and optimization of scan performance and platform stability. **Data 10%** • Monitor and maintain performance and health of distributed databases, ensuring timely availability of vulnerability data across multiple agencies and networks. • Implement and maintain backup, recovery, and data protection processes for vulnerability data repositories. • Coordinate and troubleshoot data replication and synchronization among multiple diverse environments. • Develop and maintain processes for data quality control, ensuring accuracy and consistency of vulnerability records across systems and reports. • Manage version control and compatibility of vulnerability data schemas when upgrading platform components or integrating with other systems. • Evaluate and recommend data storage strategies and performance improvements, considering scalability, retention policies, and compliance mandates.
15%	R	E	**Construction** **Software 10%** • Be aware of industry standard changes and assist with implementing new features for Tenable within the state platform • Devlop plans for platform enhancements, capacity, and improvements while monitoring enterprise performance. **Data 5%** • Ability to develop logical data models to integrate into Tenable and enterprise reporting • Lead implantations of new data connectors to automate ingestion and aggregation of vulnerability data across multiple repositories • Develop and maintain detailed and accurate data flow diagrams along with physical diagrams of the enterprise Tenable system. • Coordinate with vendor to provide support to third party integrators of new data integrations

20%	R	E	**Planning** **Software 10%** • Evaluate new vulnerability management capabilities for suitability within existing frameworks and provide recommendations. • Recommend process improvements to align with compliance requirements. • Evaluate new or existing applications to enhance the state's vulnerability management program. • Plan for enhancements and expansion to the vulnerability management program. **Data 10%** • Research, recommend and develop plans for statewide collection, storage, and retention of vulnerability data. • Research and recommend improvements on how vulnerability information is shared with agencies and integrated with compliance tools • Lead strategic initiatives to improve vulnerability data security, access controls and compliance alignment with CJIS, IRS 1075 and HIPPA. • Monitor and analyze data growth trends for appropriate time to expand. • Design and maintain reporting and dashboard solutions using vulnerability data including data received from federal partners. • Establish reporting templates and processes to meet agency and compliance needs.
5%	NC	NE	Other duties as assigned.
100%			

SECTION 4. WORKING CONDITIONS

Describe any on-going working conditions. Include any physical, sensory, and environmental demands. State the frequency of exposure to these conditions.

This position will spend large amounts of time utilizing computer equipment, computer monitors, typing and viewing data on electronic screens.

This position can spend large amounts of time sitting or standing in one place while performing tasks.

This position works in a very distractive environment and requires the ability to shift tasks and focus often.

This position is suitable for remote work options.

Duties are performed in an office environment working at a computer terminal for long periods of time, working in or around noisy machinery.

Business needs may require working irregular hours or shift work (24/7, weekends, evenings, holidays, and travel for job related purposes) in order to do work or make changes or maintenance that are not approved to be done during the hours of 6am – 6pm.

Business needs may require re-assignment to one of three shifts (days, swing or graveyard) and with short notice.

Driver's license is required or satisfactory means of transportation.

SECTION 5. GUIDELINES

a. List any established guidelines used in this position, such as state or federal laws or regulations, policies, manuals, or desk procedures.

This position is designated as an "Essential Position" (State Policy #60.015.01) in all cases of official state office closures. The incumbent in this position is required to report to work in all cases of official notification of state office closures.

Exceptions: previously approved vacation and absences. This position may be assigned tasks outside the normal position duties to respond to the special conditions of the closures. If reporting to your normal work location is deemed too dangerous, then you must contact your supervisor to be reassigned to an alternate and/or remote location.

Oregon Revised Statutes

- Oregon Administrative Rules
- Department of Administrative Services Policies and Procedures
- Enterprise Information Security Strategy
- EIS Strategic and Section Plans
- Statewide Information Security Plan & Standards
- NIST SP 800-53 R5 Security and Privacy Controls
- NIST SP 800-30 Risk Management Guide for Information Technology Systems
- NIST SP 800-37 Guide for Applying the Risk Management Framework
- All Other Applicable Statewide, DAS, and EIS Policies, Procedures and Standards
- Federal and State government regulations including:
    - Criminal Justice Information Services (CJIS)
    - Federal Information System Management Requirements (FISMA)
    - IRS Publication 1075
    - HIPAA Security and Privacy Rules
    - Oregon Consumer Information Protection Act
- Other Best Practices Resources, such as ISO 27000 series, Common Criteria, National Institute for Standards and Technology (NIST SP-800 series), CIS Controls, etc

b. How are these guidelines used?

The above guidelines provide general guidance and policy directions, and a framework that should be applied as necessary for each application. This includes decisions concerning the appropriate application and interpretation of policies and procedures that relate to highly sensitive confidential information.

They are used to determine correct operational procedures necessary for efficient and secure operation of statewide computer systems including work processes and procedures that ensure consistent quality of services.

SECTION 6. WORK CONTACTS

With whom, outside of co-workers in this work unit, must the employee in this position regularly come in contact?

Who Contacted	How	Purpose	How Often?
Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*			
Agency Customers	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Managers/co-workers	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Vendors	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries, coordination	Daily
Other State Employees	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily

SECTION 7. POSITION RELATED DECISION MAKING

Describe the typical decisions of this position. Explain the direct effect of these decisions.

Determine how to prioritize and schedule vulnerability scans across multiple agencies when resources are constrained.

Decide how to configure scan policies, credentials, and tuning options to balance accuracy with impact on production systems.

Select appropriate remediation workflows when scan results conflict with business needs.

Determine the best way to resolve complex support issues with no established solution (e.g., data corruption, large-scale scan failures).

Evaluate whether an agency's use of Tenable aligns with security and compliance expectations, and recommend adjustments.

Decide when and how to escalate incidents to vendors or internal leadership.

This position must exercise discretion and independent judgement in making decisions and resolving cyber threat findings or vulnerabilities within the state security operations center.

This position must know when to escalate cyber threat findings with agencies following policies and procedures within the State and Cyber Security Services.

This position will make decisions based on system reporting to assist agencies in deciding priorities within the scope of vulnerabilities.

This position may act independently but will consult with management before any final actions are taken.

Decisions and directions by this position will directly affect major functions within agencies and the enterprise cyber security program which could result in serious effects on over all agency technology utilization.

SECTION 8. REVIEW OF WORK

Who reviews the work of the position?

Classification Title	Position Number	How	How Often	Purpose of Review
IT Cyber Security Manager 2	1970060	In person, phone, email, by letter or electronic means	Daily/Weekly	To determine if corrective actions or directions are needed. To stay informed of active threats.
IT Cyber Security Manager 2	1970060	In person, phone, email, by letter or electronic means	Quarterly	Performance Accountability Feedback

SECTION 9. OVERSIGHT FUNCTIONS THIS SECTION IS FOR SUPERVISORY POSITIONS ONLY

a. How many employees are directly supervised by this position? N/A

How many employees are supervised through a subordinate supervisor? 0

b. Which of the following activities does this position do?

- ☐ Plan work
- ☐ Assigns work
- ☐ Approves work
- ☐ Responds to grievances
- ☐ Disciplines and rewards
- ☐ Coordinates schedules
- ☐ Hires and discharges
- ☐ Recommends hiring
- ☐ Gives input for performance evaluations
- ☐ Prepares & signs performance evaluations

SECTION 10. ADDITIONAL POSITION-RELATED INFORMATION

ADDITIONAL REQUIREMENTS: List any knowledge and skills needed at time of hire that are not already required in the classification specification:

This position is subject to a criminal records check, which may require fingerprints. If you are offered employment, the offer will be contingent upon the outcome of a criminal records check (FBI). Any history of criminal activity will be reviewed and could result in the withdrawal of the offer or termination of employment.

You are responsible to promote and foster a diverse and discrimination/harassment-free workplace; establish and maintain professional and collaborative working relationships with all contacts; contribute to a positive, respectful and productive work environment; maintain regular and punctual attendance; perform all duties in a safe manner; and comply with all policies and procedures. Working in a team oriented environment requires participative decision making and cooperative interactions among staff and management. You are to be aware of Affirmative Action and the department's Diversity strategies and goals.

Additional skills, abilities and requirements:

Technical

- Strong understanding of vulnerability management concepts, processes, and tools used to investigate and remediate security issues.
- Experience interpreting vulnerability scan results and advising technical teams on appropriate remediation steps.

- Deep knowledge of TCP/IP networking, firewalls, and standard network protocols and architecture.
- Familiarity with secure configuration baselines and hardening guides such as CIS Benchmarks.
- Knowledge of industry-standard security frameworks, including CIS Controls, NIST Cybersecurity Framework, and ISO 27001.
- Knowledge of Vulnerability Management Platforms, specifically Tenable (Tenable ONE, Tenable.io, Tenable.sc) and Microsoft Defender Vulnerability Management.
- Experience with Windows and Linux/Unix operating systems in enterprise environments.
- Experience working with cloud infrastructure and container technologies (e.g., AWS, Azure, Docker).
- Experience with Active Directory, both on-premises and hybrid/cloud integrations.
- Knowledge of Microsoft Entra (Azure AD) and Microsoft 365 security and compliance portals.
- Familiarity with SIEM solutions and integrating vulnerability data into enterprise monitoring systems.
- Understanding of relational and distributed data systems, data retention, and reporting processes.

Problem Solving

- Must be capable of approaching problems logically and systematically.
- Must have the ability to quickly grasp new concepts and techniques and apply them in different scenarios.
- Requires strong technical and analytical skills demonstrated in complex or secure environments.
- Ability to troubleshoot multi-layered technical issues involving systems, networks, and data integrations.
- Skill in analyzing and interpreting complex vulnerability data sets.

Interpersonal and Communication

- Ability to explain complex cybersecurity issues to non-technical stakeholders.
- Proven skill in establishing and maintaining effective working relationships across teams and agencies.
- Ability to schedule and manage multiple tasks concurrently to meet tight deadlines.

BUDGET AUTHORITY: If this position has authority to commit agency operating money, indicate the following:

Operating Area	Biennial Amount ($00000.00)	Fund Type
Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*		
N/A	N/A	N/A

SECTION 11. ORGANIZATIONAL CHART

Attach a current organizational chart. Be sure the following information is shown on the chart for each position: classification title, classification number, salary range, employee name and position number.

SECTION 12. SIGNATURES

Employee Signature	Date	Supervisor Signature	Date

Appointing Authority Signature	Date