

Position Identification

Title	AM – Infrastructure Services
Functional Designation	Cybersecurity Consultant

Position Objective

To find the most efficient way to protect the system, networks, software, data and **information** systems against any potential attacks. To implement vulnerability testing, threat analyses, and **security** checks. To perform the research on **cyber security** criteria, **security** systems, and validation procedures.

Competencies Required

The following competencies are required for this position:

- A. Bachelor's degree in Computer Science, Information Systems, or equivalent education or work experience
- B. System administration
- C. Network security
- D. Problem solving
- E. Information security policies
- F. On-call network troubleshooting
- G. Firewall administration
- H. Network protocols
- I. Routers, hubs, and switches
- J. Informing others
- K. Process improvement
- L. Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth and common security elements.
- M. Hands-on experience analyzing high volumes of logs, network data (e.g. Netflow, FPC), and other attack artifacts in support of incident investigations
- N. Experience with vulnerability scanning solutions
- O. Familiarity with the DOD Information Assurance Vulnerability Management program.
- P. Proficiency with any of the following: Anti-Virus, HIPS, ID/PS, Full Packet Capture, Host-Based Forensics, Network Forensics, and RSA Security.
- Q. In-depth knowledge of architecture, engineering, and operations of at least one enterprise SIEM platform (e.g. Nitro/McAfee Enterprise Security Manager, ArcSight, QRadar, LogLogic, Splunk)
- R. Understanding of mobile technology and OS (i.e. Android, iOS, Windows), VMware technology, and Unix and basic Unix commands

Responsibilities

A list of the chief responsibilities carried out by access developers is given below:

- Safeguards information system assets by identifying and solving potential and actual security problems.

- Protects system by defining access privileges, control structures, and resources.
- Recognizes problems by identifying abnormalities; reporting violations.
- Implements security improvements by assessing current situation; evaluating trends; anticipating requirements.
- Determines security violations and inefficiencies by conducting periodic audits.
- Upgrades system by implementing and maintaining security controls.
- Keeps users informed by preparing performance reports; communicating system status.
- Maintains quality service by following organization standards.
- Maintains technical knowledge by attending educational workshops; reviewing publications.
- Contributes to team effort by accomplishing related results as needed.

Reporting Structure

A resource holding this position will be reporting into Manager – Infrastructure Services.

Acknowledgement

This job description has been designed to indicate the general nature and level of work performed by employees within this classification. It is not designed to contain or be interpreted as a comprehensive inventory of all duties, responsibilities and qualifications required of employees assigned to the role.