POSITION DESCRIPTION

Title:	Senior Cybersecurity Engineer
Department:	Communications & Information Systems
Job Analysis:	August 2026

Note: Statements included in this description are intended to reflect in general the duties and responsibilities of this classification and are not to be interpreted as being all inclusive. The employee may be assigned other duties that are not specifically included.

Relationships

Reports To:	Assistant CIS Director, CIS Director
Subordinate Staff:	None
Internal Contacts:	Commissioners, County Administrator, Department Heads, All Other County Staff
External Contacts:	Vendors, Representatives from other Agencies
Status:	Exempt/Classified (S317)

Job Summary

The Senior Cybersecurity Engineer is responsible for leading and executing cybersecurity initiatives that protect County information systems, data assets, critical infrastructure, and public services. This role provides advanced technical expertise, strategic guidance, and operational leadership across all cybersecurity functions within County government.

Job Domains

A. Strategic Leadership and Governance

1. Develop and maintain a County-wide cybersecurity strategy that supports regulatory requirements and long-term technology goals.
2. Create and enforce cybersecurity policies, standards, and procedures across all County departments and agencies.
3. Advise technology leadership, elected officials, and department heads on cybersecurity risks, emerging threats, and mitigation strategies.
4. Participate in governance activities, steering committees, and long-term program planning.

5. Assist in budget development and resource planning for cybersecurity tools, staffing, and initiatives.

B. Security Operations and Threat Management

1. Oversee daily security operations including monitoring, alert triage, incident response, and threat analysis.
2. Manage enterprise security platforms such as SIEM, endpoint protection, identity management tools, and logging systems.
3. Lead proactive threat hunting activities and coordinate with regional, state, and federal partners when necessary.
4. Maintain operational documentation, security logs, and audit trails to ensure accountability and readiness.

C. Risk Management, Compliance, and Auditing

1. Conduct risk assessments, vulnerability scans, penetration tests, and compliance audits across County systems and cloud environments.
2. Ensure compliance with relevant frameworks and mandates such as NIST CSF, NIST 800-53, CJIS, HIPAA (if applicable), and state cybersecurity laws.
3. Maintain risk registers, compliance documentation, and follow-up action plans.
4. Prepare structured reports for County leadership summarizing risk levels and remediation recommendations.

D. Incident Response and Continuity Planning

1. Lead cybersecurity incident response activities, ensuring timely containment, investigation, and recovery.
2. Coordinate communication with affected departments to minimize disruption to public services.
3. Develop after-action reports, root cause analysis, and recommendations for improving processes and controls.
4. Support disaster recovery planning, business continuity exercises, and cyber readiness drills.

E. Infrastructure Security and Architecture Oversight

1. Provide guidance on secure architecture, network segmentation, cloud security strategy, and IT modernization efforts.
2. Review new technology projects to ensure security requirements are integrated from design through deployment.
3. Support secure coding practices, configuration management, system hardening, and vulnerability remediation.

4. Partner with IT teams to strengthen controls for public-facing services, internal networks, emergency operations, and critical infrastructure systems.

F. Training, Awareness, and Collaboration

1. Develop and deliver cybersecurity awareness programs and training for County employees and elected officials.
2. Mentor Communication Technicians in cybersecurity and provide technical leadership to IT personnel.
3. Coordinate with external partners including statewide cybersecurity agencies, vendors, auditors, and law enforcement.
4. Promote a culture of security through ongoing communication and collaboration across all County departments.

Knowledge, Skills, and Abilities

1. Understanding of firewalls, VPNs, secure routing, VLANs, and network segmentation techniques.
2. Familiarity with securing cloud environments such as Microsoft Azure, AWS, and government cloud offerings.
3. Knowledge of identity, access, encryption, and configuration standards for cloud workloads.
4. Knowledge of modern endpoint protection platforms, EDR/XDR tools, and secure configuration baselines.
5. Understanding of multi-factor authentication, role-based access control, privileged access management, and directory services (such as Active Directory, Azure AD).
6. Awareness of data loss prevention (DLP), encryption standards, secure data storage, and secure data lifecycle practices.
7. Proficiency with SIEM platforms, log correlation, alert tuning, and establishing monitoring baselines.
8. Ability to evaluate technical designs for security risk, propose secure architectures, and support modernization and cloud migration efforts.
9. Knowledge of securing Windows Server, Linux distributions, and mobile device environments used by County employees and public safety departments.
10. Familiarity with secure coding concepts, API security, web application vulnerabilities, and code review practices.
11. Understanding of patching processes, vulnerability prioritization, and remediation planning.
12. Awareness of CJIS Security Policy, HIPAA (if applicable), NIST guidelines, and state-level cybersecurity requirements.
13. Understanding of public procurement processes and compliance auditing.
14. Familiarity with digital forensics fundamentals, evidence handling, and coordinated response procedures.
15. Knowledge of unique security needs for emergency operations centers, public safety networks, and critical infrastructure SCADA/OT systems.

16. Understanding of backup strategies, continuity planning, and recovery testing.
17. Ability to review requirements, manage vendor relationships, evaluate security products, and participate in contract negotiations.
18. Experience developing security awareness initiatives for general government staff, including phishing simulations and targeted training.
19. Clear communication with technical and non-technical audiences
20. Project management and multitasking
21. Cross-department collaboration

Minimum Qualifications

1. Bachelor's degree in cybersecurity, information technology, computer science, or related field; or an equivalent combination of education, training, and experience.
2. Four (4) or more years of progressively responsible experience in cybersecurity roles.
3. Experience with enterprise IT infrastructure, security architecture, cloud environments, and regulatory compliance.
4. Professional certifications strongly preferred (CISSP, CISM, CEH, GIAC, or similar).