Position: **Mid-Level IA/Security Specialist** (Computer Network Defense Incident Responder)

Education: B.S. in a Computer Information Systems or related field

Job Description:
The Computer Network Defense Incident Responder supports the investigation and analysis of all response activities related to cyber incidents within the network environment or enclave. When incidents occur on NAVAIR networks being monitored established incident response processes and all applicable DOD instructions will be performed.

Responsibilities:
- Receive and analyze network alerts from various sources within the network environment (NE) or enclave and determine possible causes of such alerts.
- Monitor external data sources (e.g. CND vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND threat condition and determine which security issues may have an impact on the NE or enclave.
- Collect and analyze intrusion artifacts (e.g. source code, malware, and trojans) and use discovered data to enable mitigation potential CND incidents within the enclave.
- Perform analysis of log files from a variety of sources within the NE or enclave, to include individual host logs, network traffic logs, firewall logs, and intrusion detection system logs.
- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enclave systems.
- Coordinate with and provide technical expertise to enclave CND technicians to resolve CND incidents.
- Track and document CND incidents from initial detection through final resolution (CDRL A001)
- Perform CND incident triage to include determining scope, urgency, and potential impact.
- Correlate incident data to identify specific vulnerabilities and recommend strategies that enable expeditious remediation.
- Coordinate with intelligence analysts to correlate threat assessment data.
- Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
- Perform real-time CND Incident Handling (e.g. forensic collections, intrusion
- correlation/tracking, threat analysis, and direct system remediation) tasks for deployable Incident Response Teams (IRT).
- Maintain deployable CND toolkit (e.g. specialized CND software/hardware) to support IRT missions.
- Write and publish CND guidance and reports on incident findings to appropriate
- Constituencies Perform CND trend analysis and reporting.
- Perform command and control functions in response to incidents.

Qualifications:
- 4-9 years of experience in IT/Computer Network Operations/Cyber Security field
- DoD 8570 IAT Level II: Security +, SSCP, or GSEC Certification
- B.S. in a Computer Information Systems or related field, preferred
- Secret Clearance with SSBI or TS/SCI with SSBI