

**CALIFORNIA DEPARTMENT OF TRANSPORTATION  
DUTY STATEMENT**

<b>CLASSIFICATION TITLE</b> Systems Software Specialist I (Technical)	<b>DISTRICT/DIVISION/OFFICE</b> D20/Information Technology/Security Division/Network Technologies	
<b>WORKING TITLE</b> Network Specialist	<b>POSITION NUMBER</b> 900-170-1587-924	<b>EFFECTIVE DATE</b> July 2014

As a valued member of the Caltrans team, you make it possible for the Department to improve the mobility across California by being innovative and flexible; reporting to work regularly and on time; working cooperatively with team members and others; and treating others fairly, honestly and with respect. Your efforts are important to each member of the team, as well as those we serve.

**GENERAL STATEMENT:**

Under the general supervision of a Systems Software Specialist III (Supervisory), the incumbent functions as a technician on network and security system projects related to the Caltrans Wide Area Network (WAN). This includes working independently as a technical expert or as part of a team on network and security issues and helping guide other information technology professionals in network and security application design and integration. The incumbent will participate in the design, implementation and maintenance of network security, automated network security control systems, and proprietary security software. This includes the proper operation and configuration of firewalls, Intrusion Prevention Systems (IPS's), URL filtering systems, remote access, and highly technical network security monitoring and logging equipment. The incumbent must work with other analysts to maintain and improve the Departments security posture, investigate security events, assist in the remediation of virus outbreaks and assist in protecting the Department's data from malicious or unwanted behaviors as follows:

**TYPICAL DUTIES:**

**E - Essential**  
**M - Marginal**

- 40% (E) Individually or as part of a group, provide technical support for the Departments network security systems; including the Departments firewalls, URL filtering system, Intrusion Detection/Prevention Systems and VPN concentrators. Support to include assist in the, design, implementation, integration and maintenance of existing and future systems. Address Service Desk tickets requesting changes to the Departments Firewalls, assist in the research of services and protocols needed, how new rules will affect existing rules and implement rules during the Departments weekly change window. Apply IPS signature updates as well as tune the IPS systems to reduce the number of false positives reported. Work with the URL filtering system, Websense, to provide management as well as other Information Technology (IT) staff with reports on misbehaving devices.
  
- 20% (E) Individually or as part of a group, assist in the performance of technology research for network communication devices and their conformance to standards regarding multi-

protocol network integration, routing protocols, OSI model relationships, and network integration methodologies used to integrate various server operating systems such as Cisco IOS, Windows and Unix. An example would be how to allow wireless connectivity to the Departments network without compromising network security.

- 20% (E) Act as team member and provide technical expertise in resolving anomalies associated with network devices and network software systems; implementation within the network of proprietary software, telecommunications software and integration of new telecommunications hardware (use of Packet Analyzers and other tools to document network anomalies). Assist in the installation, configuration and maintenance of software systems and enterprise network devices such as core routers, switches and firewalls.
- 10% (M) Individually or as part of a group, provide technical network security support in the detection, notification, remediation and tracking of infected devices within the Departments computing environment. This includes reviewing syslogs, firewall and DNS logs, writing custom scripts or using the various network tools available. Perform network vulnerability assessments using tools provided.
- 10% (M) Individually or as part of a group, performs technology research for network security systems and their conformance to Departmental standards and State mandated network security policies.

**SUPERVISION EXERCISED OVER OTHERS:**

None.

**KNOWLEDGE, ABILITIES AND ANALYTICAL REQUIREMENTS:**

**Knowledge of:** Electronic computer operating systems, OSI model, software programming and configuration; electronic data processing equipment and its capabilities and interfaces between hardware and software; the requirements of the installation and implementation of the more complex computer software systems; Firewalls, IPS/IDS, URL filters, DNS, DHCP, electronic data processing equipment and its capabilities, network security standards, tools and issues, virus mitigation

**Ability to:** Analyze data and read logs and packet traces to detect network traffic anomalies; write scrip programs; develop detailed program specifications; analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions; apply creative thinking in the design and development of methods of securing data; establish and maintain cooperative relationships with those contacted in the course of the work; work under pressure; speak and write effectively; prepare effective reports.

**Analytical Requirements:** The incumbent must have a level of data processing analytical ability and expertise to permit the employee's exercise of sound judgment in all disciplines from conceptualization through detailed implementation on complex projects.

**CONSEQUENCE OF ERROR/RESONSIBILITY FOR DECISIONS:**

The incumbent is responsible for decisions, actions, and consequences related to the design, installation, operation, and security management of the Caltrans wide area network which provides backbone connectivity for all major information systems that are in use at Caltrans, including Caltrans information systems running at the Department of Technology Services. Continued secure operation of the network is essential to assure that Caltrans personnel have access to mission critical applications and data distributed throughout the State of California. Consequence of error may include: loss or misuse of sensitive Departmental data, loss or misuse of employee's sensitive and personal information, disruption of system communications and disruption of network services which could translate into the loss of large amounts of staff productivity and Departmental resources.

**PUBLIC AND INTERNAL CONTACTS:**

The incumbent will have frequent contact with managers and staff in all functional areas of Caltrans, District IT managers and staff, private consultants, and vendor representatives concerning the needs and development of system software projects. The incumbent may initiate contact with other departments, governmental agencies, or private companies concerning technology related to the security of the Caltrans network.

**PHYSICAL, MENTAL AND EMOTIONAL EQUIREMENTS:**

The incumbent may be required to sit for long periods of time using a keyboard; work in highly intense situations when network failures occur and immediate resumption of services is paramount; deal effectively with pressure, maintain focus, and intensity yet remain optimistic and persistent, even under adversity; adjust rapidly to new situations warranting attention and resolution.

**WORK ENVIRONMENT:**

While at their base of operation, employee will work in a climate-controlled office under artificial lighting using a personal computer. The incumbent will be required to work for limited amounts of time in high noise level computer rooms with lower than normal temperatures.

I have read, understand and can perform the duties listed above. If you believe you may require accommodation, please discuss this with the hiring supervisor.

\_\_\_\_\_  
Employee's Name (please print)

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Date

I have discussed the duties with and provided a copy of this duty statement to the employee named above.

\_\_\_\_\_  
Supervisor's Name (please print)

\_\_\_\_\_  
Supervisor's Signature

\_\_\_\_\_  
Date