

## SUPERVISORY CONTROL AND DATA ACQUISITION SERVER SPECIALIST

<b>RESOURCE CATEGORY</b>	Cybersecurity
<b>RESOURCE KIND</b>	Not Specified
<b>OVERALL FUNCTION</b>	
<b>COMPOSITION AND ORDERING SPECIFICATIONS</b>	<ol style="list-style-type: none"> <li>1. This position can be ordered as a single resource.</li> <li>2. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment</li> <li>3. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days</li> </ol>

Each type of resource builds on the qualifications of the type below it. For example, Type 1 qualifications include the qualifications in Type 2, plus an increase in capability. Type 1 is the highest qualification level.

COMPONENT	SINGLE TYPE	NOTES
<b>DESCRIPTION</b>	<p>The Supervisory Control and Data Acquisition (SCADA) Server Specialist position is responsible for the controller-side hardware, firmware, and software and:</p> <ol style="list-style-type: none"> <li>1. Responds to crisis or urgent situations for SCADA front-end systems and associated server-side infrastructure to manage controllers and their associated software and hardware systems</li> <li>2. Is responsible for Incident Command System (ICS)/SCADA workstations and servers</li> <li>3. Executes various approaches aimed at mitigating, preparing, responding, and recovering servers from shutdown</li> <li>4. Is an adjunct to the National Incident Management System (NIMS) Type 1 SCADA Controller Specialist</li> </ol>	Not Specified
<b>EDUCATION</b>	Not Specified	Not Specified
<b>TRAINING</b>	<p>Completion of the following:</p> <ol style="list-style-type: none"> <li>1. IS-100: Introduction to Incident Command System, ICS-100</li> <li>2. IS-200: Incident Command System for Single Resources and Initial Action Incidents</li> <li>3. IS-700: National Incident Management System, An Introduction</li> <li>4. IS-800: National Response Framework, An Introduction</li> </ol>	Not Specified

Superseded

COMPONENT	SINGLE TYPE	NOTES
<b>EXPERIENCE</b>	<p>Agency Having Jurisdiction (AHJ)-documented and validated knowledge, skills, and abilities demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Desktop, server, and mainframe operating systems including Windows, Unix, Linux, and Mac OS</li> <li>2. Human Machine Interfaces (HMI)</li> <li>3. Remote controlled equipment and front-end-servers</li> <li>4. Common two and three wire hardware control buses</li> <li>5. Physical and server security, firewalls and intrusion detection systems</li> <li>6. Data backup, types of backups, and recovery concepts and tools</li> <li>7. Host/network access controls and defense-in-depth concepts and controls</li> <li>8. Log analytics and the use of the corresponding industry tools</li> <li>9. Applying host access controls and network access controls including firewalls and screening routers</li> <li>10. Intrusion detection and prevention (IDS/IPS) systems</li> <li>11. Performing backup and recovery functions</li> <li>12. Diagnosing and troubleshooting SCADA issues</li> </ol> <p>AHJ-documentated and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Administering and operating SCADA servers, archive servers, and front-end servers</li> <li>2. Server-side controller software operation, installation and troubleshooting</li> <li>3. Master/central control terminal units and systems</li> <li>4. Vendor patch management</li> <li>5. Coordinating with and providing expert technical support to enterprise-wide computer network defense (CND) specialists to resolve CND incidents</li> </ol>	Not Specified
<b>PHYSICAL/MEDICAL FITNESS</b>	Not Specified	Not Specified
<b>CURRENCY</b>	<ol style="list-style-type: none"> <li>1. Participates in exercise, drill, or simulation at least once every year</li> <li>2. Background checks as applicable law permits and requires</li> <li>3. Active security clearance</li> </ol>	Provider must carry out and use any background checks as applicable law specifies. This may include a background check completed within past 12 months; sex-offender registry check; and a local, state, and a local, state, and national criminal history.
<b>PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS</b>	Not Specified	Not Specified

Superseded



## Position Qualification for Cybersecurity Cybersecurity

### NOTES

Nationally typed resources represent the minimum criteria for the associated category.

---

### REFERENCES

Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014

---

Superseded