Position: **Mid-Level IA/Security Specialist,** (Computer Network Defense Analyst)

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

Job Description:

This position working within a team, assists with defending the organization against cyber-attacks from domestic and international sources.

Responsibilities:

- Use data collected from a variety of CND tools (including intrusion detection system logs, firewall and network traffic logs, and host system logs) to analyze events that occur within the networks under the 7.2.6 Division's purview.
- Receive and analyze network alerts from various sources within the network environment (NE) or enclave and determine possible causes of such alerts.
- Coordinate with network enclave/environment staff to validate network alerts.
- Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
- Monitor external data sources (e.g. CND vendor sites, Computer Emergency Response Teams, SANS, Security Focus, etc.) to maintain currency of CND threat condition and determine which security issues may have an impact on the NE or enclave.
- Perform development of signatures which can be implemented on CND network tools in response to network observed threats within the NE or enclave.
- Perform event correlation using information gathered from a variety of sources within the NE or enclave to gain situational awareness and determine the effectiveness of an observed attack.
- Notify CND managers, CND incident responders, and other CND-SP team members of suspected CND incidents and articulate the events history, status, and potential impact for further action.

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