



# Controller Betty T. Yee

## California State Controller's Office

Applicants with disabilities who need reasonable accommodations, such as a Sign Language interpreter, a reader, or assistance attending an interview please call (916) 323-8579.

**Position:**

(280) Information Technology Specialist II

**Position #:**

051-340-1414-006

**Salary Range:**

\$7365.00 - \$9869.00

**Issue Date:**

10/6/2020

**Contact:**

Denise Middleton (916) 323-6695

**Location:**

Information Services Division  
300 Capitol Mall Suite 634  
Sacramento, CA 95814

**Final Filing****Date:**

10/19/2020

Individuals who are currently in this classification, or are eligible for lateral transfer or promotion, or are reachable on a certification list may apply.

For permanent positions, SROA and surplus candidates should attach "surplus letters" to their application. Failure to do so may result in your application not being considered.

**Submit application package electronically via your CalCareers account or to address below:**

State Controller's Office  
Human Resources Office  
ATTN: Classification Unit - AP  
300 Capitol Mall, Ste. 300  
Sacramento, CA 95814

**Application package must include all the required documents. Mailed application package must include either ARF # 20-117 or Position #051-340-1414-006 in the job title section. Application received without this information may be rejected.**

Looking for a job that you can feel passionate about? Looking for work in an inviting work environment? If you are interested in working in a fast-paced environment surrounded by enthusiastic and self-motivated people, then look no further! The Office of the State Controller (SCO) is the destination Constitutional employer within the State of California.

The following link outlines a summary of benefits available to state employees:

<https://www.calhr.ca.gov/Pages/California-State-Civil-Service-Employee-Benefits-Summary.aspx>

*Applications will be screened and only the most qualified will be interviewed. Application must include "to" and "from" employment dates (m/d/y), hours per week, and prior employer contact information including contact number. Applications received without this information may not be considered for this position.*

The selected candidate considered for the advertised position will be required to undergo a fingerprint clearance and any offer of employment will be contingent upon live scan fingerprint results.

**Scope of Position:**

Under general supervision of the IT Manager I within the Technical Support Section, the Information Technology Specialist II is responsible for monitoring and preventing network security incidents and intrusions by independently conducting analysis and investigations. The incumbent will act as a technical and analytical lead, consultant and team member or team lead on IT Security for the State Controller's Office network. The incumbent is responsible for maintaining an advanced knowledge of information technology system security hardening and compliance as well as advanced knowledge of scripting languages. Respond to after hours, weekends, and off service support calls including complex network related emergencies as relayed via multiple forms of communication including a mobile device. Ability to lift up to 50 pounds and required to travel to other SCO sites as needed. Duties include but are not limited to the following:

**Duties and Responsibilities:**

(Candidates must perform the following functions with or without reasonable accommodations.)

- 1 Act as technical lead in monitoring and analyzing the network's security posture on an ongoing basis. Detect, triage, investigate and conduct root cause analysis of security incidents, active attacks, and/or operational issues. Actively monitor help desk tickets to evaluate emerging support situations, prevent and respond to escalating events in accordance with established processes and guidelines, and communicate status to customers as appropriate. Identify trends, develop secure baseline configurations, apply approved solutions, and identify innovative solution enhancements. Report security incidents for distribution to managers or customer groups, collecting and summarizing information and trends. Stay current on latest threat intelligence and defense mechanisms.
- 1 Through research and analysis identify, develop and maintain software program scripts to optimize enterprise system processes. Monitor, advise and provide third level problem resolution to Service Desk incidents and emails.
- 1 Consult and provide project staff, various levels of management, technical personnel, business clients, and vendors with consistent, predictable and acceptable levels of customer service. Train and mentor project staff as needed. Stay current with the latest developments in equipment and software trends and consider their application and benefit within SCO. Identify infrastructure resource options and recommend IT systems to meet project needs. This includes preparing analytical evaluations, technical designs, and diagrams.
- 1 Create and maintain a broad variety of technical documentation which may include but not limited to authoring, editing, developing procedures, completing/responding to annual and technical reports, and other supporting documents to communicate complex and technical information more easily. Develop and maintain security standards and processes which maintain compliance with SAM, NIST, FISMA (Federal Information Security Management Act), and FedRAMP. Coordinate and respond to requests for data collection, status and statistical reporting as needed. Manage extended maintenance contracts for infrastructure hardware and software. Manage up to date network infrastructure asset location / inventory.
- 1 Functional role as a primary support specialist on assigned IT systems and the role of an active backup support specialist on other IT systems, as designated, to take responsibility for a portion of the workload and whenever the primary support specialist is unavailable.
- 1 Other NSU related duties appropriate to the classification which include, but are not limited to, traveling outside of the Sacramento area, any off shift support or maintenance, relocating and installing equipment, and working with other IT staff, vendors and consultants.

**Desirable Qualifications:**

- 1 Understanding of firewalls, proxies, SIEM, antivirus and IDPS concepts.

- 1 Experience with computer network penetration testing and techniques.
- 1 Ability to identify and mitigate vulnerabilities at all layers of the technology stack.
- 1 Advanced experience with enterprise business and large scale network security principles.
- 1 Proven ability to analyze and document data collected via data flows, telemetry, packet capture, syslog, and other methods.
- 1 Advanced understanding of TTPs (tools, tactics and procedures) and kill chains of threat actors.
- 1 Expert level working experience with advanced scripting languages such as PowerShell and VBScript.

---

*The State of California is an equal opportunity employer to all, regardless of age, ancestry, color, disability (mental and physical), exercising the right to family care and medical leave, gender, gender expression, gender identity, genetic information, marital status, medical condition, military or veteran status, national origin, political affiliation, hair style and texture, race, religious creed, sex (includes pregnancy, childbirth, breastfeeding and related medical conditions), and sexual orientation. Rev. 02/2020*