



STATE OF OREGON
Oregon Health Authority (OHA)
POSITION DESCRIPTION

Position Revised Date:

This position is:

- ☒ **Classified**
☐ **Unclassified**
☐ Executive Service
☐ Mgmt Svc – Supervisory
☐ Mgmt Svc – Managerial
☐ Mgmt Svc – Confidential

Agency: Oregon Health Authority

Division: Agency Operations Division

☐ New ☐ Revised

SECTION 1. POSITION INFORMATION

- a. Classification Title: Information Systems Specialist 8
- b. Classification No: C1488 c. REPR Code: _____
- d. Position No: _____
- e. Working Title: Senior Cyber Compliance Specialist
- f. Agency No: 44300
- g. Section Title: Information Security and Privacy Office
- h. Employee Name: _____
- i. Work Location (City — County): Salem, OR – Marion County
- j. Supervisor Name: _____
- k. Position: ☒ Permanent ☐ Seasonal ☐ Limited Duration ☐ Academic Year
☐ Full-Time ☐ Part-Time ☐ Intermittent ☐ Job Share
- l. FLSA: ☒ Exempt If Exempt: ☐ Executive ☒ Professional ☐ Administrative ☐ Computer
☐ Non-Exempt
- m. 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.

OHA values health equity, service excellence, integrity, leadership, partnership, innovation, and transparency. OHA's health equity definition is "Oregon will have established a health system that creates health equity when all people can reach their full potential and well-being and are not disadvantaged by their race, ethnicity, language, disability, age, gender, gender identity, sexual orientation, social class, intersections among these communities or identities, or other socially determined circumstances. Achieving health equity requires the ongoing collaboration of all

regions and sectors of the state, including tribal governments to address: the equitable distribution or redistribution of resources and power; and recognizing, reconciling, and rectifying historical and contemporary injustices.” OHA’s 10-year goal is to eliminate health inequities.

The Agency Operations Division is aligned with the Oregon Health Authority’s core values of partnership, service excellence, leadership, integrity, health equity, innovation, and transparency. In our practice, these values are expressed through:

Service Excellence:

- Understanding and responding to Oregon public health needs and the people we serve
- Pursuing our commitment to innovation and science-based best practices
- Fostering a culture of continuous improvement

Leadership:

- Building agency-wide and community-wide opportunities for collaboration
- Championing public health expertise and best practices
- Creating opportunities for individual development and leadership

Integrity:

- Working honestly and ethically in our obligation to fulfill our public health mission
- Ensuring responsible stewardship in public health resources

Health Equity:

- Eliminating health disparities and working to attain the highest level of health for all people
- Ensuring the quality, affordability, and accessibility of health services for all Oregonians
- Integrating social justice, social determinants of health, diversity, and community

Partnership:

- Working with partners and communities to protect and promote the health of all Oregonians
- Seeking, learning from, and respecting internal and external ideas and opinions
- Exploring and defining the roles and responsibility of public health staff and partners

Innovation:

- We are not satisfied with the status quo if there are new and better ways to meet the needs of the people we serve. We bring creativity, experience, and openness to our search for solutions to problems. We pursue opportunities to develop new evidence to evolve our practices.

Transparency:

- We communicate honestly and openly, and our actions are upfront and visible. We provide open access to information and meaningful opportunities to provide input and participate in our decision-making.

The Office of Information Services (OIS) provides shared technology services that support the work of two agencies—the Oregon Health Authority (OHA) and the Oregon Department of Human Services (ODHS). OIS delivers and maintains the systems and tools that enable staff and partners across the state to carry out essential programs and services. These include determining eligibility for benefits; administering medical, housing, food, and employment assistance; supporting behavioral health and rehabilitative services; protecting children, older adults, and people with disabilities; processing claims and benefits; managing provider licensing and state hospital systems; and promoting and protecting public health. OIS also supports internal administrative functions such as human resources, financial management, and procurement.

OIS supports more than 250 business-facing applications used by approximately 17,000 agency and partner staff located across 166 sites throughout Oregon. In addition to supporting agency staff, OIS provides technology services to a wide network of partners who rely on OHA and ODHS systems to serve their communities. OIS ensures the reliability, security, and accessibility of these systems through service desk support, ongoing system maintenance, and coordination of network and computing operations. The office also supports technology strategy and delivery through project management, systems architecture, database administration, and IT asset and change management.

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:

The primary purpose of a Senior Cyber Compliance Specialist position is to play a crucial role in an OHA/ODHS IT security program by managing and securing IT assets such as desktops, laptops, servers, virtual and on-premises platforms and mobile devices. This position combines information technical expertise with customer service skills to ensure the protection of agency information assets, while also addressing agency security requirements supporting business operations and customer needs.

IT Security Management: The Senior Cyber Compliance Specialist is responsible for developing, implementing, and maintaining security solutions that align with state and federal requirements that enable business units to meet their statutory mandates. The role focuses on enhancing IT security for the agencies by implementing best practices, policies, and standards. The Senior Cyber Compliance Specialist ensures that IT assets are configured to meet security requirements based on the Center for Internet Security and National Institute of Standards (NIST) and Information Technology frameworks including adherence to Center for Internet Security (CIS) benchmarks and IT industry standards.

Incident Response: In the event of IT security events, incidents or breaches, the Senior Cyber Compliance Specialist plays a critical role in responding to and mitigating the impact on agency IT assets. This involves investigating events, incidents, identifying compromised assets, and taking remedial actions to contain and eradicate threats.

Vulnerability Management: The position assists in identifying and remediating vulnerabilities on IT Assets ensuring that all software and hardware are up to date with the latest security patches and firmware

Policy Compliance: The Senior Cyber Compliance Specialist advises on the development of information protection and IT security policies and enforces the policies to ensure both agencies are compliant with state and federal requirements in delivering secure and protected IT assets in support of business unit functions.

Security Monitoring and Alerting: This position will ensure continuous monitoring strategies are in place for each system/platform, work with Enterprise Information Services (EIS) Cyber Security Services (CSS) Security Operations Center (SOC) for suspicious activity, unauthorized access, or potential security incidents. The Senior Cyber Compliance Specialist responds to security alerts, conducts investigations, and escalates incidents as necessary to ensure compromised IT assets are contained, Isolated, and incidents are eradicated from the network.

Documenting and Reporting: Accurate and up-to-date documentation is essential in IT security. The Senior Cyber Compliance Specialist maintains records of security events and incidents, vulnerabilities, and remediation efforts. They also generate reports to provide insights to management and demonstrate compliance with IT security standards and regulations.

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.

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

% of Time	N/R/NC	E/NE	DUTIES
25%	N	E	Cyber Protection Analysis - Lead research, standards development, and architectural design to support secure technologies, processes, and infrastructure aligned with CIS and NIST frameworks. - Collaborate with business units and application teams to define and implement secure configurations and drive continuous improvement of IT assets. - Develop implementation and migration plans that support the agency’s IT security strategy and require coordination across vendors and jurisdictions. - Create strategic roadmaps to address identified security gaps and guide security configuration and controls implementation across all agency assets. - Ensure effective transition from current to future state and maintain continuous monitoring to strengthen the agency’s security posture.
25%	N	E	Cyber Protection Construction - Analyze integration requirements to ensure IT security controls, standards, and operational processes are aligned; document assumptions and transition approved work to supporting operations teams. - Support the selection and implementation of IT asset protections, encryption mechanisms, and related security controls to maintain strong baseline defense and threat response capabilities. - Collaborate with business and technical teams to identify and define security requirements for integrating and enhancing IT assets, identity, and access management solutions. - Provide design, deployment, and operational guidance for enterprise security technologies to ensure consistent and effective implementation of control. - Partner with architects, project managers, infrastructure teams, and application teams to maintain secure and standardized account lifecycle management practices. - Contribute to developing IT security strategies for web and mobile applications, including device security standards,

			registration, provisioning, access control, and secure integration methods across modern application environments.
15%	N	E	Security Incident Response Management • Lead and coordinate all aspects of IT security event and incident response for both agencies, ensuring timely detection, triage, containment, eradication, and recovery. • Establish and maintain standardized incident response processes, playbooks, and escalation paths aligned with recognized IT security frameworks and agency requirements. • Direct cross-functional response teams during security events, providing authoritative guidance and high-confidence decision-making under pressure. • Oversee continuous monitoring practices to identify emerging threats, validate alerts, and reduce response time across both agencies' environments. • Report to the primary incident commander for major security incidents, ensuring effective communication, documentation, and executive-level reporting. • Conduct post-incident reviews to identify root causes, define corrective actions, and drive long-term improvements in security operations and resilience. • Develop and deliver incident response training and tabletop exercises to strengthen readiness and coordination across technical and business teams. • Collaborate with external partners, vendors, and government entities as needed to coordinate multi-agency or multi-jurisdictional incident response efforts. • Maintain threat awareness and ensure that incident response capabilities evolve with changing risks, technologies, and regulatory requirements.
15%	N	E	Customer Service and Professional Conduct • Provides operational and technical support for upgrades, modifications, maintenance, and tuning for systems hardware and software in accordance with established policies, procedures, and schedules. • Works collaboratively with internal employees, vendors, operations and management staff of OIS, consultants, and the state data center to effectively implement solutions. • Fosters and sustain customer service relationships, customer assistance, provides training, and technical help to systems, a variety of agencies, business partners and agency users. • Work with software vendors and other OIS groups for problem resolution and technical support purposes.

			• Responsible for the ongoing operation and maintenance of applications for the assigned IT functional areas, including the definition and monitoring of the measures to ensure system availability. • Responsible for the effective and efficient provision of level incident support, change management, and maintaining the upkeep of technical records and documentation. • Proactively communicates the status of ongoing daily support and problem resolution. Ensures effective problem analysis and resolution of issues of complex scope in a timely fashion and escalates issues when needed to appropriate levels of IT or Business. • Analyzes system performance and addresses performance problems while evaluating costs, specifications, and organizational policies for system performance tuning recommendations. • Responds to customer requests for complex access needs, may provision accounts.
Ongoing	NC	NE	Cultural Competence • Promote and foster a diverse workforce and discrimination/harassment-free workplace. • Recognize value of individual and cultural differences; create work environment where individual differences are valued. • Consistently treat customers, partners, co-workers with dignity and respect. • Value diverse viewpoints. Core Values • Demonstrate awareness, understanding and alignment with OHA Core Values of Service Excellence, Leadership, Integrity, Health Equity, Partnership and Innovation. Customer Service • Consistently treat customers, partners, vendors and co-workers with dignity and respect. • Maintain a work environment that is respectful and accepting of diversity; model expected office professional behaviors.

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.

The location of this position is in an office, cubicle and/or an agreed upon remote work environment with significant use of a computer and video conferencing.

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:

The person in this position should have a working knowledge of the agency rules, policies and programs as outlined in the OIS Employee Handbook; Oregon Revised Statutes (ORS) and Oregon Administrative Rules (OAR) related to OHA; and the policies and processes specific to these systems.

National Institute for Standard and Technology (NIST) Special Publications:

SP800-30 Revision 1 Guide for Conducting Risk Assessments

SP800-37 Revision 1 Guide for Applying the Risk management Framework to Federal Information Systems: A Security Life Cycle Approach

SP800-39 Managing Information Security Risk: Organization, Mission, and Information System

SP800-53 Rev. 5 Security and Privacy Controls for Information System and Organizations

NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0

Federal Information System Management Requirements (FISMA)

IRS Publication 1075

HIPAA Privacy and Security Rules

CFR 95-621 Automatic Data Processing

Oregon Consumer Identity Theft Protection Act

OHA|ODHS Security and Privacy Policies

Center of Internet Security (CIS) Controls

MARS-E

PMI PMBOK

CJIS Security Policy

Regarding CJIS:

Criminal Justice Information Services (CJIS) Policy

Federal Information Processing Standards (FIPS) Publication (Pub) 199

Federal Information Processing Standards (FIPS) Publication 200

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

MARS-E Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5

NIST SP 800-88

Social Security Administration Information Exchange Security Requirements and Procedures

Other federal and state laws, rules and regulations governing data privacy and security

Oregon Administrative Rules

Oregon Revised Statutes

Statewide Cyber Security Standards

Department of Administrative Services (DAS) rules, policies, and procedures

Department, Authority and program rules, policies, and procedures

b. How are these guidelines used?

All policies, rules and guidelines must be used when accessing, analyzing or sharing information regarding the Information Security and Privacy Office. These guidelines are used for providing information to the public, and to employees of both agencies.

These guidelines set standards for performance, provide direction, procedural information and

specific mandates (laws and policies) and outline criteria for the program, services and business practices. Knowledge of them allows the employee to provide accurate information.

Regarding CJIS (as cited in 5a):

Serve as a basis for making judicious assessments and decisions regarding the privacy and security posture and configurations of networks, systems, and data.

SECTION 6. WORK CONTACTS

With whom, outside of co-workers in this work unit, must the employee in this position regularly come in contact? When applicable, please identify contacts that might be virtual/ in-person, or both.

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

Who Contacted	How	Purpose	How Often?
OIS Management	Phone/Person/email/in writing/in meetings	Consult/advise/recommend and provide information	Daily
Agencies' committees	Phone/Person/email/in writing/in meetings	Updates/status reports/issue resolution/decision making	Monthly
Key Staff & Partners (Agency & External)	Verbal & Written	Determine system requirements and proposed solutions	Daily/Weekly
Other OIS groups and vendors	Verbal, Written, Presentations	Status, Issue Resolution	Daily/Weekly
Agency Managers/Staff	Meetings/Phone	Provide updates and recommendations on security controls and continuous monitoring strategy	2x Weekly
Enterprise Information Services (EIS)	Meetings/Written/Phone	Collaborate: Enterprise Security Operations Center, Cyber Security Services and Data Center Services for security solutions and implementation requirements.	Monthly/ Quarterly

SECTION 7. POSITION-RELATED DECISION MAKING

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

Person in this position will be involved in decision making that impacts both agencies on policies, process, state rule and laws, and service delivery to clients. These decisions impact both staff and clients of the agencies.

The Senior Cyber Compliance Specialist is expected to anticipate problems and take the initiative to propose and recommend preventative actions.

The Senior Cyber Compliance Specialist provides support in addressing information security events, incidents, complaints, and concerns, and offers guidance on appropriate next steps and potential corrective actions.

Ability to be cleared by the FBI Criminal Justice Information Services (CJIS) and Oregon State Police through a fingerprint-based criminal background check for access to criminal justice information (CJI).

Must be able to pass CJIS training and testing to CJIS Level 4 rating.

SECTION 8. REVIEW OF WORK

Who reviews the work of the position?

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

Classification Title	Position Number	How	How Often	Purpose of Review
ITM3 Sr. IT Regulatory Compliance Manager	0003008	In person, verbal, written, meetings, phone, email	When needed	Review work, schedules, discuss risk decisions and ensure risk documentation adheres to ODHS/OHA standards. Work may be reviewed for competency, accuracy, timeliness and conformance to policies and procedures.
ITA1 Director of ISPO	0003030	In person, written, electronically	As needed	Program oversight.

SECTION 9. OVERSIGHT FUNCTIONS (*Supervisory positions only*)

- a. How many employees are directly supervised by this position? _____
How many employees are supervised through a subordinate supervisor? _____
- b. Which of the following activities does this position do?
- | | |
|--|---|
| ☐ Plan work | ☐ Coordinates schedules |
| ☐ Assigns work | ☐ Hires and discharges |
| ☐ Approves work | ☐ Recommends hiring |
| ☐ Responds to grievances | ☐ Gives input for performance evaluations |
| ☐ Disciplines and rewards | ☐ Prepares and 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.

All positions in OHA require a Criminal Background Check and an Abuse/Neglect Check. Fingerprints may be required.

Successful completion of one of the following certifications or willingness to obtain one within 12 months of hire: (a) Certified Information Systems Security Professional (CISSP) OR (b) Certified Information Security Manager (CISM)

Experience using management strategies and techniques to lead information security technical and program professionals.

Experience working under federal, state and agency regulations and guidelines related to information security and protection from unauthorized disclosure of individually identified information.

Experience with data governance and managing regulated data.

Ability to translate technical issues and concepts to non-technical audience.

Knowledge of the ODHS and OHA programs and other related government programs.

Previous Project Management experience.

Excellent written and verbal communication and presentation skills.

Experience working with diverse groups with varying priorities and goals and moving those groups toward consensus.

Knowledge Preferred:

Proficiency in Microsoft Defender including knowledge of threat protection, endpoint security, and advanced threat analytics.

Encryption: Understanding of encryption technologies for data protection in transit and at rest.

Operating Systems: Strong knowledge of Windows operating systems and security features.

Experience in Secure Risk Management Frameworks and Standards with Center for Internet Security version 8, National Institute of Standards and Technology, Special Publications, 800-30, 800-37. 800-39. 800-53 at a minimum.

Understanding of cybersecurity frameworks, standards, and regulations, such as GDPR, HIPAA, and ISO 27001.

Network Security: Basic knowledge of network security principles, protocols, and technologies, especially in the context of Azure and cloud environments.

Vulnerability Management: Understanding of vulnerability assessment tools and processes for identifying and mitigating security weaknesses.

Incident Response Management: Proficiency in incident response procedures, including containment, eradication, and recovery processes, with a focus on Azure and Microsoft environments.

Knowledge:

Azure and Active Directory: Deep understanding of Azure Active Directory (Azure AD) and on-premises Active Directory, including user management, group policies, and directory synchronization.

Microsoft Defender: Proficiency in Microsoft Defender for Endpoint, including knowledge of threat protection, endpoint security, and advanced threat analytics.

Microsoft BitLocker Encryption: Understanding of BitLocker and disk encryption technologies for data protection at rest.

Intune: In-depth knowledge of Microsoft Intune Endpoint Security Configuration.

Endpoint Security Solutions: Familiarity with endpoint security software and solutions, including Microsoft Defender and other relevant security tools.

Operating Systems: Strong knowledge of Windows operating systems and security features.

Skills Desired:

Microsoft Defender Configuration: Ability to configure, manage, and fine-tune Microsoft Defender for Endpoint to optimize threat detection and response.

IT Asset Hardening: Skill in hardening IT asset devices for improved security, including Group Policy management and configuration.

Security Incident Handling: Capability to respond effectively to security incidents and analyze logs and telemetry data from Azure and Microsoft Defender.

Analytical Thinking: Strong analytical skills for assessing security risks and identifying anomalies in endpoint security within Azure and Microsoft environments.

Documentation and Reporting: Ability to document security incidents, vulnerabilities, and remediation efforts and generate reports for management and compliance purposes.

Scripting and Automation: Knowledge of scripting and automation tools, such as PowerShell, for automating security tasks and processes in Azure and Microsoft environments.

Collaboration: Effective communication and collaboration skills to work with cross-functional teams, including IT, helpdesk, and management, while focusing on Microsoft technologies.

Policy Development: Skill in creating and enforcing security policies and standards aligned with Industry standards.

Forensics: Familiarity with digital forensics tools and methodologies for investigating security incidents in Azure and Microsoft environments.

Continuous Learning: A commitment to staying up-to-date with the latest information security and privacy compliance strategies, and best practices.

Adaptability: The capacity to adapt to evolving Azure, Microsoft Defender, and Intune technologies and security challenges.

Vendor and Threat Intelligence: Awareness in specific threat intelligence feeds and vendor data for proactive security measures

Leadership: Leadership skills are essential for guiding security initiatives and fostering a security-conscious culture within OIS, ODHS and OHA agency partners.

Regarding CJIS:

Ability to be cleared by the FBI Criminal Justice Information Services (CJIS) and Oregon State Police through a fingerprint-based criminal background check for access to criminal justice information (CJI).

Must be able to pass CJIS training and testing to CJIS Level 4 rating.

Requires a successful OHA background check, including a fingerprint-based national background check and abuse/neglect check.

BUDGET AUTHORITY: If this position has authority to commit agency operating money, indicate the following: <i>Note: If additional rows of the below table are needed, place cursor at end of a row (outside table) and hit "Enter".</i>		
Operating Area	Biennial Amount (\$00,000.00)	Fund Type

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