# CYBER SECURITY ARCHITECT

FC: 000071
PB: 08
FLSA: Exempt

PC: 891
BU: 91 (Non Represented)
Created: September 2013
Correction: August 2016

*Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are **not** intended to reflect all duties performed within the job.*

## DEFINITION

Under general guidance the Cyber Security Architect performs a variety of professional cyber security architectural duties including providing the development design, execution and administration of project work plans while maintaining direct, client-facing engagement responsibilities. Serving as both role model and trainer, the Cyber Security Architect will assist other District Personnel in developing technical and professional competency; and performs related duties as assigned.

## CLASS CHARACTERISTICS

This class is responsible for developing and executing Information Security project work plans. Employees at this level receive only occasional instruction or assistance as new or unusual situations arise, and are fully aware of the operating procedures and policies of the work unit. This class is distinguished from the Cyber Security Specialist in that the latter classification is responsible for implementation and this position is responsible for the developing complex designs using specialized, technical and functional expertise within the area of assignment or may exercise lead supervision over assigned lower level staff.

## REPORTS TO

This position reports to the Manager of Information Systems or his/her designee.

**EXAMPLES OF DUTIES** – *Duties may include, but are not limited to, the following:*

1. Under general supervision designs, implements and maintains the District's Unified Cyber Security Program including the validation and approval of all cyber security policies and procedures.

2. Provides complex level design, and administration of various architectural projects; ensures work quality and adherence to District’s policies, guidelines, specifications.

3. Identifies institutional security vulnerabilities and designs enterprise remediation solutions; Designs complex computer algorithms used to monitor both machine and human behavior.

4. Provides the overall direction for targeted cyber investigation.

5. Acts as a resource for management in the selection of hardware, software and consulting services related to District Infrastructure.

6. Participates in the Communication Information Office (CIO) leadership team, offering recommendations to the District's Technology as needed; Certifies cyber security within the District's Technology Project Approval Process.

7. Identifies core metrics to measure the effectiveness of security solutions; Performs post-mortem forensic cyber investigations after breach.

8. Works with District stakeholders to establish design guidelines and architectural standards for security-related investments.

9. Works with Local, State and Federal officials to coordinate Cyber Defense Initiatives.

10. Performs other duties as assigned.

## QUALIFICATIONS

### Knowledge of:

Information security tools such as Nessus, Kismet, Airsnort, NMAP, Ethereal, WebInspect and Nikto.
Information Systems and Information Security which address organizational structure and administration practices, system development and maintenance procedures, system software and hardware controls, security and access controls, computer operations, environmental protection and detection, and backup and recovery procedures.
Information system architecture and security controls, such as firewall and border router configurations, operating systems configurations, wireless architectures, databases, specialized appliances and information security policies and procedures.
Technologies such as IDS/IPS, vulnerability assessment tools, remote access methodologies, log management tools, firewalls, cryptography and digital certificates.
Programming languages such as Java, C, C++, C#, and .NET.
Industry Standards, eg, ISO 17799/27001, NIST Publications and other Industry Related Security Standards.

Principles and practices of business processes and project management.
Current office procedures, methods, and equipment, as well as programs for word processing.
Related Federal, State and local laws, codes and regulations pertaining to work and to generally accepted industry and associations standards.

**Skill in**:
Developing and writing Cyber Security Policy and Procedures.
Utilizing information security tools such as Nessus, Kismet, Airsnort, NMAP, Ethereal, WebInspect and Nikto.
Performing manual techniques to exploit vulnerabilities in the OWASP top 10 including but not limited to cross-site Scripting, SQL injections, session hi-jacking and buffer overflows to obtain controlled access to target systems.
Performing network traffic forensic analysis, utilizing packet capturing software, to isolate malicious network behavior, inappropriate network use or identification of insecure network protocols.
Analyzing and testing attack and penetration of Internet infrastructure and Web-based applications utilizing manual and automated tools.
Preparing clear and concise reports and documentation.
Executing troubleshooting tasks.
Application source code security review.
Communicating clearly and concisely, both orally and in writing.
Establishing and maintaining effective working relationships with those contacted in the course of work.

## MINIMUM QUALIFICATIONS

**Education**:

A Bachelor's degree in Computer Science, Computer Information Systems, Management Information Systems or a closely related field from an accredited college or university.

**Experience**:
Three (3) years of full-time equivalent verifiable professional experience in an Information Security Operations role or three (3) years in a related field, preferably in professional services and/or industry and one (1) year experience in a Cyber Security Project Management Role

**Substitution:**
Additional professional experience as outlined above may be substituted for the education on a year-for-year basis. A college degree and information security related certification (s) is preferred.

**Other Requirements:**

Physical condition necessary to conduct field inspections and testing as assigned.

## WORKING CONDITIONS

### Environmental Conditions:
Office environment; exposure to computer screens.

### Physical Conditions:
May require maintaining physical condition necessary for sitting for prolonged periods of time.

**EEOC Code: TBD**