Nothing in this job description restricts management's right to assign or reassign duties and responsibilities to this job at any time.

DUTIES This is a non-career term job at the Metropolitan Washington Airports Authority (Airports Authority). Serves as a Security Engineer in the Information Security Department of the Office of Technology (Office). Monitors, tests, and reports on the confidentiality, integrity, and availability of Airports Authority information assets in compliance with Airports Authority information security policies and other security and compliance standards such as the National Institute of Standards and Technology (NIST) 800-53, the Payment Card Industry Data Security Standards (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA). Implements, operates, and maintains all technologies used in support of the Airports Authority Security Operations. Works with other Information Technology (IT) teams to address information security related issues. Performs related functions.

--Assists with the implementation, operation, and maintenance of technologies used in support of the Airports Authority's Information Security Program. This includes real-time monitoring, detection of security threats, correlation of security events, notifications, reporting, creation of dashboard views, and investigating them to completion. Maintains, upgrades, and implements new information security tools to ensure the Airports Authority systems and information are protected.

--Works with other IT groups to ensure devices and applications added to Airports Authority networks are configured to security standards and policies and are in compliance with mandates such as PCI DSS, HIPAA, and other applicable regulations.

--Manages and maintains Security Information and Event Management (SIEM) systems to provide real-time monitoring, correlation of security events, notifications, reporting, and creating dashboard views. Performs configuration management tasks to ensure all devices and applications added to Airports Authority networks are configured to send automatic security event notifications to devices for security incident response and investigations.

--Manages and maintains the Airports Authority intrusion prevention systems (IPS) and intrusion to identify, log, block, and report malicious activity occurring within Airports Authority networks and/or systems. Deploys, configures, and monitors all IPS and IDS appliances. Responds to and resolves security alerts and escalates high risk events to the appropriate technology team for resolution.

--Reviews Airports Authority firewalls to ensure firewall rules are appropriate for the protection of Airports Authority information and systems. Ensures firewall changes have been reviewed and approved by the Information Security Director prior to their deployment into production environments.

---Conducts continuous vulnerability scans and penetration testing on all Airports Authority networks to ensure all identified vulnerabilities are resolved according to established information security policies and standards. Participates in the Airports Authority patch management processes to ensure operating systems, applications, databases, etc., are effectively patched.

Recommends changes and improvements to the patch management process when deficiencies are identified.

--Works with other Information Security staff to ensure PCI regulated environments are continuously compliant with the payment cards industry's Data Security Standards (PCI-DSS). Works with external PCI compliance assessors during their annual audits, external and internal scans, and penetration testing. Conducts network and systems audits and prepares assessment reports. Conducts end-point assessments to ensure compliance with anti-virus, anti-malware, software, local admin, and other security policies.

--Continuously monitors user access (employees, contractors, and third party vendors) to ensure access is authorized, provisioned, and de-provisioned according to Information Security policies and procedures. . This includes reviewing access for: LDAP, databases, VPN and firewalls. Identifies information security policy violations and takes the appropriate measures to correct, resolve, and prevent their reoccurrence.

--Serves as a primary member on the Security Incident Response Team (SIRT) to respond to, prevent reoccurrence, and recover from security breaches. Keeps abreast of security industry developments to proactively identify threats (such as zero-day exploits, phishing scams, etc.) against Airports Authority networks and systems, and takes the appropriate actions to mitigate information security threats; and ensure the Airports Authority security architecture standards align with evolving legal and mandated compliance standards.
--Conducts information security awareness training to educate Airports Authority staff and other users such as vendors/contractors on securing Airports Authority networks, systems, and protected data. Conducts periodic phishing testing to evaluate the effectiveness of the Awareness program. Supports the creation of newsletters in support of the awareness training program.

--Communicates and interacts effectively with internal and external business contacts including, but not limited to, other members of the unit/team, other members of the Office of Technology, other Airports Authority employees (such as managers, supervisors, professionals, and support staff), vendors, contractors, and suppliers.

--Uses a computer and (a) modern office suite software for various applications such as, but not limited to, planning/scheduling, communicating (email), word processing, data manipulation (databases and spreadsheets), charts/graphics and presentations; (b) enterprise systems/software (such as ERP) to collect, store, manage and interpret data from business activities; and (c) specialty systems/software (such as OBIEE) used in the Office.

--*Performs related duties as assigned.*

Critical features of this job are described under the headings below. They may be subject to change through reasonable accommodation or otherwise.

MINIMUM QUALIFICATIONS (MQs)

To be rated qualified for this job, an applicant must meet all of the MQs listed below at the time of vacancy announcement closure.

1. A Bachelor's Degree in Computer Science, Computer Engineering, Information Security, or Information Assurance or any other field providing a strong foundation for successful performance of the DUTIES in this job description, or an equivalent combination of education, experience and training that totals four years.

2. Five years of progressively responsible experience in Information Security that includes substantive work in most of the DUTIES in this job description, including: (a) implementing, upgrading, and maintaining various security tools including, but not limited to: intrusion prevention/detection systems (IPS/IDS) tools; vulnerability and/or penetration testing tools; firewalls; SIEM, Anti-virus/Anti-malware; endpoint encryption; and Data leakage prevention (DLP) tools; and (b) configuring and/or reviewing firewalls; experience conducting security assessments.

   Included in these five years must be a minimum of 3 years implementing security devices and tools such as IDS/IPS, Web security tools, Email security tools, Firewalls, Two factor authentication devices.

   A Master's Degree in Computer Science, Computer Engineering, Information Security, or Information Assurance or another field providing a strong foundation for successful performance of the DUTIES in this job may be substitute for two of these five years.

3. Certification as a Certified Information Systems Security Professional (CISSP) or Systems Security Certified Practitioner (SSCP) from the International Information Systems Security Certification Consortium (ISC2) or ability to obtain CISSP or SSCP certification within one year from the date of the Final Offer Letter. A qualified candidate who is selected, but lacks CISSP or SSCP certification must obtain certification from ISC2 within one year of the date of the Final Offer Letter.

PREFERRED QUALIFICATIONS

The qualifications listed below (if any) are preferred and may be considered in the selection process, but they are not required to be rated qualified for this job.

1. A Master's Degree in Computer Science, Engineering, or Math.

2. Certification as a Certified Information Systems Security Professional (CISSP) or Systems Security Certified Practitioner (SSCP) from the International Information Systems Security Certification Consortium (ISC2)

3. Hands-on experience implementing and supporting at least 3 of the following technologies: CISCO security devices and products, SIEMs, enterprise Endpoint security products, network and web application scanners, Web and Email Security solutions.

4. Experience participating in PCI DSS and HIPAA, or other industry regulation audits.

KNOWLEDGE, SKILLS, ABILITIES AND OTHER FACTORS (KSAOs)

The following KSAOs are required for successful performance of this job and are a basis for rating and ranking applicants who are found to meet the MQs. *Local, Federal, airport industry or Airports Authority specific bodies of knowledge listed below may be acquired on the job, typically; ability to rapidly acquire them is required at the time of vacancy announcement closure.*

1. Comprehensive knowledge of network and application firewalls, SIEMs, VPNs, and IPS using at least three of the following technologies: SPLUNK, Tripwire Enterprise, Cisco ASA firewall, Palo Alto firewalls, Sourcefire IPS, or Websense to implement, configure, and fine tune information security devices so as to protect organizational systems and networks from security incidents.

2. Comprehensive knowledge of detecting, responding to and analyzing security events and alerts; knowledge of SIRT procedures to serve as a primary participant resolving confirmed security incidents such as major virus outbreaks, internal or external security breaches, etc.

3. Knowledge of SIEMS to configure them with minimal direction, to receive logs from network attached devices, and to create and configure alerts for critical security events that threaten the security posture of Airports Authority networks and systems. Ability to create security dashboards and reports for management that provide important security status updates.

4. Conducted security reviews and/or assessments of major operating systems (Microsoft, Linux, IOS) and databases, web applications, firewalls using : network and web application scanning tools, , scripting languages test, and report security postures and statistics.

5. Skill in problem solving to select, organize, and logically process relevant information (verbal, numerical, or abstract) to solve a problem. This includes the ability to recognize subtle aspects of problems, identify relevant information, and make balanced recommendations and decisions. Examples include implementing corrective action plans to respond to, prevent reoccurrence, and recover from security breaches; and recommending effective changes to the patch management process when deficiencies are identified.

6. Skill to analyze data and established procedures within the Airports Authority to recommend and develop information security policies and standards to protect information assets from accidental or intentional unauthorized access or damage.

7. Interpersonal skills to interact effectively with business contacts in a businesslike, customer

service-oriented manner such as collaborating with colleagues on the SIRT and Change Management Team to address information security related issues.

8. Skill in oral communication to understand verbal information (including instructions, descriptions, and ideas) and to express such information verbally so that others will understand. This includes presenting technical information, advice, findings, and recommendations to technology peers and management and conducting information security awareness trainings for staff and contract personnel.

9. Skill in written communication to understand written information (facts, descriptions, ideas, concepts, conflicting assertions and arguments), draw inferences, form hypotheses and develop logical arguments, and to express such information in writing so that others will understand, and concerning some issues, be convinced or persuaded. This includes preparation of status reports and documentation of new standards, policies, and procedures.

10. Skill in using a computer and (a) modern office suite software (such as MS Office) to plan, schedule, communicate, word process, prepare and develop reports, and perform research (Internet use, as in searching for performance information and keeping up with technology); (b) enterprise systems/software (such as ERP) to collect, store, manage and interpret data from business activities; and (c) special systems/software/tools used in the Office.

RESPONSIBILITY Works with Department staff in the implementation, operation, and maintenance of technologies used to support the information security operations of the Airports Authority. Work supports the goal of securing all Airports Authority information assets in compliance with internal information security policies, as well as industry best practices and Federally mandated security compliance standards.

Reports to the Chief Information Security Officer (Supervisor). Most work flows to the incumbent as a result of assigned functions and established work processes. The Supervisor provides broad objectives and policy guidance for recurring assignments and, in consultation with the incumbent, brief instructions and time frames for special projects. Most work is accomplished independently but requires collaboration with colleagues. The incumbent collaborates with and keeps the Supervisor informed and typically elevates only highly complex or highly sensitive issues for assistance in resolution. Work is typically reviewed in terms of quantity, quality, timeliness, customer service, teamwork adherence to guidelines, and other factors.

Guidelines and references include Office policies, procedures, and standards (e.g. Office of Technology Standards, Change Management Process, Root Cause Analysis Procedure, Technology Advisory Committee Project Submittal Procedure, Electronic Communications System Policy, and Enterprise Technology Management Policy); security software tools manuals/guidelines; PMO best practices; and information security industry frameworks (e.g. TOGAF, NIST, ISO 27001, and COBIT). The incumbent uses seasoned judgment to adjust and apply guidelines to particular situations.

EFFORT The work is primarily sedentary, but requires moving about to obtain work information. The incumbent may sit for extended periods while performing desk work. Regularly uses a computer, a telephone, and other office equipment. Typically exerts light physical effort in opening/closing file drawers, retrieving files and otherwise moving about. Regularly reviews computer screens, printouts, contracts, and regulations containing small print.

WORKING CONDITIONS Works primarily in an adequately lighted, ventilated, and temperature controlled office and conference rooms.

OTHER SIGNIFICANT JOB ASPECTS Must be able to work varied schedule of days and outside normal 8am-5pm business hours for scheduled and emergency maintenance and/or upgrades as well as standard on-call rotation. Is subject to hold-over and recall for IT emergencies and may need to work nights and weekends depending on operational requirements and other factors.