**PERFORMANCE WORK STATEMENT**

**CYBER SECURITY SUPPORT**

**THE WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY (WMATA)**

# PART 1: GENERAL INFORMATION

## ****1.1 Introduction****

The mission The Office of Metro IT Security is to ensure a safe, secure, and resilient digital environment based on and sustained through strong teamwork, investment in personnel development and retention, and procurement of cost effective Cyber Security products & services. Metro IT Security would like to procure the services of a company that can provide a team of resources to deliver the services necessary for a successful data security program. The requirements needed to support Metro IT Security’s objectives are contained herein and identify the specific team responsibilities, including, written reports or other deliverables that the team will be required to produce for Metro’s IT Security Management. This team of resources will be a critical part to the data security, data assurance and security operations for the Metro IT Security department.

## 1.2 Scope

The Contractor shall provide all personnel, equipment, tools, materials, supervision and other items necessary to perform the task defined in this Performance Work Statements (PWS), except as specified in Part 3, WMATA-Furnished Resources. The Contractor shall provide timely, technically accurate and efficient Cyber Security services that support the Office of Metro IT Security’s mission. This effort encompasses technical, engineering, management, operation, logistical and administrative support for the Office of Metro IT Security. The Contractor shall provide qualified personnel and other resources necessary to perform the required services. Required services include: program planning and execution; regulatory compliance; management and technical briefings; performance measurement and reporting; program policy and standard operating procedures (SOPs) development; intelligence and law enforcement liaisons; critical infrastructure support; Computer Incident Response Team (CIRT) operations; network monitoring and intrusion detection system (IDS); security information and event management (SIEM); penetration testing; advanced cyber threat analyses; internal threat analyses; security research and engineering; system test and evaluation; vulnerability assessments and management; compliance assessments and management; security standards development; intra-agency and inter-agency working group representation; policy and standards development; security awareness training; operation and maintenance of IT hardware and software necessary to support the Office of Metro IT Security; websites content development and management; inventory management; and logistical and administrative support.

## 1.3 Period of Performance

The Period of Performance (PoP) shall be from: July 01, 2015 through 30 June 30, 2020.

## 1.4 Hours of Operation / Principal Place of Performance

Work in support of this PWS shall be performed in support of the Office of Metro IT Security located at 600 Fifth Street, NW Washington, DC 20001. However, the place of performance is not limited to the above due to evolving requirements throughout WMATA. Work at an alternate location/Telework may be enacted upon WMATA approval. The contract must at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within a task order when the WMATA facility is not closed for recognized holidays, inclement weather, or other unexpected reasons. Normal business hours are from ­­0800 to 1700 Monday through Friday. Alternate Work Schedule (AWS) may be authorized by the COTR on a case by case basis.

## 1.5 Installation Closure

Facilities may be closed unexpectedly due to inclement weather or other reasons. Notification is normally by way of local radio, television (TV) stations or via WMATA’s website at [www.wmata.com](http://www.wmata.com). Information concerning other methods of notification will be provided by WMATA. No price adjustments will be made for any delays resulting from an installation closing. When area radio stations, TV stations or WMATA’s website report that a facility has "delayed reporting" until a particular time, the Contractor's personnel have until that time to report to work. No price adjustment will be made if personnel arrive at work between the normal start time and the delayed reporting time.  A WMATA installation or activity may be closed for other reasons on short notice. It is at WMATA’s option to cancel some or all services with written notice. Natural or man-made events (i.e. catastrophic weather, changes in Homeland Security Condition, etc.) may result in restricted access to the WMATA facility. Such events limit access to personnel that are identified as Essential. In the event of such an occurrence, various local media mechanisms and WMATA’s website will be used to broadcast that only Essential Personnel are to report. Identified personnel will report as directed by the COTR.

## 1.6 Points of Contact

The COTR (whose authority is limited to providing basic guidance and advice to the contractor while on-site) and Alternate COTR (ACOTR) for this effort shall be identified at the time of award.

## 1.7 Support Personnel Labor Categories

#### 1.7.1 Cyber Security Program Manager

**Responsibilities**

Provides task tracking, resource allocation, ticket management, requirements review, budgeting, project status reports, coordinate Business Project Intake (BPI), Process and SOP development and management.

Develops schedules and project plans to ensure timely completion of projects, including identification of scope changes, critical path items, dependencies, etc.

Work with technical and operational staff to resolve information security tasks and projects

Ensure that the appropriate standards (e.g. compliance requirements), processes and documentation are followed for all projects.

Proactively identifies project issues and risks, and work with the project team for timely resolutions.

Coordinates with appropriate stakeholder to identify process improvement opportunities.

Coordinates technical and administrative teams, manage vendor, client and customer relationships.

Implements and coordinates security operational tasks and projects.

Provides support services.

Identifies and manages risks to information security tasks and project.

**Minimum Requirements**

Technical experience in cyber security, information assurance, network security, computer information systems, computer science, or management information systems.

Two or more years experience performing the duties identified above in an information technology operations of the same or larger magnitude.

Hold a bachelor's degree in computer science, information technology, management information systems or related field; or a current PMP Certification.

Knowledge and understanding of security requirements and provisioning to enable task routing according to customer’s security needs.

**Experience Levels**

Expert level: master’s degree in computer science, engineering or a related technical discipline, 8+ years of related technical experience.

Intermediate level: bachelor’s degree in computer science, engineering or a related technical discipline, 5+ years of related technical experience.

Junior level: associate’s degree in computer science, engineering or a related technical discipline, 2+ years of related technical experience

#### 1.7.2 Cyber Security Design Engineer

**Responsibilities**

Develops and recommends technical solutions to support the Office of Metro IT Security’s requirements in solving moderately complex network, platform and system security problems.

Engineers and develops secure systems including systems security requirments analysis, secure system definition and specification development based on systems security and systems engineering “best practices.”

Develops systems security engineering project plans based on systems engineering “best practices” that document system key performance parameters aligned with risk countermeasures and reliability & resiliency needs.

**Minimum Requirements**

Experience with design and development of secure enterprise communications systems.

Experience with the analysis, systems design, implementation and testing of secure enterprise information systems.

Experience in Network engineering with emphasis in design, implementation, operations and maintenance of a variety of Windows Services & AIX/UNIX Services, Application and Database servers, relevant Network Security appliances and Endpoint Security products.

• Expert knowledge of firewalls, Intrusion Prevention Systems (IPS), and Virtual Private Network (VPN) technologies;

• Expert knowledge of encryption, anti-virus, and patch management technologies;

• Specific knowledge of the Juniper Firewall NPN and related technologies;

• Specific knowledge of the Juniper Secure Socket Layer (SSL) VPN and related technologies;

• Specific knowledge of the McAfee network and host-based IPS;

• Specific knowledge of the McAfee Anti-Virus and Remediation Manager;

• Expert knowledge of various IP protocols and their behavior;

• Expert knowledge of the OSI model and Transmission Control Protocol /Internet Protocol (TCP/IP) stacks;

• Expert knowledge of network routing and switching methodologies;

• Functional working knowledge of internet content filtering;

• Functional working knowledge of wireless communications;

• Functional knowledge of analysis and system scanning tools.

**Experience Levels**

Expert level: master’s degree in computer science, engineering or a related technical discipline, 8+ years of related systems engineering experience.

Intermediate level: bachelor’s degree in computer science, engineering or a related technical discipline, or the equivalent combination of education, technical training, or work/military experience 5+ years of related systems engineering experience.

Junior level: associates degree in computer science, engineering or a related technical discipline, 2+ years of related systems engineering experience.

**1.7.3 Cyber Security Risk Analyst**

**Responsibilities**

Serves as a lead cyber and information security consultant to the project team by conducting security risk assessments and providing guidance on securing information systems, applications, and networks.

Provides technical guidance and expertise in the areas of secure application development, security risk management and assessment, security policies and standards, security architectures and implementations, and effective security risk assessment practices.

Performs application and technology design reviews, security risk assessments, requirements analysis, security testing oversight, risk remediation planning, and security project management.

Develops, reviews, and implements security risk management policies, standards, and practices.

Defines security and policy compliance requirements in supporting the acquisition and deployment of security software, systems, and services.

Provides guidance on the development and integration of a security development lifecycle (SDL) to include secure development, testing, and configuration of application and web architectures.

Review and assess other vendor’s information security solutions and deliverables, including technologies and architectures, security controls and procedures, and review contract documentation.

**Minimum Requirements**

Experience with design and development of secure enterprise communications systems.

Experience with the analysis, systems design, implementation and testing of secure enterprise information systems.

Experience in Network engineering with emphasis in design, implementation, operations and maintenance of a variety of Windows services, application and database servers, relevant network security appliances and Endpoint security products.

• Expert knowledge of firewalls, Intrusion Prevention Systems (IPS), and Virtual Private Network (VPN) technologies;

• Expert knowledge of encryption, anti-virus, and patch management technologies;

• Specific knowledge of the Juniper Firewall NPN and related technologies;

• Specific knowledge of the Juniper Secure Socket Layer (SSL) VPN and related technologies;

• Specific knowledge of the McAfee network and host-based IPS;

• Specific knowledge of the McAfee Anti-Virus and Remediation Manager;

• Expert knowledge of various IP protocols and their behavior;

• Expert knowledge of the OSI model and Transmission Control Protocol /Internet Protocol (TCP/IP) stacks;

• Expert knowledge of network routing and switching methodologies;

• Functional working knowledge of internet content filtering;

• Functional working knowledge of wireless communications;

• Functional knowledge of analysis and system scanning tools.

**Experience Levels**

Expert level: master’s degree in computer science, engineering or a related technical discipline, 8+ years of related technical experience.

Intermediate level: bachelor’s degree in computer science, engineering or a related technical discipline, 5+ years of related technical experience.

Junior level: associates degree in computer science, engineering or a related technical discipline, 2+ years of related technical experience.

#### 1.7.4 Cyber Security Operations Engineer

**Responsibilities**

Work on all systems and/or projects within the the Office of Metro IT Security which is responsible for providing network defense utilizing network and host- based computer network defense tools, appliances and end point products

Integrate security products, including designs for all organizational networks as well as designing, engineering, configuring, testing and deploying them.

Maintain system baselines and configuration management items, including security event monitoring "policies" in a manner determined and agreed to by program management.

Provide engineering documentation and software testing (patches, other updates) including interaction with analysts and operations and maintenance personnel to ensure a complete and functioning system that meets requirements.

**Minimum Requirements**

Experience conducting “proof of concept” testing and support of current infrastructure.

Experience in the design, testing, and integration of new security products and updating all network defense capabilities including patching, and security configurations.

Experience monitoring key security infrastructure elements, identifying security events, performing analyses, and initiating response activities.

Experience and knowledge of OSI layers and TCP/IP troubleshooting techniques.

Experience with Firewall and VPN techniques and protocols, Site -to-site and SSLVPN design concepts and implementation.

Technical experience in cyber security, information assurance, network security, computer information systems, computer science, or management information systems.

Solid understanding of network security concepts.

Understanding and familiarity with Security Information and Event Management (SIEM) systems.

Familiarity with intrusion detection / protection, firewalls, and anti-virus systems.

Proven understanding of network protocols.

Microsoft and Linux hosting and systems Administration experience.

• Expert knowledge of firewalls, Intrusion Prevention Systems (IPS), and Virtual Private Network (VPN) technologies;

• Expert knowledge of encryption, anti-virus, and patch management;

• Specific knowledge of the Juniper Firewall NPN and related technologies;

• Specific knowledge of the Juniper Secure Socket Layer (SSL) VPN and related technologies;

• Specific knowledge of the McAfee network and host-based IPS;

• Specific knowledge of the McAfee Anti-Virus and Remediation Manager;

• Expert knowledge of various IP protocols and their behavior;

• Expert knowledge of the OSI model and Transmission Control Protocol /Internet Protocol (TCP/IP) stacks;

• Expert knowledge of network routing and switching methodologies

• Functional working knowledge of internet content filtering;

• Functional working knowledge of wireless communications;

• Functional knowledge of analysis and system scanning tools.

**Experience Levels**

Expert level: master’s degree in computer science, engineering or a related technical discipline, 8+ years of related technical experience.

Intermediate level: bachelor’s degree in computer science, engineering or a related technical discipline, 5+ years of related technical experience.

Junior level: associate’s degree in computer science, engineering or a related technical discipline, 2+ years of related technical experience

#### 1.7.5 Application Security Engineer

**Responsibilities**

Draft security development practices.

Create maintain and monitor new applications security practice.

Perform applications security penetration testing and code review in order to identify application vulnerabilities.

Develop new applications for use by the Office of Metro IT Security to maintain and improve operations.

Develop new toolkits and examples for new security initiatives at such as SSO, Encryption Key Management, OWASP practices and library usage.

Design test scenarios and support testing of new and enhanced software products.

**Minimum Requirements**

Experience with application layer vulnerability threat analysis and tools used to discover application vulnerabilities both at coding development stage and at authorization to operate deployment testing stage.

Experience in security software engineering with specialized experience in designing, developing and/or programming security related efforts.

Experience in enterprise applications.

Experience in JAVA, C/C++, .NET, and secure coding best practices.

**Experience Levels**

Expert level: master’s degree in computer science, engineering or a related technical discipline, 8+ years of related technical experience.

Intermediate level: bachelor’s degree in computer science, engineering or a related technical discipline, 5+ years of related technical experience.

Junior level: associates degree in computer science, engineering or a related technical discipline, 2+ years of related technical experience.

#### 1.7.6 Cyber Threat Engineer

**Responsibilities**

Work on all systems and/or projects within the Office of Metro IT Security responsible for providing cyber security threat detection utilizing network and host- based computer security tools, appliances and end point products.

Maintain system baselines and configuration management items, including security event monitoring "policies" in a manner determined and agreed to by program management.

Provide documentation, software testing (patches, other updates) and interaction with other analysts and operations and maintenance personnel to ensure a complete and functioning system that meets requirements.

Perform analysis of all security systems log files, review and keeps track of triggered events, research current and future cyber threats, reconcile correlated cyber security events, develop and modify new and current cyber security correlation rule sets, and operate security equipment and technology.

**Requirements**

Experience in documenting security incidents as identified in the incident response documentation and escalating to management as required.

Experience monitoring key security infrastructure elements, identifying security events, performing analysis, and initiating response activities.

Experience performing packet analysis, identifying malformed packets and their payloads. Experience in

Integration of security products, including designs for all networks as well as designing, engineering, integrating, configuring, testing and deploying them.

Experience and knowledge of OSI layers and TCP/IP troubleshooting techniques.

Experience with Anti-Virus, Intrusion Detection Systems, Firewalls, Active Directory, Vulnerability Assessment tools and other security tools found in large network environments; experience working with Security Information and Event Management (SEIM) solutions.

Technical experience in cyber security, information assurance, network security, computer information systems, computer science, or management information systems.

Understanding of common network services (DNS, web, mail, FTP, etc.), network vulnerabilities, and network attack patterns.

Understanding and familiarity with Security Information and Event Management (SIEM) systems.

Familiarity with intrusion detection / protection, firewalls, and anti-virus systems.

Proven understanding of network protocols.

Microsoft and Linux hosting and systems administration experience:

• Expert knowledge of firewalls, Intrusion Prevention Systems (IPS), and Virtual Private Network (VPN) technologies;

• Expert knowledge of encryption, anti-virus, and patch management technologies;

• Specific knowledge of the Juniper Firewall NPN and related technologies;

• Specific knowledge of the Juniper Secure Socket Layer (SSL) VPN and related technologies;

• Specific knowledge of the McAfee network and host-based IPS;

• Specific knowledge of the McAfee Anti-Virus and Remediation Manager;

• Expert knowledge of various IP protocols and their behavior;

• Expert knowledge of the OSI model and Transmission Control Protocol /Internet Protocol (TCP/IP) stacks;

• Expert knowledge of network routing and switching methodologies;

• Functional working knowledge of internet content filtering;

• Functional working knowledge of wireless communications;

• Functional knowledge of various analysis and system scanning tools.

**Experience Levels**

Expert level: master’s degree in computer science, engineering or a related technical discipline, 8+ years of related technical experience.

Intermediate level: bachelor’s degree in computer science, engineering or a related technical discipline, 5+ years of related technical experience.

Junior level: associates degree in computer science, engineering or a related technical discipline, 2+ years of related technical experience.

## 1.8 Disclosure of Information

Contractor employees shall not discuss nor disclose any information to which they are exposed during the execution of this contract to parties other than the originator of the information, authorized WMATA investigative personnel, or COR personnel. Improper disclosure of sensitive information may be grounds for removal of Contractor personnel. The Contractor shall provide the COTR and COR, a signed non-disclosure agreement (NDA) for each individual Contractor employee before the employee begins performance.

## 1.9 Training

The Contractor shall provide qualified personnel who are capable of performing their duties identified in each of the labor category classifications . Training for contractor personnel will be at the contractor’s expense. All training requirements must be coordinated with the COTR. Training labor and travel expenses shall be coordinated and approved in advance by the COTR and COR, approval will be at the WMATA’s discretion.

# PART 2: WMATA FURNISHED ITEMS AND SERVICES

2.1 Facilities, Supplies and Services- WMATA will supply office space, office supplies, computer equipment and telephones when the Contractor is working on-site to the extent permitted by WMATA and Contractor.

## 2.2 Information

WMATA will provide the Contractor withcopies of, or access to, all required directives, publications, and documents, as available. WMATA will also provide Contractor necessary and reasonable access to their personnel.

## 2.3 Materials

Materials shall be provided by the Contractor when essential to the task performance. All materials purchased by the Contractor for the use or ownership of WMATA will become property of WMATA. The Contractor shall document the transfer of materials in the monthly progress report and appropriate WMATA documentation.

# PART 3: CONTRACTOR FURNISHED ITEMS AND SERVICES

## 3.1 Security

Contractor personnel shall be required to have access to sensitive material. Information or data that the Contractor accesses shall be handled at an appropriate classification level. Contractor personnel shall abide by all published WMATA policies and instructions.

## 3.2 Identification Badges

Contractor identification badges shall be issued by WMATA to on-site Contractor personnel and shall be visible at all times while personnel are at the WMATA work site. The Contractor shall furnish all requested information required to facilitate issuance of identification badges and shall conform concerning the use and possession of badges. The Contractor is responsible for ensuring that all identification badges issued to its employees are returned to the Security Department at the WMATA site in accordance with WMATA Policy following completion of the task order, relocation or termination of an employee, or upon request from the COTR.

## 3.3 Contractor Access

WMATA will provide the Contractor with access to WMATA facilities, as required, for performance of tasks under this Contract.

## 3.4 Organizational Conflict of Interest

WMATA requires that a Contractor-provided Organizational Conflict of Interest (OCI) mitigation plan be submitted at the time of its proposal. All Contractor personnel must receive company sponsored OCI training within fourteen (14) calendar days after contract award. NDA requirements are stated in the “Disclosure of Information” section.

## 3.5 Telework Availability

Telework eligibility will be authorized on a case by case basis, by the COTR.

## 3.6 Limitations on Contractor’s Responsibilities

The COTR will exercise all signatory and decision making authority regarding the assigned workload. The COTR shall monitor all work in progress to ensure correctness and completeness. Contractor personnel will be provided with Contractor support guidelines explaining prohibitions on personal services contracting and inherentlyWMATA functions.

The Contractor shall not:

* Approve, decide or sign as a Contracting Officer;
* Negotiate and/or obligate WMATA or its funding with suppliers;
* Accept or reject supplies or services;
* Determine disposal of WMATA property;
* Determine cost reasonableness, allowability or allocability;
* Vote on a source selection board; or
* Determine policy

Under the guidelines of non-personal services contracts, the COTR shall have technical, not supervisory, oversight of Contractor personnel.

# PART 4: SPECIFIC TASKS

## 4.1 Performance Requirements

The Contractor shall perform Cyber Security Program services such as enterprise monitoring and defense, risk management, identity management, cyber operations and application security in order to protect the confidentiality, integrity and availability of WMATA’s resources. The Contractor shall assess risks to identified IT assets utilizing available threat and vulnerability information and provide risk recommendations as well as technical expertise & capability to identify security-related issues of current and planned systems and networks and associated architecture on WMATA’s enterprise and industrial networks.

The Contractor shall remain current on technological advances relevant to the requirements they support and provide documented recommendations where appropriate. All services shall be performed in accordance with appropriate WMATA, federal, and PCI initiatives, standards, policies and mandates.

The Contractor shall successfully integrate and coordinate all activity necessary to execute the tasking within this performance work statement.

#### 4.1.1 Cyber Security Program Management

The Contractor shall provide on-site program management (expert level of knowledge in Cyber Security) who shall be responsible for management and oversight of work performance under this Task Order. The Program Management function responsibilities include:

1. Serve as a point-of-contact for customer relations.
2. Ensure adequate program controls are applied to each task area including resource allocation, direction, cost ,quality control, report preparation, record keeping and resolution of customer complaints.
3. Resolve quality, timeliness, and accuracy issues.
4. Ensure quality prior to WMATA submission.
5. Attend meetings with the COR / COTR to discuss the resolution of any perceived performance problems.
6. Perform project management functions.

#### 4.1.2 Enterprise Monitoring & Defense Services

The Contractor shall provide Enterprise Monitoring & Defense(EM&D) support services for WMATA networks under the Office of Cyber Security’s purview. The Contractor shall perform the following duties:

1. Provide technical /analytical recommendations for improvements to current EM&D operations.
2. Perform EM&D indicator reporting, incident handling and reporting.
3. Provide system enhancement and engineering design.
4. Perform incident response processes.
5. Provide a roadmap for architectural changes that support process improvements, such as consolidation of event data from monitored networks and elimination of manual tasks associated with transitioning between systems.
6. Provide insight into evolving threats, vulnerabilities, countermeasures and industry trends while making recommendations on future direction for the cyber security program.

#### 4.1.3 Cyber Security Risk Management Services

The Contractor shall deliver risk assessment analysis to the appropriate WMATA team lead as project milestones are reached. The Contractor shall execute the following, high level processes for Risk Management :

The WMATA team lead will assign a list of projects in various departments to the Contractor based on milestone expiration dates for the current calendar year. The Contractor shall partner with departmental personnel to define a risk program plan for that particular evaluation and create a project plan based on WMATA’s format.

As the Contractor receives data/deliverables from departmental personnel, the Contractor shall perform a risk assessment based on WMATA Risk Management Compliance Instructions & Directives within five (5) business days of receipt.

#### 4.1.4 Identity Management Services

Create an Identity Management Program Plan/Integrated Master Schedule.

As part of establishing an Identity Management Program Plan for Metro using the Oracle Identity and Access Management Suite, the Contractor will assist Metro in reviewing, designing, building, and implementing

three major functional areas:

**Identity Management:** This function will be responsible for establishing and cancelling accounts, password management, providing a self-service functionality, and centrally enforcing identity policies and procedures. In this function, Metro strives to improve management and administration of all identities affiliated with Metro’s roles, group membership, and user data.

**Access Management:** This function will manage and streamline authentication, authorization, and identity federation processes across the entire organization. An effective Access Management solution will reduce overhead and simplify the integration of new applications and services with these functions.

**Audit, Reporting, Compliance and Governance:** This function will streamline, automate, and simplify the reporting of identity data. Using systems provided, WMATA is striving to reduce time and overhead in reporting and responding to audit requests and ensuring compliance with regulatory requirements.

**1. Simplify the End User Experience**

a. Map accounts and unify/reduce the number of different passwords a user

maintains.

b. Provide centralized self-service password reset capabilities for all Metro users.

c. Enable Single Sign On for enterprise applications.

d. Expedite access management enablement process for the end user.

**2. Establish an Audit and Compliance Ready Access Management Environment**

a. Minimize administrator and infrastructure personnel overhead required to

support the audit process.

b. Centrally generate Audit reports for users' Access across enterprise applications.

c. Prevent excessive permission requests through enforcement of a centralized access request process.

**3. Streamline User and Role Life Cycle Management Process**

a. Streamline and automate establishment and cancellation of user accounts across enterprise applications.

b. Link the user's identity and access privileges across enterprise applications including PeopleSoft HCM and physical security badges.. .

c. Enable access requests, grant, approve, delegate, re-certify and/or terminate tasks through a centralized online portal.

The detailed task list is as follows:

**Work Stream I - Provisioning and Identity Aggregation**

Ongoing Responsibilities (across all work streams)

* Consult on Best Practices and Thought Leadership (IAM Expert recommendations);
* Provide Customer Mentoring/Training;
* Support Documentation development;
* Provide Project Planning;
* Provide Schedule and Financial Tracking;
* Issue Escalation and Resolution Procedures;
* Provide Communications Management Analysis/ Design
* Finalize requirements
* Provide gap analysis using case definitions;
* Provide application, data store, OS inventory;
* Create Detailed Design;
* Create Test Plan.

Implementation:

* Install and configure secure, robust identity and cccess management platform;
* Provide IAM Platform integration with PeopleSoft HCM, Physical Access Card, Active Directory (AD) and Single Sign On Directory;
* Automate establishment and cancellation of accounts across PeopleSoft HCM, Physical Access Card, AD, Exchange, Single Sign On Directory and Maximo;
* Configure Self Service functionality for Employees and Contractors;
* Configure Password Reset .functionality for Help Desk personnel and IT

Administrators;

* Configure email notifications such as password expirations.

QA

* Provide Production Deployment in HA and DR Environment.

**Work Stream II - Access Management and Strong/Multi-Factor Authentication**

Roadmap

* Provide Single Sign Solutions for multiple PeopleSoft applications, SharePoint Portal 2007,. IBM Maximo, Documentum and various .NET and Java based Agency applications;
* Integrate with Oracle Identity Manager;
* Integrate with Juniper VPN;
* Integrate with Oracle Adaptive Access Manager.

QA

* Product Deployment in HA and DR Environment.

**Work Stream III – Role Management, SoD and Recertification**

* Provide Project Management;
* Create Extended Design with HA and .DR capabilities.

Roadmap

* Manage direct report access recertification/attestation processes;
* Access cleanup notification workflows as a result of recertification processes;
* Provide roadmap for OIM/OIA Integrations;
* Institute Role Mining and OIA-OIM Integrations.

QA

* Production Deployment in HA and DR Environment.

**Work stream IV - System Administration**

Roadmap

* Monitor IAM/SSO servers for performance and tune applications as needed based on results obtained.
* Patch the IAM/SSO development, QA and production servers for monthly Windows updates, provide quarterly Oracle critical patch updates, and security updates for Windows, Java and Oracle components.
* Monitor establishment and cancellation of user accounts using OIM as well manual implementation on *ad hoc* basis.
* Monitor the SSO proxy servers for high traffic and loads and take necessary steps to avoid any proxy server failures.
* Perform quarterly comparisons of user's data and status in IAM with the user's data and status in system of records i.e. PeopleSoft HR and Prowatch and take corrective steps in IAM, if needed.
* Provide on-call support in case of planned/un-planned system failures, system outages, data center outages and restore system functionality. Prepare incident response documents for each incident.
* Regularly update and maintain the IAM/SSO system documents, code repositories and project plans.
* Report the IAM/SSO system status on a weekly and *ad hoc* basis.

## 4.2 Procedures and Guides

The Contractor shall document and update Standard Operating Procedures (SOPs) and Work Instructions for each position within all task order functional areas. The Contractor shall outline the changing processes within the functional areas and electronically store updates for WMATA’s access, as directed by the COTR.

Standard Operating Procedures and Work Instructions

The Contractor shall provide a monthly status report to summarize its accomplishments during the reporting period and clearly demonstrate that the Performance Requirements Summary (PRS) objectives were satisfied for the reporting period. The report shall also include planned vs. actual task completion to include milestones, anticipated activity (including anticipated deliveries) for the next reporting period, lessons learned, risks, outstanding issues and recommendations. In addition, the Contractor shall provide financial resource reporting as follows:

The Contractor shall provide information to include cost details for Item/Name, Description, Unit Cost, Number of Units, and Extended Costs for ODC’s/Material, etc.), financial status of cost deliverable (i.e., funding applied, expenses incurred during current reporting period, total expenses to date, amount remaining, etc.) and forecast of funds depletion by type based on known requirements.

Status and financial reporting will be in accordance with each deliverable as follows: Cyber Security Program Management, Enterprise Monitoring & Defense, Cyber Security Risk Management, and Identity Management Services.

Monthly Status Report.

# PART 5: CONTRACT DELIVERABLE REQUIREMENTS LIST

## 5.1 Contract Deliverables All deliverables must meet professional standards and the requirements set forth in contractual documentation. The contractor shall be responsible for delivering all end items specified unless otherwise directed by the COR / COTR.

|  |  |
| --- | --- |
| Job Title | Monthly Deliverables: |
| 4.1.2 | Incident Remediation Report |
| 4.1.2 | Threats & Vulnerabilities Analysis |
| 4.1.4 | Identity Management Program Plan/Integrated Master Schedule |
| 4.2 | Standard Operating Procedures and Desk Guides |
| 4.2 | Monthly Status Report |
| 4.1.3 | Cyber Security Risk Management Report(s) |
|  |  |

# PART 6: PERFORMANCE REQUIREMENTS SUMMARY (PRS)

## 6.1 Performance Requirements Summary (PRS)

The Contractor’s service requirements are summarized into performance objectives that relate directly to mission essential items as well as performance thresholds which briefly describe the minimum acceptable levels of service required for each requirement. A PRS is provided below and outlines the performance objectives, performance thresholds, surveillance methods, and associated performance determinations/payments.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance Objective | Performance Threshold  (Satisfactory Performance) | Method of  Surveillance | Performance Determinations (Corrective Action Plans) |
| PRS #1 (PWS Part 5)  Excellent staffing stability and resource planning. | Management of personnel (retention, replacement, etc.) does not negatively impact quality or timeliness of products and services across the program. | 100% Inspection of applicable CDRLs by COR with COTR input.  Customer Feedback | Contractor will immediately establish (WMATA) acceptable Corrective Action Plan within five (5) working days. If WMATA determines that the Contractor’s attempt to resolve the issue is not acceptable, 15% of the monthly payment may be withheld upon Contracting Officer’s review and direction. |
| PRS #2 (PWS Part 5)  Consistent high quality deliverables. | Deliverables were accurate, complete and incorporate all pertinent data with no or only minor adjustments required by WMATA.  Any errors / omissions identified by WMATA are corrected within ten (10) business days. | 100% Inspection of applicable CDRLS by COR with WMATA input.  Customer Feedback | Contractor will immediately correct or establish (WMATA) acceptable Corrective Action Plan within five (5) working days. If the Contractor’s attempt to resolve the issue is not acceptable to WMATA, 15% of the monthly payment may be withheld upon Contracting Officer’s review and direction. |
| PRS #3 (PWS Part 5)  Required deliverables and services were provided according to schedule. | Services and deliverables were submitted according to, or ahead of, agreed upon schedule. Exceptions were due to circumstances outside of the Contractor’s control. | 100% Inspection of applicable CDRLS by COR with COTR input.  Customer Feedback | Contractor will immediately correct or establish (WMATA) acceptable Corrective Action Plan within five (5) working days. If the Contractor’s attempt to resolve the issue is not acceptable to WMATA, 15% of the monthly payment may be withheld upon Contracting Officer’s review and direction. |
| PRS #4 (PWS Part 5)  Positive Business Relations, Customer Satisfaction, Timely and Open Communication and effective Task Order performance coordination with other supporting vendors. | The Contractor was responsive to WMATA concerns and promptly applied corrective action to performance issues.  The Contractor provided timely notification of issues and/or items requiring WMATA’s action.  The Contractor coordinated all applicable tasking with other supporting vendors. | Customer Feedback  COR / COTR Input | Contractor will immediately correct or establish (WMATA) acceptable Corrective Action Plan within five (5) working days. If the Contractor’s attempt to resolve the issue is not acceptable to WMATA, 15% of the monthly payment may be withheld upon Contracting Officer’s review and direction. |
| PRS #5 (PWS Part 5)  Timely, Accurate and Complete Program Reporting | Monthly Status Report is delivered on time and meets all PWS content requirements. | 100% Inspection by COR with COTR input. | Contractor will immediately correct or establish (WMATA) acceptable Corrective Action Plan within five (5) working days. If the Contractor’s attempt to resolve the issue is not acceptable to WMATA, 15% of the monthly payment may be withheld upon Contracting Officer’s review and direction. |

# PART 7: TRANSITION PLAN

## 7.1 Planning

The Cyber Security Transition Plan will minimize the impact on current mission activities while ensuring the completeness of the transition, assess its impact on WMATA, define the activities that need to be accomplished, define the roles and responsibilities of all participants, provide a detailed schedule to be followed and describe how any issues or discrepancies will be resolved.

## 7.2 Transitioning Strategy

The transition strategy shall maintain the Office of Metro IT Security’s mission with minimal impact on timeliness of processes while ensuring that critical data and knowledge transfer occurs. It will serve as the framework for IA Support task order execution. At a minimum the following areas shall be addressed:

1. Task Order Leadership;
2. Key positions;
3. Materials transfer;
4. Knowledge transfer;
5. Information /data transfer;
6. Impact;
7. Risk;
8. Schedule.

## 7.3 Phase-In

A smooth and orderly transition between the Contractor and the predecessor Contractor is necessary to assure minimum disruption to vital Contractor services and WMATA activities.

The Contractor shall not disrupt official WMATA business or in any way interfere with the assigned duties of the predecessor Contractor’s employees. The Contractor may notify the predecessor Contractor’s employees that the Contractor will be assuming services upon the Contract start date. The Contractor shall not interview, recruit, schedule interviews or conduct extensive discussions with the predecessor Contractor’s employees while they are on duty.

WMATA will allow a maximum of thirty (30) days for transitioning planning activities prior to Period of Performance (PoP) start.

# PART 8: DEFINITIONS & ACRONYMS

ACOTR – Alternate Contracting Officers Technical Representative

Best Effort – Effort expended by the Contractor to perform within the awarded ceiling price all work specified in individual task orders and all other obligations in the basic contract.

CIO – Chief Information Officer

COR – Contracting Officer’s Representative

COTR- Contracting Officers Technical Representative

Defective Services – A service that does not meet the standard of performance associated with it in the Performance Work Statement.

EM&D- Enterprise Monitoring & Defense

FFP – Firm Fixed Price

IT – Information Technology

Major Incidents – A major incident is an incident that has severe impact to departmental operations and may require significant effort to correct beyond normal business hours.

Minor Incidents – A minor incident has low impact to departmental operations and may be corrected during normal business hours.

NDA – Non-Disclosure Agreement

Normal Business Hours – 0800 to 1700 Monday through Friday

NTE – Not To Exceed

OCI – Organizational Conflict of Interest

PCI – Payment Card Industry

PD – Position Description

PoP – Period of Performance

PRS – Performance Requirements Summary

PWS – Performance Work Statement

QA – Quality Assurance - Actions taken to assure services meet the requirements of the Performance Work Statement.

QASP – Quality Assurance Surveillance Plan – An organized written document specifying the surveillance methodology to be used for surveillance of Contractor performance.

Quality Control – A plan prepared by the Contractor to control the performance of services so that they meet the requirements of the Performance Work Statement.

QCP – Quality Control Plan – An organized written document submitted as part of the proposal to illustrate how the Contractor shall meet the requirements of the Performance Work Statement.

WMATA- Washington Metropolitan Area Transit Authority.