

Job Description Chief Information Security Officer

DEPARTMENT:	Information Technology & Security	REPORTS TO:	Chief Technology Officer
TITLE CODE:	8042MR	DATE:	7/22/2025
POSITION CODE:	TBD	ADMINISTRATIVE REVISION:	

Job Summary

Under administrative direction, the Chief Information Security Officer (CISO) is responsible for establishing and leading the enterprise-wide strategy and vision for information security across the Orange County Employees Retirement System (OCERS). This executive-level role ensures the confidentiality, integrity, and availability of digital assets, data, and IT infrastructure by proactively assessing threats, setting strategic direction, and implementing robust security frameworks and architectures. The CISO is a trusted advisor to the executive leadership team and the Board of Retirement on cybersecurity risk and compliance matters and is the agency's primary authority on information security.

Distinguishing Characteristics

The Chief Information Security Officer is an executive-level position that reports directly to the Chief Technology Officer and serves as a key executive leadership team member. This position is responsible for the oversight, development, implementation, and maintenance of OCERS' information security strategy and governance framework. The CISO leads cross-functional efforts to assess risk, ensure compliance with industry standards, and protect the agency's mission-critical systems, sensitive member data, and confidential financial information.

This role requires an accomplished leader with strategic foresight, deep cybersecurity acumen, and the ability to navigate and influence at the highest levels. The CISO builds collaborative relationships across business units, drives cultural change regarding cybersecurity awareness, and leads the agency in responding to emerging threats in an ever-evolving threat landscape.

Performance Attributes

Include but are not limited to the following:

- ▶ Lead the development, implementation, and continuous improvement of a long-term, risk-based cybersecurity strategy aligned with OCERS' mission, vision, values, and business goals.
- ▶ Serve as the agency's executive authority on cybersecurity matters, providing strategic guidance to the Board of Retirement, executive leadership, and other stakeholders.
- ▶ Build and oversee a governance structure that includes policies, standards, guidelines, and procedures that align with industry frameworks (e.g., NIST, ISO, COBIT).
- ▶ Direct enterprise-wide security risk assessments, gap analyses, and audits, ensuring the timely mitigation of identified vulnerabilities and risks.
- ▶ Lead the creation, implementation, and testing of the enterprise Cybersecurity Incident Response Plan (CSIRP), and oversee forensics, investigations, and post-incident reviews.

Job Description

Chief Information Security Officer

- ▶ Oversee compliance efforts related to privacy, regulatory mandates, and cybersecurity frameworks.
- ▶ Foster a cybersecurity-aware culture across all levels of the organization through ongoing education, training, and communication strategies.
- ▶ Direct the implementation of advanced security technologies, including threat intelligence platforms, security orchestration, and automated response tools.
- ▶ Actively monitor the external threat landscape and anticipate shifts in regulatory or operational risks to proactively safeguard OCERS' infrastructure.
- ▶ Lead the security architecture function, ensuring that all new and existing systems are designed with appropriate security controls and protocols.
- ▶ Develop, mentor, and retain top cybersecurity talent and manage vendor and third-party relationships to ensure delivery of critical security services.
- ▶ Collaborate with IT and business leadership to integrate cybersecurity into enterprise projects, digital transformation efforts, and vendor procurements.
- ▶ Prepare and present cybersecurity updates, threat intelligence briefings, and annual security reports to executive leadership and the Board.
- ▶ Develop and manage the cybersecurity division's annual strategic plan and operating budget.

Minimum Qualifications

Education and Experience

- ▶ Bachelor's degree in Computer Science, Information Systems, Cybersecurity, or a related field; Master's degree (MS, MBA, MPA) highly desirable.
- ▶ Ten (10) years of progressively responsible experience in cybersecurity and information technology, including at least five (5) years in a senior leadership or executive-level role.
- ▶ Proven experience in designing and managing enterprise-wide security programs, policies, and risk mitigation initiatives.
- ▶ Demonstrated expertise in compliance, data privacy laws, risk management, incident response, and security frameworks.

Special Notes, Licenses or Requirements

- ▶ Professional information certifications such as:
 - Certified Information Systems Security Professional (CISSP),
 - Certified Information Systems Auditor (CISA)
 - Certified Information Security Manager (CISM)
 - Similar industry certifications
- ▶ Extensive knowledge of industry standards and best practices (NIST, ISO 27001/27002, COBIT, SOC 2, OWASP).
- ▶ Proven ability to build and maintain strong relationships with executive stakeholders, Board

members, and regulators.

Knowledge/Skills/Abilities

Sample KSA's necessary to perform essential duties of the position:

KNOWLEDGE

- ▶ Executive-level leadership, strategic planning, and governance practices.
- ▶ Enterprise risk management methodologies and cybersecurity frameworks.
- ▶ Emerging technologies (e.g., AI, blockchain, zero trust) and their cybersecurity implications.
- ▶ Security architecture and engineering, cloud security, endpoint protection, and encryption standards.
- ▶ Business continuity and disaster recovery planning.
- ▶ Regulatory requirements impacting public pension systems and government agencies.
- ▶ Procurement and contract negotiation for security technologies and services.

SKILLS/ABILITIES

- ▶ Plan, organize, and manage cyber security infrastructure development, operations, and support for OCERS.
- ▶ Communicate complex security concepts clearly to both technical and non-technical audiences.
- ▶ Inspire, manage, and grow a high-performing cybersecurity team.
- ▶ Build an enterprise security architecture aligned with business, IT, and OCERS' strategy.
- ▶ Develop policies and practices that balance security with operational efficiency.
- ▶ Remain calm under pressure and make decisions during high-impact incidents.
- ▶ Manage and prioritize multiple projects while maintaining a high standard of professionalism, confidentiality, and ethical conduct.
- ▶ Exercise sound judgment, maintain confidentiality, and act with integrity and professionalism.

Physical, Mental and Environmental Conditions

The following is a description of the physical and mental abilities that are customarily required to perform the essential job functions of this position.

PHYSICAL AND MENTAL REQUIREMENTS

- ▶ Ability to communicate clearly and understandably in person and over the telephone, both one-on-one and in small groups.
- ▶ Ability to operate a telephone, keyboard, computer, and calculator.
- ▶ Ability to interact professionally with members of the Investment Committee, employers,

Job Description **Chief Information Security Officer**

peers, and consultants.

- ▶ Ability to access a standard office environment.
- ▶ Ability to sit for prolonged periods of time.

ENVIRONMENTAL CONDITIONS

- ▶ The primary workplace is in an office environment with standard office equipment.
- ▶ Peripheral office equipment generates a quiet to moderate noise level.
- ▶ The work environment may include interaction with elected officials, non-elected officials, government agencies, community interest groups, and the general public in the development and coordination of OCERS' affairs.
- ▶ Out of area travel will be required to attend professional conferences, investment due diligence meetings, and other meetings.

Job Description
Chief Information
Security Officer

Acknowledgement

By signing below, I acknowledge that I have reviewed and discussed the contents, requirements, and expectations included in this job description with my supervisor and a copy has been provided to me.

Employee Signature

Date

Supervisor Signature

Date

Reviewer Signature

Date