SECTION I – STATEMENT OF WORK

1.1 Introduction

The Diversion Information Technology Section (TGD), provides innovative IT solutions to support the mission of the Diversion Control Division (DC). The Diversion Control Program (DCP) is the mission of DC, whose purpose is to prevent, detect, and investigate the diversion of pharmaceutical controlled substances and listed chemicals from legitimate channels while ensuring an adequate and uninterrupted supply of pharmaceutical controlled substances and listed chemicals to meet legitimate medical, commercial, and scientific needs. A complete history of the DCP is provided in Exhibit 7, and includes information on the statutory requirements governing the program, the organizational structure, and the functional statements of DC, which includes specific information on the responsibilities of each section within DC.

1.2 Scope

This contracting effort directly impacts the DCP's mission, which is a major enforcement effort of the DEA. The DC is mandated by law to enforce the Controlled Substances Act by preventing the diversion of controlled substances and listed chemicals. Currently, the information technology applications are used on a daily basis by DEA personnel throughout the United States to monitor the manufacturing and distribution of legitimately produced pharmaceuticals and listed chemicals. The Contractor shall provide the support necessary to improve the information technology infrastructure and the associated administrative business processes in DC to enhance DEA's ability to accomplish its mission.

1.3 Objective

The purpose of this contract is to obtain the services of a qualified information technology vendor to provide the continuous modernization, maintenance, and enhancement of DC's IT applications and infrastructure.

1.4 Background

In October 1970, Congress passed the Comprehensive Drug Abuse Prevention and Control Act, better known as the Controlled Substances Act (CSA), to consolidate and replace more than 50 pieces of national drug legislation. The CSA went into effect on May 1, 1971. The Drug Enforcement Administration (DEA) was established in 1973 to serve as the single Federal agency to coordinate the Federal government's drug control activities.
In support of the DEA's overarching mission to enforce the mandates of the CSA, the Diversion Control Division's (DC) specific responsibilities are to prevent, detect, and investigate the diversion of pharmaceutical controlled substances and listed chemicals from legitimate channels. The DC ensures that an adequate and uninterrupted supply of pharmaceutical controlled substances and listed chemicals meet legitimate medical, commercial, and scientific needs. Activities in support of DC's Diversion Control Program (DCP) and its mission include:

- Determination of program priorities
- Field management oversight
- Coordination of major investigations
- Drafting and promulgating regulations
- Support in the design and proposal of national legislation

- Advice and leadership on state legislation/regulatory initiatives
- Oversight of the importation and exportation of controlled substances and listed chemicals
- Establishment of national drug production quotas
- Activities related to drug scheduling and compliance with international treaty obligations
- Designing and executing diplomatic missions
- Automated monitoring and tracking of the distribution of certain controlled substances
- Planning and allocation of program resources
- Liaison efforts with industry and their representative associations as well as the DEA's regulatory and law enforcement counterparts at the federal, state, and local levels.

A more comprehensive discussion of the history of the DEA and the Diversion Control Division is provided in Exhibit 8.

1.5 Current Information Technology Environment

To meet the mission of both the agency and the Diversion Control Division, the use of Federal Information Processing resources is critical. DEA's Information Systems Division provides general Information Technology (IT) services for the agency, while the Diversion Information Technology Section (TGD) provides specialized IT services in sole support of the Diversion Control Program.

1.5.1 Diversion Control Infrastructure (DCI)

The Diversion Control (DC) infrastructure provides the technical framework to support DC mission-critical systems. These systems require a high-level of technical discipline and management to ensure operational availability to the Division. The DC infrastructure is a wholly contained network environment with limited interfaces to non-Department of Justice (DOJ)/DEA resources. The DC infrastructure utilizes the DOJ Justice Unified Telecommunications Network (JUTNet) for Wide Area Network (WAN) connectivity with the DOJ Trusted Internet Connection (TIC) for connectivity and filtering of all external traffic. The primary DC infrastructure is located at the Sterling Park Technology Center (SPTC), Sterling, Virginia, with external connectivity provided through the gateway cluster at the Equinix facility in Ashburn, Virginia. Additionally, DEA maintains an Alternate Compute Facility (ACF) located in Dallas, Texas that provides disaster recovery capability for mission-critical applications. Disaster recovery capability has been implemented within the ACF for all DC's mission critical systems.

The DC infrastructure consists of two (2) primary networks: RSN and CSOS. Each network consists of two (2) tiers: an external, public internet-facing Demilitarized Zone (DMZ) component, and a primary, internal, government-exclusive component. TGD implements government-required security controls and standards between defined boundaries. Each network hosts one or more systems and applications. The Registrant Support Network (RSN) within the DC infrastructure is categorized as a moderate control baseline per NIST Special Publication 800-53. Accordingly, applications and the Diversion Control Division website security controls are inherited from RSN, and appropriate controls are applied to assist with the privacy protection and risk reduction of unauthorized access and disclosure. The Controlled Substance Ordering System (CSOS) within the DC infrastructure is categorized as a moderate control baseline based on NIST Special Publication 800-53. Appropriate controls are applied to assist with the privacy protection and risk reduction of unauthorized access and disclosure.

The DC infrastructure consists of a Nutanix hyperconverged platform which supports 450 virtual servers using both VMWare and the native AHV hypervisor as well as approximately 115 servers on various HP and Cisco Unified Computing System (UCS) hardware configurations. The physical servers are a mixture of database,

virtualization hosts, and vendor appliance servers. Servers operating systems consist of a combination of Microsoft Windows Server and Red Hat Enterprise Linux (RHEL). CommVault and Cohesity provide a comprehensive backup strategy to provide data recovery within the DC infrastructure. Backups are copied and stored for short-term retention, and to tape library for long-term retention. Both disk-based storage and tape libraries are housed at the SPTC facility in Sterling, Virginia.

Diversion Control Infrastructure (DCI) network services consist of both hardware and software, including Local Area Networks (LAN)/Wide Area Networks (WAN), Cisco routers, Cisco switches, Cisco firewalls, DMZs (demilitarized zones), F5 appliances, and Intrusion Detection System (IDS). The infrastructure supports the Cisco unified Internet Protocol (IP) Interactive Voice Response (IVR) for internal/external Registrant Support Network (RSN) and internal/external Controlled Substance Ordering System (CSOS) Domain Name Servers (DNS) in the environment.

The DCI utilizes an IBM Data Warehouse system for the Diversion Division's (DC), Automation of Reports and Consolidated Orders System, to store transactional and CSA registrant data in a robust appliance optimized for complex analytical analysis. The Targeting and Special Projects Section of DC, evaluates current diversion trends both nationally and internationally to proactively plan and assist the field in target investigations, which is critical to support criminal and civil cases. The Data Warehouse system is comprised of the following IBM components: Cognos Analytics, Cloud Pak for Data, Netezza Performance Server, DataStage, and Informatica's Fast Clone.

In addition to the infrastructure support, TGD also provides specific IT support for the following major programs.

1.5.2 Diversion Call Center Support

The Interactive Voice Response (IVR) infrastructure provides the backbone for the DC Call Centers. The IVR provides after-hours customer support and facilitates Call Center staff response to customer support inquiries. The IVR operates entirely in a VMWare ESXi virtual host environment with a Cisco Unified Contact Center product suite, Nuance voice recognition and Calabrio call recording solution for physical and remote call recordings to provide comprehensive call management, , and after hours call forwarding to the caller's local field office Monday through Friday from 5:50pm to 8:00pm Eastern Time.

1.5.3 Print on Demand (POD)

POD is a printing and mailing solution that helps fulfill the Office of Diversion Control's (DC) mission. A responsibility of DC is to issue registration certificates and order forms for controlled substances to individuals and organizations authorized to distribute controlled substances and List I chemicals. Using high-capacity track-fed printers; POD is designed to print a high volume of certificates, forms, and letters in a timely manner. POD then prepares these documents for mailing, which includes folding, inserting, and metering. POD uses Quadient Inspire Designer and Content Manager to enable management of customer communications from a single, central platform. Ricoh Process Director (RPD) print workflow software is used to control processes and print devices from multiple vendors via a web-based dashboard. RDP integrates with composition software, inserters, and other systems with industry-standard password management and LDAP/AD integration. After RPD processes jobs, Business Computer Center (BCC) Manager calculates the postage statement, which goes to post office to inform them of the total postage cost.

1.5.4 Geographic Information System (DCEGIS)

Diversion Control Enterprise Geographic Information System (DCEGIS) provides improved spatial analysis and data reporting for DC staff members. DCEGIS provides accurate GIS location records of the Controlled Substance

Act (CSA) along with registrant population. DCEGIS provides a web-based framework that makes map making and spatial analysis easily accessible to end users while also allowing them to upload and publish their own data, create

maps, and run analysis as needed. The Environmental System Research Institute (ESRI) fulfills the enterprise GIS requirements, through its Basemaps, and Pitney Bowes provides the primary address validation and geocoding services. In addition, the DCEGIS server stack utilizes the ESRI World Geocoder to allow end users to upload non-geocoded address source data for web maps, applications and analysis.

1.5.5 National Forensic Laboratory Information System (NFLIS)

The National Forensic Laboratory Information System (NFLIS) provides a systematic approach for collecting data on drug analyses conducted by federal, state, and local forensic laboratories, and is a platform for participants to submit reports on controlled substance analyses conducted. The system provides tools for geo-mapping the data to provide regional context for DEA field operatives and management teams. DC personnel query, analyze, compile, and report on the information submitted. The current production NFLIS system includes two (2) configurations, SQL Server/.NET/IIS and Oracle 19c/Java/JBoss. The JBoss/Java based NFLIS system is the recently redesigned website that hosts the NFLIS public pages and the Data Query System; data processing for the NFLIS-TOX data collection is performed in Oracle 19c. The .NET based site is still active for the Case Management System, NFLIS Web Data Entry, and the File Upload and Transfer tools; NFLIS-Drug data processing is currently performed in SQL Server.

1.6 Future IT Environment

DEA is committed to exploring new and innovative technologies for gathering, storing, managing, analyzing, and exploiting data and intelligence in furtherance of its mission. DEA's plan to modernize its IT systems is mandated by Executive Order, Congressional legislation and by the expansive need to quickly and accurately predict and react to civil infractions and criminal threats. The Contractor must demonstrate their ability to adapt to the extremely dynamic environment of a modern, future-looking, law enforcement administration.

1.7 Project Requirements - General

A complete list of DC's current operating applications are included in Exhibit 1.

1.7.1 Core System Component Development

The Contractor shall provide full support for all DC IT systems. The following tasks deal with innovative planning for the next generation, development, enhancements, maintenance, and support of selected DC IT applications and infrastructure.

1.7.2 Network System Administration

The Contractor shall be responsible for administering the Registrant Support Network (RSN), which is DC's primary network environment, to maintain the its availability, its support to the DEA and DC customers, and the security and integrity of the information stored within the environment. These administrative activities include, but are not limited to: file management/maintenance, software management (to include installation of new and upgrade of existing software), implementation of new hardware components into the environment, management and maintenance of existing hardware (various platforms), and continually optimizing the configuration of the network.

The contractor shall provide network management and operational support to monitor network performance, identify potential problems, and perform resource load balancing. Support shall also include troubleshooting to ascertain maintenance needs to be performed on all equipment incorporated into the network, configuration management, and systems integration of new and existing customers. The Contractor shall conduct analyses of

network functions and failures in an effort to isolate problem areas, determine and perform corrective actions required, and define and document findings. This shall also include backup and recovery of disk storage. Under the direction of the government, the contractor shall coordinate with other contractors or agencies that are developing software on the network for DC supported customers. The contractor shall be prepared to provide instructions to the end-users in all aspects of the backup processes. The contractor shall ensure that the information resources contained on supported networks are restorable in the event of equipment failures.

The Contractor shall assist DC in providing efficient, effective, reliable, and responsive configuration, installation, and troubleshooting of hardware and software support services in accordance with this SOW and shall participate in the planning and preparation of IT continuity measures, response actions, and restoration activities to ensure the continuation of DEA mission essential functions.

1.7.3 System Administrators and Network Administrators (SA/NA)

System Administrators (SAs) and Network Administrators (NAs) must be trained, experienced, and currently certified on the Information Systems that they are required to maintain. The SA/NA shall enforce system access, operation, maintenance, and disposition in accordance with applicable federal regulation and policy.

The SA or NA shall:

- verify that personnel meet required security clearance, authorization, mission requirements, and obtain supervisory approval from the GPM or COR before granting access to the Information System
- report security violations and incidents to DC management and to IS as required by DEA's Incident and Intrusion Reporting
- perform scanning and vulnerability assessments of network assets with approved software and authorization
- ensure secure configurations to include all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and, after GPM or COR approval, proactively update systems with fixes, patches, definitions, and service packs
- ensure any system changes resulting from updating or patching are documented prior to implementation
- maintain current anti-virus (AV) engines and definitions on all ISs
- manage and review user accounts, access, and logins and suspend or terminate accounts in accordance with policy guidelines
- obtain approval from the GPM or his/her designee for any accounts to be suspended or terminated
- remove inactive accounts that exceed 45 days and departing customers' accounts on the day of departure
- manage, enforce, and audit all account passwords, permissions, inactivity, and suspension policies
- remove or disable all default, guest, and service accounts in ISs or network devices, and rename administrative accounts as applicable
- use separate accounts for SA/NA privileged level and general user access
- review IS and network audit logs and log files, and report anomalous or suspicious information to the DEA Program Manager and the Contractor Program Manager
- monitor IS performance to ensure that recovery processes, security features, and procedures are properly restored after an IS has been rebooted
- monitor IS performance to ensure that processes, security features, and operating system configurations are unaltered
- ensure configuration management for security-relevant IS software (including IS warning banners) and the hardware to support is maintained and documented
- implement and test IS and data backup procedures for integrity and prohibit attempts to strain or test security mechanisms or to perform network line or keystroke monitoring without authorization

- establish audit trails, conduct reviews, and create archives as directed by TC or DC
- provide a monthly report to the GPM of active and disabled accounts listing all user accounts and any action performed
- assist with property accountability as necessary

1.7.4 Database and Application Support

The DC requires data processing systems to be standardized to common software and user interfaces wherever possible. The Contractor, with direction from the GPM or COR, will administer, support, and maintain all databases and applications. In addition, the Contractor shall:

- Ensure that any changes minimize adverse effects on other systems and maintain requirements mandated by DEA.
- Design and maintain databases and applications in support of an enterprise architecture.
- Provide On-line Transaction Processing (OLTP) and On-line Analytical Processing (OLAP) topology to ensure fast query processing, maintaining data integrity in a highly transactional process measurable by the number of transactions per second, as well as an efficient query of complex transactions that involve aggregations for data analysis
- Conduct continuous performance monitoring to track the integrity and availability of all systems. All test results, as well as software discrepancies, shall be logged for reporting as outlined in the deliverables of the contract
- Migrate from waterfall development model to a CI/CD pipeline according to DEA requirements
- Architect and maintain a database normalization and standardized data dictionary for all databases
- Coordinate enhancements and revisions to databases, applications, data warehouses, etc., and actively assist with accreditation and certification
- Ensure current versions of approved software are in use and advise government of new versions of software and maintenance coverage
- Provide/maintain fully operational database and application infrastructure and products
- Maintain and monitor security to ensure that applications, databases, and the processes by which these elements are developed, tested, deployed, and operated are compliant with government mandates

1.7.5 Website Development, Management, and Maintenance

The DCWEB (www.deadiversion.usdoj.gov) is DC's public website and serves as a link between DEA and the public. The DCWEB provides both static cont ent as well as access to Internet-facing applications. The static content is primarily Diversion Control information for public consumption while applications allow registrants to submit information and reports to DEA. In addition, DC manages these other outward facing websites: www.deaecom.gov, www.NFLIS.deadiversion.usdoj.gov, and www.synthopioids.NFLIS.deadiversion.usdoj.gov

The Contractor shall:

- Maintain and support existing Diversion websites
- Update GUI to improve usability
- Update website software including server patches and updates
- Maintain and improve existing applications
- Maintain required artifacts to assist with Certification and Accreditation
- Use Public Key Infrastructure (PKI) technology, as necessary, to control access and ensure all transactions are encryptedMaintain a detailed log of all inquiries/responses and security incidents

- Maintain and implement necessary security requirements
- Alert the COR, the GPM(s), and a TGD representative on security measures and vulnerable areas
- Maintain a statistical report on website activity (Traffic Report)
- Provide on-call support 24 hours a day, 7 days a week by providing the manpower needed to maintain a 24/7 operation. The work functions necessary to support this task will require work to be conducted at the DEA Headquarters, SPTC, or the Department of Justice Data Center in Rockville, Maryland and other locations as required
- Maintain fully functional interactive websites
- Maintain and update the NDDRS database and bulletin-board, if required
- Create, maintain, and update additional web forms as required
- Provide the GPM and/or COR with on demand reports regarding the status of the website
- Comply fully with 508 requirements and federal regulation and policy

1.7.6 Certification and Accreditation

The Contractor shall prepare all necessary documentation for obtaining and maintaining Certification and Accreditation (C&A) of all DC systems. The Contractor shall coordinate the preparation and submission of the C&A package with the Office of Security Programs, Information Security Section. All documents will be reviewed and approved by the COR, the GPM and/or a DC representative prior to publication.

The certification package must contain the final copies of the required documentation for review by the Certifying Official. These documents are prepared with certification evidences, deciding on the acceptability of IT safeguards, approving corrective actions, insuring the corrective actions are implemented, and making the accreditation decision. The following documentation is developed and or identified for all DEA Systems Security Authorization Agreement (SSAA) certification packages:

- Facilitated Risk Assessment Process (FRAP)
- Security Test and Evaluation (ST&E)
- Requirements Traceability Matrix (RTM)
- Security Policy
- Rules of Behavior (ROB)
- Security Features User's Guides (SFUG) for Administrators and Users
- Continuity of Operations Plan (COOP)
- Security Awareness and Training Plan
- Personnel and Technical Security Controls
- Incident Response Plan
- (Applicable) Memoranda of Agreement/System Interconnection Agreements
- Certification Statement
- Accreditation Statement

In addition to the documentation developed in an SSAA, the following security documentation must also be provided to the Information Security Section (ISI) to support the certification activities:

- System Security Plan (SSP)
- Privacy Impact Assessment
- Waivers (where applicable)
- Configuration Management (CM) Plan

- Concept of Operations (CONOPS)

1.7.7 Continuity of Operations, IT Incidence Responses, and Disaster Recovery Plans

The Contractor shall work with the government to ensure that all IT systems covered by the SOW are included in the DOJ, DEA, DC and other IT systems' Continuity of Operations Plan (COOP), IT Incidence Response Plan (ITRP), and Disaster Recovery Plan (DRP). The contractor shall assist in the preparation of these plans by providing technical guidance and must be prepared to participate in the implementation of the plans should a disaster occur.

1.7.8 IT Security Support

The Contractor shall provide IT security support that complies with the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Department of Justice (DOJ), Drug Enforcement Administration (DEA), Office of Management and Budget (OMB), and with Federal Bridge Certification Authority (FBCA) guidance, directives, policies and procedures, as well as all applicable DOJ/DEA requirements pertaining to the certification, accreditation, maintenance, and continuous monitoring of all Federal Information Systems.

The Contractor shall provide:

- System Security Life Cycle (SSLC) development and support
- SSLC certification phase support
- SSLC accreditation phase support
- Continuous monitoring of controls support
- System security plans development and support
- System security policy and procedure development and support
- Security controls assessmentSystem security categorization support
- System Security risk assessment support and documentation
- Contingency plan and disaster recovery plan, support, and documentation
- Configuration management development and support
- Incident response plan development, support, and documentation
- Security monitoring development and support
- Performance of Security Officer roles and responsibilities as dictated per policy
- Privacy impact assessment and Personally Identifiable Information (PII) support
- Memorandum of Understanding or Agreement (MOU/MOA) per security agreements support
- Network security support to include scanning with related tools
- Application level scanning (e.g. software code, scripts, websites)
- Security Engineering (e.g. intrusion detection analysis, configuration of devices, and website scanning)
- Technical writing (e.g. develop, edit, manage, and maintain documentation)

Performance of these services and/or any other related security service(s), will be done through existing processes, procedures, and tools (e.g. SourceFire, Tenable Security Center – Nessus, Cyber Security Management (CSAM), Splunk, BigFix, and Trustwave App Scanner). The Contractor shall follow directives and guidance provided by the Diversion Control Division's, Technology Security (DCTS) management, and its governing bodies as listed above.

1.7.9 Lifecycle Management

The Contractor shall provide support for all DC IT systems. The support shall include, but is not limited to:

- Providing lifecycle management and maintenance for all systems within the scope of this contract
- Providing technical maintenance and support necessary to maintain operational systems in an effective and efficient status
- Correcting anomalies found in the application(s) and incorporate new functionality as directed and approved by the GPM(s), and/or a DC representative
- Updating documentation to include but not limited to (1) Requirements Specification, (2) Systems Design Document, (3) Requirements Tractability Matrix and, (4) Acceptance Test Plan and Report. All updated documents will be reviewed and approved by the GPM(s) and/or a DC representative prior to publication
- Developing for the DEA's Office of Security Program's approval, an Acceptance Test Plan containing only objective and measurable standards
- Submitting those applications that will operate on the DEA enterprise-wide network to the GPM(s), and/or a DC representative for DEA SI for Integration Testing, along with Independent Verification and Validation Testing
- Providing lifecycle management and maintenance progress with appropriate Quarterly Executive Status Reports per task

1.7.10 New Technical Requirements Caused by Regulatory or Policy Changes

The DEA, in order to perform its mission, must react quickly to changes in drug abuse and diversion. Some of these changes are legislative and require rapid development and deployment of new IT applications or modifications to existing applications. The Contractor must be prepared to provide innovative methodologies to make efficiencies for iterative development of business needs as a result of legislative, regulatory, policy changes or public safety initiatives. If a new or unforeseen IT requirement emerges during the life of this contract, the Contractor shall coordinate with the COR and GPM for a change in priorities, or, if necessary, the addition of a new task order to the contract.

1.7.11 Technology Refresh and Physical Relocation of System Components

The Contractor shall participate in technology refresh efforts and provide innovative ideas to meet the future needs of DC. The Contractor shall conduct Research & Development (R&D) and work with vendors on proof of concepts that will demonstrate a needs assessment with the key benefits of the refresh. Once a solution has been determined the contractor shall provide an implementation/migration plan to the government. New products shall be tested and evaluated before being placed into the production environment. Once operational the contractor shall monitor production system performance statistics and report to the GPM when upgrades or system enhancements are necessary.

1.7.12 Inventory Management

TGD maintains over 1000 pieces of IT equipment for which an accurate accounting must be maintained. Inventory records are maintained in the DEA's United Financial Management System (UFMS). There are specific guidelines for tracking inventory in UFMS, such as cost, type, and end-of-life cycle. Loss or theft of accountable property is a serious infraction, thus, each employee, whether contractor or government, must maintain accurate records for each piece of accountable property. DEA property is inventoried each year and the Contractor will be required to assist the government in the inventory process. As part of the inventory process, the Contractor shall maintain inventory

to ensure current versions of all approved software are in use and shall: advise government of new versions of software and maintenance coverage; provide the COR, the GPM(s), and a TGD representative with a Quarterly Executive Status; and report on the progress of the current application/system under development or in standard production mode. Additional guidance on inventory requirements will be provided upon contract award.

1.7.13 Testing and Evaluation

Testing and Evaluation are required to ensure systems' full functionality in accordance with DC and DEA requirements and standards. Software testing and evaluation reduces the cost of system, network, and operational maintenance. It also ensures that application software meets requirements, identifies and prevents inefficient design, identifies actual and potential errors, and prevents those errors from reaching production software.

The contractor will migrate current DC quality assurance methodologies to continuous integration and continuous deployment/delivery (CI/CD). The contractor will actively pursue and communicate with the Government best practices for CI/CD and provide the government with reports on migration status as required.

Once migrated, the contractor will follow Agile practices for documenting test plans and reports in consultation with the GPM and COR.

While migrating, the contractor will continue to maintain current quality assurance processes/practices. Copies of test reports, test plans, software problem reports, system evaluation reports, scalability and stress test reports, software technical reviews, and system testing and evaluation reports shall be provided for review on a quarterly basis to the GPM. The Contractor shall:

Provide structured technical reviews, testing, and evaluation of all software applications developed by the Contractor in support of DEA. The details in support of this effort include but are not limited to:

- Development of test plans and test cases compatible with system requirements
- Functional testing
- System testing based on requirements
- Acceptance testing
- Regression testing
- Confidence testing
- System testing to include load and timing tests
- Detailed documentation, prioritization, and tracking of test results and deviation
- Generation of software problem reports and suggested corrections
- Resolution of software test issues and production of test report results
- Assistance to the programming development team with discrepancy analysis
- Reviewing proposed changes and conducting impact analysis
- Assisting developers for the generation of unit test cases, test procedures, and test results documentation
- Evaluation and documentation of system performance
- Evaluation and documentation of user manuals
- Documentation of test results
- Maintenance of policies, processes, and procedures for software technical reviews, testing, and evaluations including walkthroughs and inspections
- Providing results of systems testing and evaluation to the GPM and/or a DC representative.
- Making all required changes based upon Certification and Accreditation process review and execute

additional testing and evaluation

- Making all required changes necessary for compliance with DEA enterprise-wide network. All systems that will operate on the DEA enterprise-wide network will undergo the DEA's SI Integration Testing, Independent Verification, and Validation Testing prior to implementation

1.7.14 Training and Cross-Training

When needed, the Contractor shall develop and provide the necessary training to government employees, for new or significantly modified DC IT systems. The Contractor may be required to travel to DEA CONUS field offices to provide training when significant improvements to new or existing systems are deployed. If requested by the government, the Contractor shall conduct feasibility studies of new systems for use in embedded training modules and present its recommendations to the government for incorporation of embedded training in the SDLC.

The Contractor shall:

- Maintain training programs (end-user and administrative) for individual systems developed under this SOW
- Submit training plans to the COR, the GPM, and/or an DC representative for approval
- Develop and submit training material (e.g., visual aids, handouts, video presentations) to acclimate users to new or enhanced systems
- Execute approved training plan

The contractor shall cross-train government IT Specialists in the various DC applications and systems. This training will be scheduled by the GPM.

1.7.15 Documentation

All documents developed by the Contractor on the government's behalf as it relates to this contract, are the intellectual property of the government. As such, the government reserves the right to request any documentation developed by the Contractor in support of this contract at any time in addition to that listed within specific tasks. The Contractor shall provide that information within five working days of the request. Copies of the User Manuals and Guides and Specification Documentation shall be provided for review during the transition phase.

The Contractor shall:

- Develop, produce, and maintain user manuals and guides on all systems under this Contract
- Develop, provide, and maintain interface specifications and system engineering documentation for all systems under this Contract
- Develop, provide, and maintain all other documentation identified under the individual tasking or requested by the GPM or COR

1.7.16 Data Call Requests

TGD is often directed to provide data for a myriad of subjects or systems for which it is responsible. These directives are often voluminous and require a short turn-around. The Contractor will be required to assist with any data call request by providing the information required to the TGD government employee responsible for gathering such information within the timeframe determined by the data call originator.

1.8 Project Requirements - Unique DC Applications

The contractor shall provide 24/7 support for all applications developed, maintained, or implemented within the scope of TGD's work with the DEA Diversion Control Division.

This section provides requirements for contractor support and an overview of DC applications.

1.8.1 Application and IT Support

The contractor shall provide the following services for all DC applications and systems:

- Continuous system security monitoring in conjunction with daily and weekly health checks
- System/Operational Deliverables to include, a Weekly Operations Brief consisting of operational and systems status, a Monthly Builds Report consisting of monthly and cumulative system updates, and Monthly Program Progress Review Reports
- Ensure compliance with the federal bridge where applicable
- Notify Tier II support of any/all system/application issues
- Perform software upgrades, virus file updates, and patch assessment
- Perform assessment/maintenance of all hardware upgrades and devices
- Manage firewall and router monitoring/maintenance, to include upgrades and assessments
- Maintaining an active inventory of all software and hardware utilized within the system
- Develop, test, stage, and deploy all applications and systems
- Manage the operation of DC IT systems, including receiving, analyzing, and recommending changes through the DC configuration control board.
- Manage, maintain, and monitor all servers (physical/virtual); operating systems and their networks and connectivity; databases, enterprise applications to include production, staging, development and disaster recovery (DR) systems
- Support and enhance infrastructures for current and next generation technologies and adhere to security directives to ensure compliance on all components
- Provide day-to-day administration, maintenance, and performance reporting of all network infrastructures
- Provide technical support and assistance in administering connectivity and interaction
- Develop/maintain capacity and failure/recovery plans including notification of system anomalies
- Keep applications and systems technologically advanced with industry standards and emerging technologies
- Submit and track requests for additional equipment and software. These requests will be approved by the GPM(s), and a TGD representative
- Provide operational development, support, and maintenance for printing required forms
- Maintain and monitor security to ensure that systems are compliant with DOJ security requirements

1.8.2 Development Environment

The current environment implements waterfall methodologies for developing, testing, and deploying systems and applications. The contractor will migrate current development practices to Agile and to the CI/CD pipeline.

1.8.3 Registration Support Network (RSN)

The RSN platform houses applications in the Registrant Information Consolidated System (RICS) and in the Automated Reports Consolidated Ordering System (ARCOS). It provides an environment for additional applications and systems to support DC activities and requirements, such as printing physical forms and correspondence, and providing a VOIP infrastructure for the Diversion Control Division Support Center.

1.8.3.1 RICS

The Registrant Information Consolidated System is a suite of applications and databases that permit the public to submit requests to DEA for evaluation and approval. Anyone intending to handle controlled substances or list 1 chemicals must register with DEA for approval, and must thereafter adhere to laws, regulations and policies restricting the handling, distribution, and use of those substances, and to reporting requirements. RICS applications facilitate communications between public registrants and DEA's investigators, managers, analysts, enforcement teams, and customer service representatives.

Because RICS applications receive data from the public, most applications have both an external-to-DEA and an internal component.

Some of the functions provided by RICS applications are listed below:

- Register to handle controlled substances or listed chemicals
- Maintain a current DEA registration (make changes, renew, request proof-of-registration such as receipts and certificates)
- Validate the standing of other registrants
- Report thefts and losses of controlled substances and chemicals
- Report the import/export of controlled substances, chemicals, regulated machines, and the domestic sale of regulated machines.
- Apply for an annual manufacturing quota for controlled substances
- Report controlled substance inventory to DEA
- Report suspicious orders to DEA
- Submit a tip to DEA
- Register for DEA conferences, workshops, etc.
- Allow DEA to analyze, manipulate, and otherwise manage the requests, reports, data, and intelligence collected from the public and from registrants
- Allow DEA to manage DC personnel and assets

RICS has over 2 million unique external user accounts, each associated with a registrant. Additional user accounts are available in applications that permit validated and authorized registrant associates to report registrant information, which grows exponentially by the thousands each year. In addition to registration, around 22,000 other records are generated by registrants to RICS applications (such theft and loss reports, import and export declarations, etc.).

Registrations and reports all generate various workflows in the applications to which they are entered; RICS applications manage these workflows, facilitating collaboration between DEA personnel, registrants, associates, and the public.

General communication with the registrant population and the public are maintained through the Diversion websites. The websites consist of both static pages relating policy, procedures, guidance, and contact information, as well as web-facing applications that facilitate information gathering and reporting.

The contractor must support the ingestion of new data by maintaining the applications already deployed and by developing new applications, functions, and processes, as required, to improve DC's fulfillment of its regulatory and operational missions.

The contractor must support communication with the registrant population and public by maintaining current DC websites and developing new functionalities, pages, sites, applications, and data gathering apparatuses as required by DEA.

The contractor must support processes for extracting, transforming, and loading RICS data into the Data Warehouse and other data collection and analysis systems as required by DEA.

1.8.3.2 ARCOS

ARCOS is a collection of applications that receive transaction reports from registrants and facilitate DEA's analysis of those transactions. ARCOS consists of a web-facing reporting tool, a web-facing bulk transaction reporting tool, and the internal-to-DEA application facilitating analysis of reported transactions. Additionally, ARCOS houses the primary National Drug Code (NDC) dictionary for the Diversion Control division. Data in the NDC dictionary is provided through interconnections to First Databank, and by reports received from the Food and Drug Administration and from

The internal ARCOS system is responsible for providing both raw data to DEA personnel and business intelligence. Transactions reported to ARCOS are subject to automated evaluations.

ARCOS users are a subset of registrants, registrant associates, and DEA personnel (see section 1.8.2.1). ARCOS contains billions of transaction records dating as far back as 2002, and receives about a 40 million additional transaction reports yearly. The ARCOS data set is easily the largest data collection undertaken by the Diversion Control Division, and has the most data requirements attached to it.

The contractor must support the ingestion of new data by maintaining the applications already deployed and by developing new applications, functions, and processes, as required, to improve DC's fulfillment of its regulatory and operational missions.

The contractor must support processes for extracting, transforming, and loading ARCOS data into the Data Warehouse and other data collection and analysis systems as required by DEA.

1.8.3.3 Data Warehouse

The Diversion Control Division has an IBM Pure Data System for Analytics System, which has a Massive Parallel Processor as the main component of the data warehouse. The Contractor shall enhance and maintain the data warehouse appliance, which contains data from DCP applications. Annually, DC maintains around 2 million registrant records and collects approximately 40 million purchase/sale transactions, 10 thousand theft and/or loss transactions, and 12 thousand import/export transactions. A properly designed data warehouse may show that a controlled substance was imported as raw material by registrant "A," converted to a drug product by registrant "B," distributed by registrant "C," and sold to retail vendor registrant "D." This information would be useful to DEA investigators that want to trace diverted controlled substances back through the chain of distribution.

The Contractor shall continue to:

- Enhance the efficiency of the Data Warehouse
- Review data architecture and provide methods to maximize effectiveness of the data analytics
- Provide innovative ideas for future data storage or virtualization to provide faster data access

1.8.3.4 Geo-analytics System

DCP has implemented an ESRI geographic information system to assist with targeting and analysis of geospatial data. The Contractor shall maintain current services and develop new functionalities at both enterprise and desktop levels. The contractor shall work in concert with other DEA GIS teams to integrate GIS components or spatial analysis through the DEA-entire geospatial environment. The contractor shall provide nightly backups of the system, OS upgrades, and other typical IT administrative tasks as defined by the Government. The contractor shall provide geodatabase management, connectivity, and troubleshooting

services to any and all datasets to be used by the DC GIS. The contractor shall provide connectivity between the mapping interface component and data warehouse utilizing existing software and shall continue to manage geo-coding practices of addresses to selected databases. The contractor shall work with a 3rd party vendor to maintain the current 3-pronged address validation, geocoding, and designation service currently in place until the current contract expires. The geo-coded databases will be used in conjunction to provide a spatial locater with the mapping software. The contractor may be required to provide GIS staff member(s) to support the DCGIS implementation and maintenance efforts. The following items are capabilities required to provide the support needed for this effort at a minimum:

- An advanced knowledge of ESRI's Geographic Information Systems (GIS) system integration, GIS Integration Planning Managers as well as Enterprise GIS implementation practices
- Ability to meet with users to define data needs, project requirements, required outputs, or to develop custom tools
- Ability to compile geographic data from a variety of sources including censuses, field observation, satellite imagery, aerial photographs, and existing maps
- Ability to analyze spatial data for geographic statistics to incorporate into documents and reports
- Ability to prepare metadata and other documentation
- An advanced knowledge and capability to operate and maintain GIS system hardware and software in a Linux based environment using Oracle and VMWare
- An advanced working knowledge of Oracle Spatial, ArcSDE, ArcGIS Server and ArcGIS desktop
- Ability to provide cartographic design, image processing, graphic editing, database management services, and map production services as needed
- A working knowledge of geospatial web APIs to include the creation of mobile applications and web mapping mashups
- Experience with Flex/Flash, Python scripts and Model builder
- A working knowledge of Business Intelligence software and how it integrates with Enterprise GIS software

1.8.3.5 Mobile Applications

The contractor shall provide support for agile development methodologies, operations and maintenance, change management, quality assurance, and training necessary to support mobility environments. The Contractor shall design, develop, and test mobile based applications on Android and/or Apple iOS platform and assist in bringing mobile applications to the App Catalog. In addition to designing and developing, the contractor shall test and debug mobile applications, and create development, testing, and deployment documentation as required, and work with users to define existing or new requirements and objectives. The contractor shall provide analytical support and technical advice during the conceptualization, development, and implementation phases and maintain applications, including bug fixes, performance enhancements, and runtime production support.

The contractor shall generate technical documentation for various aspects of the applications developed and review and evaluate systems and software for adherence to government or commercial directives, standards, guidelines, and criteria concerning software and systems security. Upon completion of the mobile application's development, the contractor shall assist with installation as well as assist in submitting the application to any app stores or repositories. Upon completion of all services, the contractor shall provide to the government without delay, any and all code and databases related to the mobile application development agreement.

1.8.3.6 National Forensic Laboratory Information System (NFLIS)

The Drug and Chemical Evaluation Section (DOE) is responsible for evaluating drugs and chemicals to determine whether these substances are being abused or potentially involved in illicit traffic. These evaluations are used by DEA as a basis for developing appropriate drug control policies, determining the status of controlled, excluded, or exempted drugs and drug products; and supporting U.S. initiatives in international forums. In addition, the DOE-Section provides information to support international control of essential and precursor chemicals and abusive drugs under the treaty provisions of the United Nations.

In support of DOE's endeavors, the National Forensic Laboratory Information System (NFLIS) is a forensic data collection and management system that stores scientific analysis results and other associated information from volunteer participants. These volunteers allow NFLIS to flourish and grow while making it unique among other systems in the Government. Without volunteer entities contributing data, NFLIS would fail. The NFLIS program is composed of three components:

- **NFLIS-Drug** collects drug analysis results from Federal, State, and local crime laboratories. It contains information on controlled substances, non-controlled substances, and listed chemicals, and reports of miscellaneous substances such as baking soda or ibuprofen that cannot be identified by law enforcement until it is analyzed by the laboratory. Launched in 1997, it was the sole collection effort for 20 years. Thus, many people referencing "NFLIS" data are referencing NFLIS-Drug data.

- **NFLIS-Tox** collects toxicological findings from ante- and post-mortem samples analyzed by public and private toxicology laboratories.

- **NFLIS-MEC**: collects data from medical examiner and coroner offices on deaths in which drugs were identified.

NFLIS also partnered with the DEA Real-Time Communication Network on Synthetic Opioids to form the **NFLIS Synth-Opioids website**, an Amazon Web Services (AWS) Government Cloud based forum for sharing and searching information on new and emerging drugs, analytical techniques, drug control, and other drug-related information. It provides critical information on drug trends which enable DOE to make informed decisions on drug policy. NFLIS collects analysis results for materials that are seized by local, state, and Federal law enforcement entities, which is analyzed by reporting laboratories.

In addition, the Data Query System (DQS), a component of the secured portion of the NFLIS website, offers a series of standardized queries, by submission date to the laboratory or by the completion date of analysis, which can be used to extract information from the NFLIS-Drug and NFLIS-Tox databases and generate reports. These reports can be grouped by the type of laboratory (Federal, state, or local), geographic location (national, regional, state, metropolitan statistical area, county), and date (annual, semi-annual, quarter, or month). The following are the current available queries:

- All Reported Drugs
- Base Drug List
- Top 50 Drug Lis
- Item Detail

All of the NFLIS IT systems reside within the Registrant Support Network (RSN), and thus, are a critical area of responsibility under the contract. The government utilizes the NFLIS system daily and depends on the data to establish and prioritize drug enforcement objectives. Therefore, the IT Contractor shall maintain daily communication with NFLIS government and contractor staff to coordinate and collaborate on the technical needs for the NFLIS scientific and analytical IT infrastructure needs. This collaboration shall include the management, maintenance, and modernization of the systems. It shall also include ensuring that there is system availability at all times for the three specific NFLIS IT applications - NFLIS Website, Data Query System, and SynthOpioids Website – including support of all databases, tables, and entries.

In addition, the Contractor shall support the NFLIS government and contractor staff by providing any and all IT infrastructure software development required for the NFLIS program, reporting information, and assisting with data management as needed.

All access to NFLIS data by other entities must be submitted to the Government for approval. Sensitive case information or names will not be collected in the NFLIS database. NFLIS system security requirements will be dictated by the DEA Office of Security Programs.

1.8.3.7 Interactive Voice Response (IVR)

The IVR system is a computerized telephony system that acts as the first point-of-contact to callers to the DC Call Center. It is intended to provide twenty-four hour-a-day basic information on the registration process and user specific information on the registrant's account. Registrants also are provided with a means to request information and documents from DC. DEA requires the use of the IVR system to provide after-hours customer support and to reduce the workload of the Call Center staff for customer support issues. The existing IVR is fully deployed and will require maintenance, enhancements, and script changes. New IVR systems may be required at DEA Headquarters or in several DEA field offices. The Contractor shall:

- Design, develop, test and evaluate, implement, manage, and administer the IVR System to include speech recognition for new systems requested in DEA field offices
- Design, develop, test and evaluate, implement, manage, and administer the existing IVR Systems
- Perform all system administrative functions to ensure a fully operational IVR system
- Continuously evaluate the IVR options menu for relevancy, efficiency, and accuracy
- Maintain an IVR report system usage statistics, problems, and corrective actions implemented to resolve the problems
- Develop customized reports
- Submit system change recommendations as needed for evaluation and approval of the Government
- Incorporate all approved enhancements and revisions into the IVR system, test and evaluate, and report completion of changes
- Ensure current versions of DEA approved IVR software are in use and advise the government of new versions of software and maintenance coverage
- Participate as needed during certification and accreditation of the IVR
- Develop and test contingency operations in support of the IVR Continuity of Operations Plan (COOP)
- Maintain IVR's integration with RICS data
- Develop and/or implement a system that will fully back-up the IVR data

1.8.3.8 Print On Demand (POD)

The Contractor shall provide IT support for the POD system. This support includes system administration, maintaining the print server, patching printing software, and conducting any other IT operation to ensure successful functioning of the Printing Operation Center.

1.8.4 Controlled Substance Ordering System (CSOS)

TGD has developed a new CSOS-II system, which is ready to launch once regulatory requirements have been completed in DC. Until the system is launched, the Contractor shall maintain the current CSOS and ensure that it remains operational. The Contractor shall coordinate with the COR, the GPM, and a DC representative to establish priorities and tasks related to the support required for the current CSOS and the future CSOS-II system.

Currently, DEA's Controlled Substance Ordering System (CSOS) program allows for secure electronic controlled substance transactions between controlled substance manufactures, distributors, pharmacies, and other DEA authorized ordering entities, without the supporting paper DEA Form 222. Using Public Key Infrastructure (PKI) technology, CSOS requires that each individual purchaser enroll with DEA to acquire a DEA digital certificate. The framework for the CSOS program includes the following elements: PKI electronic ordering system, Certification Authority, Registration Authority, and CSOS subscribers. Under this contract, in addition to IT Support (see section 1.8.1) there are two major areas of support for the CSOS Program, which the Contractor shall provide:

1.8.4.1 Certificate Authority Support

The CSOS Certification Authority (CA) is the entity which creates, signs, and issues the PKI certificates to authorized CSOS subscribers. The CSOS CA is responsible for all aspects of the issuance and management of a certificate, including: the registration, identification and authentication processes; the certificate manufacturing process; the revocation of certificates; and for ensuring that all aspects of the CA services, operations, and infrastructure related to the certificates issued under CSOS are performed in accordance with the requirements, representations, and warranties of the Certificate Policy (CP). The Contractor shall provide support that shall conform to the stipulations of the CP and will prepare a Certification Practices Statement for review and approval by the COR and DEA Program Manager, that supports and includes references to the CP.

1.8.4.2 Registrant Authority Support

The CSOS Registration Authority (RA) collects and verifies each subscriber's identity and information that will be entered into his/her PKI. The CSOS RA shall process applications of CSOS subscribers and coordinators, verifying the information that is to be entered into the subscriber's public certificate. The contractor shall provide support that will conform to the CP and which will provide complete SDLC support.

SECTION II – MANAGEMENT AND PERFORMANCE CRITERIA

2.1 Transition Plan

The Contractor shall address transition of all services defined in this contract to ensure no impact to operational availability. The Contractor shall include the specific requirements of this contract section with their proposal. An updated Plan, if required/requested, is due 10 days after contract award. The transition plan of the successful Contractor will be incorporated into the contract.

A. ***Transition Phase-In***

Transition is an integral part of a contract's start-up. The Contractor's proposal shall include a plan for assuming 100 percent responsibility for services required in performance of this contract. The plan shall include a timeline for completion of all phase-in activities within 60 days, the intent of which is to provide additional time for in-depth analysis of the program. Transitioning of employees to the new contract should also be completed within 60 days. The plan for transition-in shall include, but is not limited to:

- Management of phase-in activities
- Initial manning levels and timeline to achieve full manning level
- Development and dissemination of operational instructions, procedures, and control directives
- Ensuring no disruption of work and maintaining continuity of operations.
- Transfer of government furnished property, material, equipment and data, if applicable

B. Transition Phase-Out

The Contractor's proposal shall develop a plan for a transition-out period, in the event that the Contractor is not selected for a follow-on contract or the government elects not to exercise any options to extend the performance period. The Transition Phase-Out plan is due to the COR 180 days after contract award. The plan for transition-out shall include, but is not limited to:

- An Executive Summary that documents at a high level, how the Contractor will transition the projects, duties, activities, functions, tasks, and tools from the Contractor to the incumbent contractor
- Transition Approach methodology that outlines how the Contractor will maintain existing staff, if all staff will be on-site throughout the transition period, and the approximate amount of time the Contractor anticipates it will take to transition to the incumbent contractor
- A detailed Transition Team Organization Plan, that is, an organizational chart that shows all transition plan players and their roles/responsibilities
- A Transition Tracking System, that will list every project and which will track the progress of all projects during the transition
- A Personnel, Security Clearances, and Badging Phase-out Plan, that is, a plan that will identify all positions/employees to the COR, with specific requirements stated for those employees who will leave DEA (those who will not transfer to the incumbent contractor), including security termination statements, collection of all badges on the last day of employment, and revision of the JPAS to remove each employee clearance from the Contractor's CAGE code; and for those employees staying with DEA as employees of the new contractor, a plan that will list the employee's name and transfer date to the incumbent contractor so that the security clearance and badge can be transferred

- A plan for Work Execution During Transition that will describe in detail the work that will continue by the Contractor during the transition period to ensure no disruption in service, that is, a comprehensive list of all activities/projects to be transferred to the incoming contractor and a transition schedule for all ongoing activities

- A Property Transition Plan that outlines in detail how the following property will be transitioned:

    1. *Government Furnished Equipment* – what/how/when all property will be returned to DEA, to include any identification numbers associated with the equipment (i.e., DEA number and serial number)
    2. *Incumbent Owned Equipment* – a list of any equipment owned by the Contractor that supports DEA applications and services with a plan to identify such equipment and details as to how all information contained on that equipment will be transitioned to DEA
    3. *Intellectual Property* – discuss how all intellectual property that is a direct result of the work on the contract deliverables will be transitioned to the new contractor with a statement that all outgoing employees will sign a non-disclosure agreement
    4. *User Accounts and Passwords* – provision of a comprehensive list of all employees and those accounts for which they have access and how access will be transferred to the new contractor, to include the current user(s), manager of the system, and employee with incumbent contractor to whom the account will be transferred

- A Knowledge Transfer Plan that provides specific details on how the knowledge of the current activities and processes of the staff will be transitioned to the new contractor – e.g., instructional manuals, formal training classes, one-on-one training, etc., and the timing of each phase of the knowledge transfer
- A Handover and Acceptance Plan that provides details as to how all activities will be handed over to the new contractor, including whether or not a formal checklist will be required that documents the acceptance and sign-off of equipment/systems from the Contractor to the incumbent contractor.

2.2 Contractor Program Management Plan

2.2.1 Service Level Management Agreement Plan

A Service Level Management Agreement Plan (SLMAP) is essential in any organization so that the level of IT Service needed to support the business can be determined, and monitoring can be initiated to identify whether the required service levels are being achieved, and if not, why. Service Level Management Agreements (SLMA) and Initial Service Agreements (ISAs), which are managed through the SLM Process, provide specific targets against which the performance of the IT organization or support services vendor can be judged.

After contract award, the contract awardee, in coordination with DC/TC as its customer, shall develop and mutually agree on a Service Level Management Agreement Plan (SLMAP) for all services to be provided under the contract. All parties will phase in the implementation of the SLMAP over the contract's base period in accordance with the agreed schedule.

The Contractor shall review all Underpinning Contracts (UC's) and Operational Level Agreements (OLAs) in place with those suppliers (external and internal) upon whom the delivery of service is dependent. In the event the UC's or OLA does not support the SLAs they will notify the COR.

The Contractor shall develop, and incorporate into DC/TC an SLMA process as outlined in their proposal. The Contractor shall plan, provision, perform, improve, and assign key elements of each phase into a management life cycle. The Contractor awardee shall provide a comprehensive, consistent, and coherent set of Best Practices and

Standard Operating Procedures for IT service management within 45 days of contract award. The Contractor shall identify any SLM tools or software they require to implement the SLM program.

The contractor awardee is expected to produce the SLMAP within 90 days of contract award and the SLM Best Practices document within 45 days of contract award, in accordance with the Deliverables Schedule (Exhibit 3) and to provide a Compliance Report monthly.

2.2.2 Work Breakdown Structure and Schedule

A. Initial Project Management Plan and Work Breakdown Structure and Schedules

The contractor shall be solely responsible for developing an initial Program Management Plan (PMP) and Work Breakdown Structure and Schedules (WBS&S) that will be included as part of the draft Quality Control Plan which shall be submitted to DEA as part of the Technical Proposal response.

B. Updated PMP and WBS&S

Following the contract award, the updated PMP and WBS&S shall be submitted to DEA every six months as defined in the Articles of Delivery of this SOW (Exhibit 3).

2.2.3 Configuration Management Plan - Conforming to an Industry Standard

The Contractor must conform to an industry standard Configuration Management Plan (CMP) to carry out the development, maintenance, and enhancements outlined in this SOW. The Contractor must establish configuration management controls in accordance with DEA's SDLC, which will be provided to the Contractor upon contract award. Two configuration control boards currently exist in DEA which include the DC/TC Configuration Control Board (CCB) and the Office of Information Systems' Infrastructure Configuration Control Board (ICCB). DC and TC technical staff and technical personnel assigned under this contract comprise the CCB and changes that do not affect DEA's internal enterprise-wide network are approved by the CCB. Changes that affect DEA's Firebird network are forwarded to the ICCB for review and approval. Regulatory changes that affect the modernization effort must be captured and approved through the CCB. A CMP currently exists and will be provided for review.

2.2.4 Government Quality Management Requirements

TGD has a Quality Management (QM) process that is in alignment with the Level 3, Software Quality Management Key Process Area requirements of the Software Engineering Institute (SEI). The DEA QM program applies to all DEA information technology activities related to the development of internal or external work products, the execution of DEA defined processes and procedures, and the delivery of services to external or internal customers. The QM also applies to all software development activities. DEA is routinely audited to determine its compliance and adherence to the defined processes and procedures. Thus, the Contractor will be responsible for compliance with the mandates.

2.2.5 Quality Control Plan

2.2.5.1 Quality Control Plan Requirements

The Contractor shall provide a comprehensive, detailed Quality Control Plan (QCP) to ensure services are performed in accordance with this contract as part of their Technical Proposal. The QCP shall also include the Contractor's Initial Project Management Plan and Work Breakdown Structure and Schedules and its draft Service Level Management Plan. The contractor shall clearly and concisely depict how the QCP will be

implemented and monitored for any and all contractor/subcontractor employees' work products, including the quantitative standards and measures utilized in determining successful/unsuccessful performance.

The contractor shall include the proposed quality management system including the quality control approach/processes to be applied to the performance of the requirements listed in the Statement of Work. The contractor shall define the roles and responsibilities for assuring quality performance. The contractor shall address the required level of experience and/or qualifications required by those identified to perform quality control functions. The contractor shall identify the staff (by labor category) dedicated to perform quality control. The contractor shall provide the planned approach to maintaining continuity of its support to the mission of the Diversion Control Division and the Diversion Control Program.

The contractor shall describe its preventative action for eliminating errors. The contractor shall provide its communication plan for preparing and distributing quality control reports and other information. The contractor shall describe its record-keeping system for maintaining a repository for quality control records. The contractor shall describe how work output levels will be measured and how day-to-day operational and contractual issues will be handled. The contractor shall demonstrate the ability to anticipate risk and opportunities that may be encountered in the performance of the work and the measures to be taken in response. The contractor shall define a process that supports the execution of the tasks delineated in this contract and a plan that will develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The QCP shall include a method of surveillance, inspection, validation, evaluation, corrective action, and procedures necessary to affect quality control of all performance and products including those of sub-contractors and members of the Contractor's team.

2.2.5.2 *Contract Inclusions*:

The QCP shall be part of the contractor's technical proposal. After contract award, the contract awardee's final QCP will be accepted by the Government and shall be incorporated into this contract.

2.2.5.3 Quality Control Plan Revisions

After contract award, the operation of the QCP shall be maintained current and made available to the COR. Any revisions to the QCP shall be approved in writing by the Contracting Officer (CO) prior to implementation. DC/TC will perform Independent Verification and Validation of vendor performance metrics.

2.2.6 Customer Service Strategy

The Contractor shall implement innovative approaches for a strong customer-focused culture. The Contractor shall be required to maintain a high-level of customer service focus for the life of this contract. As part of sustaining customer focus, the Contractor shall execute surveys to measure and manage customer satisfaction with respect to the performance of the services provided. The Contactor shall report on customer satisfaction as it pertains to Contractor expertise, courtesy, timeliness, and professionalism when requested and all data collected from DEA and Registrant customers shall be provided to DC management unedited.

2.3 Communication and Reporting Requirements

2.3.1 Program Management

Key Personnel must be assigned for the duration of the contract and may be replaced or removed by the government due to standards of conduct violations or unsatisfactory performance which does not improve. The Contractor shall provide the identification of the Program Director (PD) in its contract proposal submission, and must substantially meet the requirements identified in the contract. The PD is expected to start on the first day of the contract and provide the contractor management with tasks on a day-to-day basis. In the event the proposed PD is not available at contract award, a candidate with equal qualifications must be provided. The PD shall be responsible for all aspects of the contract and shall serve as the Service Level Manager for the duration of the contract

The PD is responsible for the day-to-day coordination of project activities and client contact. The PD is responsible for the Service Level Management (SLM) process that addresses the entire life cycle of a service, from the implementation of the service to the retirement of the service. The PD shall manage projects in compliance with plans and strategy briefs in relation to one or multiple, small or highly complex projects. The PD shall be directly responsible for scheduling, tracking, risk analysis, cost management, variances, change management, evaluating, and controlling projects. The PD shall be responsible for ensuring that personnel resources are provided that are capable of performing administrative support functions commensurate with the contracts personnel staffing levels. Examples of administrative support functions include, but are not limited to, information dissemination to staff members, preparation of monthly progress reports, data entry, assisting with property accountability, monitoring employee work schedules, providing phone rosters, preparing briefing materials, providing meeting minutes, meeting agendas, and responses to data calls.

In addition, the PD shall provide monthly personnel activity reports to accurately account for all levels of effort in key personnel areas and on data calls. Monthly personnel activity reports will include all information that is required to complete Exhibit 53's, Investment IT Summaries, Portfolio Statistical Reports, and other data calls when required. A sample format of the specific information required for this reports will be provided at contract award.

The PM is responsible for the completion of a Transition Plan, which recommends the steps necessary to migrate from existing Government and Contractor operations to the newly awarded contract, inclusive of all hardware/software contracts and maintenance agreements. The plan shall be defined in detail by specific task, deliverable, and milestone to ensure an orderly and complete transition. The transition shall be executed as quickly as possible with minimum disruption to business application operations and customer service.

The PD is responsible for the completion of an Exit Transition plan, which recommends the steps required to transition business application operations from the current Contractor service provider back to DC/TC and/or the follow-on service provider at the conclusion of the contract. This plan shall include provisions for the return of all government furnished property and the disposition of any Contractor proprietary tools that may have been installed to support business application operations such that DC/TC and/or the follow-on service provider may remain fully operational up to the standards established before exit.

2.3.2 Program Management Review (PMR)

The Contractor shall meet with the COR and the Government Program Manager (GPM) weekly or each month (as determined upon contract award) to conduct a PMR. The Contractor may also be requested to meet with DC managers responsible for a particular portion of the Contract to provide project status reports. The PMR must have a summary of all projects underway, with details for each specific project. The Contractor shall also provide the COR, the GPM, and DC managers (when requested) with detailed monthly progress status reports for specific projects. These reports must be technically and grammatically correct. Progress reports must reflect work performed in the reporting period, problems encountered, milestones achieved, deliverables submitted, and work scheduled for the next reporting period, test results, comments, and funding status. Barriers to successful completion of tasks should be identified and proposed solutions outlined.

2.3.3 Capital Asset Plan and Business Case for Modernization

The Department of Justice (DOJ) may require the submission of a Capital Asset Plan (CAP) (OMB-300), and/or, submission of the OMB Exhibit 53 IT Investment reporting requirement. The contractor shall be provided with copies of the last OMB-300 or OMB-53 submitted by DEA after contract award, and must maintain those documents should the requirement to submit an updated OMB-300 or OMB-53 be requested. Should these requirements arise, the Contractor must review the existing OMB-300 and/or OMB-53 and shall perform the following:

- Gather information and documentation and establish a base line
- Review existing documents – sample documents, document writing guidelines, previous versions of submitted CAPs, Business Case (BC), IT Investment reports, and comments from reviewers
- Meet with COR, GPM and identified government management officials to examine all existing information and analyses that can be used/re-used for the submission
- Divide and organize work such that approximately one (1) work day is dedicated to each major section required, e.g., project description, justification, performance goals, and measures
- Interview targeted DEA employees (not to exceed 45 minutes each) for each report section or research provided documents
- Prepare each section and provide to DC/TC for agreement
- Develop documentation in response to inquiries (as needed)
- Prepare final documents
- Compile all sections into a cohesive presentation in accordance with documented guidelines
- Write, review, and edit as required
- Provide final CAP and BC document
- Provide final OMB Exhibit 53

2.3.4 Project Performance Dashboard Updates

The Contractor may be required to provide monthly project status reports to the Department of Justice using the Office of the Chief Information Officer, Project Dashboard, and Project Manager's Worksheet, to track project milestones, risks, and costs. The Contractor shall coordinate this report with the COR, the GPM, and a DC/TC representative (as appropriate).

2.3.5 Internal Use Software Capitalization Report

The Contractor shall report monthly, software development costs to the Office of Finance (FN) using the spreadsheet developed by the Office of Finance. The Contractor shall coordinate this report with the COR, the GPM, and a DC/TC representative (as appropriate).

2.3.6 Contract Actuals and Resource Leveling Report

The Contractor shall report monthly the contract actuals of hour and fund expenditures for each labor category, other direct costs, and for travel. The report shall also indicate the number of hour/funds left in each category. The Contractor shall also include a summary of all employees on board, departed, or in process. A sample template will be provided to the Contractor upon contract award. The report is due on the 10th working day of each month, when the invoice is submitted.

2.3.7 Vendor Accounts Payable Report

The Contractor shall submit quarterly, a cumulative accounts payable estimate as of a particular date (to be defined by the requester), to DEA's Office of Finance. The accounts payable estimate shall include billed, but unpaid invoices, as well as unbilled services provided to DC. The report must include invoice numbers and support (if needed) for these estimates.

2.4 Articles of Delivery

2.4.1 Acceptance of Deliverables

Where directed, deliverables are subject to review and approval by the Government through the COR. The COR and or GPM will return comments and/or approvals within ten (10) business days of submission by the Contractor, for those deliverables requiring content review prior to publication.

All project deliverables listed in Exhibit 3 shall conform to standard DEA templates as directed by the government, and are subject to the policies and procedures in the relevant DEA Process Plans, such as the Requirements Management Plan and the Configuration Management Plan.

2.4.2 Rejection of Deliverables

If the government determines that a Deliverable does not have the characteristics or otherwise meets the acceptance criteria set forth in the contract, the government will inform the Contractor in writing of its rejection, remedies for correction, and a timeline for correction.

SECTION III – PERSONNEL

3.1. Key Personnel

Key Personnel must demonstrate successful past performance of the type of work defined in this SOW. The Contractor shall provide the resumes of all proposed Key Personnel for the Government's review and approval prior to employment. The Position Descriptions for all Key Personnel are outlined in Exhibit 5.

3.2. Staff Personnel

It is expected that all Contractor personnel possess the individual training/experience requirements as outlined in each position description. As stated previously, the DEA reserves the right to review the qualifications of all staff selected to work for the contract prior to assignment, and to reject any individual whom it determines is not suitable for the contract requirements. The Position Descriptions for all Staff Personnel are outlined in Exhibit 6.

3.3 Management of Personnel

The Contractor shall manage all personnel matters regarding contract employees and shall interface with the COR with regular status reports (e.g., weekly or biweekly) either orally or in writing, regarding all personnel matters affecting the contract. The responsibility for these matters must be provided by the Program Director or his/her designate. All personnel matters, to include recruitment, appointment, security issues, schedules, time and attendance, performance issues, and terminations, shall be managed by the Program Director or his/her designee. At a minimum, the Contractor is expected to perform the following personnel related responsibilities:

- Assess on a daily basis the status of the workload, and, if required, recommend or take appropriate measures to correct any emergency developments, which may impede timely performance of the contract
- Recommend personnel assignments and changes to ensure satisfactory performance
- Interface with the COR as needed regarding performance issues
- Sort and log quality control error slips, assign document control numbers to the errors for review, and ensure that corrective actions are implemented
- Prepare daily, weekly, and semi-monthly project status reports with the analysis of statistical data relating to staff productivity, accuracy rates, and staff attendance
- Review employee time sheets for accuracy and completeness, as well as compliance with established contractor preparation guidelines and DEA time and attendance reporting requirements
- Ensure accuracy of submitted invoices
- Revise standard operating procedures to ensure the completion of tasks, projects, reports, and other duties
- Manage and prepare personnel actions, memoranda, and other correspondence related to contractor personnel issues
- Coordinate contractor personnel training and monitor the effectiveness of the training program.

3.4 Recruitment Plan

The Contractor shall implement and maintain a recruitment plan to provide for quality and timely services in accordance with this contract. Proper recruitment practices allow the Contractor to effectively respond to Government performance requirements. The Contractor's recruitment services shall include the following:

- The Contractor shall be solely responsible for advertising for personnel. The advertisement should include security requirements and specify the requirement for a background investigation. Advertisements should describe the specific position being recruited -- not a generic labor category description

- The Contractor shall be solely responsible for the recruiting of candidates. The Contractor shall utilize established procedures for recruitment, including personal interviews, checking references, and matching candidates to offices. Recruitment shall be managed to provide quick identification of recommended personnel for security review
- The Contractor shall not perform any recruitment activities at Government locations, nor shall the Contractor utilize any Government resources/equipment for any recruitment activities, except in the case of a career fair or other Government sponsored recruiting event
- Upon request by the COR or government PM, the Contractor shall allow and schedule a "meet and greet" between any prospective key personnel employee and the government manager for whom the contractor will be assigned

3.5 Retention Plan

In addition, the Contractor shall implement and maintain the retention program included in its technical proposal to encourage continued employment of qualified personnel. Objectives of the retention program should address how the Contractor will minimize turnover of existing Contractor staff, identify employees with upward mobility potential, and make career advancement options (within the Contractor's organization) available to those employees. Attainment of these objectives as well as the staffing of ordered positions will be of significant consideration when evaluating the Contractor's past performance. A report reflecting status on these factors is due to the COR the 1st working day of each week or month, as determined by the government upon contract award.

3.6 Security Designation and Requirements

All Contractor personnel must undergo a comprehensive security screening prior to start with the DEA. The personnel security access level for this contract is Sensitive but Unclassified (SBU). Only U.S. citizens shall be permitted to perform services on this contract. Under no circumstances shall contractors have access to National Security Information (NSI) or NSI systems. The risk level associated with this contract is "Moderate" and the personnel working on this contract effort must undergo the appropriate background investigation or be issued a waiver by the Office of Security Programs, Personnel Security Section (ISR), prior to commencing work on this contract. ISR will conduct suitability reviews on all contractor personnel requiring access to DEA facilities, information technology systems, or SBU materials. ISR will make a final suitability determination on each contractor meeting the specified requirements. For additional information, see DEA-2852.204.83 attached at Exhibit 4. Also at Exhibit 4, are blank copies of all the required security forms. The Security Package to the COR must be submitted as follows, in the order indicated:

- Cover memorandum on company letterhead, stating individual's name, CLIN, and title of position to which assigned
- Completed eQuip JSTARS Information Form
- Three Applicant Fingerprint Cards – FD-258 or results from a fingerprint scan from the FBI's fingerprint identification database (IAFIS), including rap sheet
- OF-306-Declaration for Federal Employment
- Additional Questions for Moderate Risk Positions
- DEA Contract Employee's Authorization to Conduct Agency-Specific Record Checks
- Contractor Drug Use Statement
- Drug Questionnaire – OMB No. 1117-0043
- Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
- Release-Fair Credit Reporting Act of 1970, As Amended
- Credit Report from one of the three primary credit bureaus – TransUnion, Equifax, or Experian

- On-Site Contractor Responsibilities form
- Contractor Ethics Questionnaire
- Self-Reporting Requirements for all Contractor Personnel form
- Non-Criminal Justice Applicant's Privacy Rights form

In addition to the above forms, it is advisable that the Contractor conduct a Background Screening inquiry on each candidate, which will provide information on any arrests, criminal allegations, registration with the national sex offender database, motor vehicle records, and civil allegations. The results from this screening should be provided to the COR along with the other security forms identified above.

In the course of reviewing the security package, the COR and/or DEA's Office of Security Programs, may request additional information from a candidate such as proof of the resolution of credit issues, Naturalization and/or Loyalty Oath or Passport, and Foreign National Relatives Statement. The COR will examine the security package and may advise the Contractor to disqualify a candidate from further consideration based on derogatory information disclosed in the packet.

SECTION IV – CONTRACT ADMINISTRATION

4.1 Time and Place

4.1.1 Place of Performance

Work shall be performed at the primary location at DEA Headquarters in Arlington, Virginia or at the DEA Sterling Park Technology Center in Sterling, Virginia, and at any future DEA work locations to be established. The Contractor shall provide a monthly report along with the invoice that verifies each employee's attendance for each work day, the details for which are indicated under Invoicing.

4.1.2 Core Work Hours

For exempt and non-exempt employees, the standard daily shift is 8.5 hours, in which 8 hours is billable to DEA. Within the 8.5 hours, an employee has two 15 minutes breaks (15 minutes for every 4 hours worked) and a 30 minute lunch. The standard work hours begin no earlier than 7:00 am and end no later than 7 pm (without prior approval or depending on each section's needs). The standard work schedule is: 7:30am to 4pm, 8am to 4:30pm, or 8:30am to 5:00pm.

The COR may request that the Contract Program Director (PD) establish set working hours for each contract employee. Changes in the established schedule should not occur without the advanced permission of the PD or his/her designate. In addition, the COR may request that the PD establish staggered lunch breaks to ensure adequate coverage of offices. If lunch breaks are established, deviations should not occur without the advanced permission of the PD or his/her designee.

On rare occasions, and not as a regularly established work schedule, the allowance of flextime (e.g., making up time off on another day) may be allowed. The flex schedule must be approved in advance by the PD or his/her designee. The PD must ensure that any flex schedule approved is carefully documented to ensure hours worked equal 40/80 for the week/pay period.

4.1.3 Telework Policy

Telework for contractors may be available to allow for flexibility in meeting the DEA's mission. Telework is defined as work performed at home or within 50 miles of the Contractor's duty station. Contractors may be allowed to telework on a situational/project basis or routine basis based upon position and person suitability, as determined by the government and outlined in the DEA Telework Procedural Guide (see Exhibit 7). Telework is not a right and is subject to final government and company approval. All contractors who telework must follow all applicable procedural requirements outlined in the DEA Telework Procedural Guide, including annual telework training, and daily and/or weekly telework reports in accordance with stated procedures. The specific telework parameters are outlined in DEA-2852-242-80, Contractor Telework, October 2018.

Remote work is defined as work performed outside 50 miles of the Contractor's duty station and will be considered by the government on a case-by-case basis.

4.1.4 Overtime

Service Contract Act (SCA) exempt employees may be required to work after hours or on weekends to address emergency situations or to meet the deadline for special projects. The PD or his/her designee must obtain advance approval for these occasions from the COR. In those instances where after-hours work is required, the PD may

modify work schedules of the exempt employees to accommodate the extra hours. SCA non-exempt employees are entitled to time and half pay for any hours worked beyond a 40-hour work week. Thus, the PD must obtain approval in advance from the COR for any non-exempt employee who may be required to work after hours. Any overtime hours worked by a non-exempt contract employee that has not been approved in advance by the PD and the COR will be compensated at the COR's discretion.

4.2 Training of Contractor Personnel

The Contractor shall be responsible for providing fully qualified, trained, and experienced staff for the work to be performed under this contract, and shall be responsible for continuously monitoring, managing, and controlling the work of all contractor staff throughout the life of the contract.

The Contractor shall train its own staff to ensure that all personnel are compliant with the qualifications and requirements of their labor category and are able to satisfactorily perform those duties under each Task Order issued. The Contractor is responsible for ensuring that individual employees have achieved the required competency levels required under this contract and upon request by the Government, the Contractor shall furnish the COR with formal documentation of training provided to contractor staff.

In addition to technical training, the DEA requires that a number of training courses are completed annually. Completion of these courses is mandatory and will be monitored by the COR. The incompletion of any DEA required course by an employee will be reported to the PD for appropriate action.

4.3 Travel and Related Costs

Travel is not a primary function under the contract; however, Contractor personnel may be required to travel to facilities other than the primary reporting office(s). For example, contractor personnel may be required to establish a satellite office or a disaster recovery site. All travel costs will be authorized by the COR and senior DC/TC management on a case-by-case basis and approved as set forth herein.

All travel must be reviewed and approved by the COR prior to travel. Any expenses incurred by Contractor personnel without prior COR approval may be denied for payment. Travel requests shall be submitted to the COR as follows:

- Traveler's name, positon title, and CLIN
- Destination
- Authorization for travel from PD, GPM, or other official
- Purpose of travel
- Duration of travel, including departure and arrival days
- The current GSA per diem allowable rates for hotel and M&IE for the destination city (available at www.GSA.gov)
- A detailed breakdown of the estimated travel costs, including: airfare, hotel, M&IE, car rental, estimated G&A costs, and other miscellaneous expenses
- Justification for hotel expenses above the allowable rate (if applicable)

Once travel has been completed, the Contractor must submit documentation with the invoice to the COR supporting the travel costs. The documentation must include the following information:

- traveler's name, position title, and CLIN
- Destination and dates of travel

- A breakdown of all costs, including air fare, car rental, hotel, M&IE, G&A, and miscellaneous costs
- Receipts for air fare, car rental, hotel, and any other receipts that can be provided indicating costs, such as gasoline, parking fees, or transportation (e.g., Uber or taxi)

The Contractor shall be reimbursed for actual, allowable travel costs and travel allowances (per diem) of personnel who are were authorized to travel in advance of the travel, in accordance with the established policy of the Federal Travel Regulation. Such transportation costs will not be reimbursed in an amount greater than the cost of first class rail or economy air travel, unless first class rail or economy air travel space are not available and the contractor certifies to these facts in the voucher or other documents submitted for reimbursement.

Travel directed by the government under this contract shall be incurred in accordance with the Department of Justice and DEA travel regulations, Federal Acquisition Regulations Part 31, 41 Code of Federal Regulations § 300 and 301, Federal Travel Regulations (FTR), and applicable Fair Labor Standards Act regulations. Travel expenses will be reimbursed on an actual expense basis in accordance with the FTR. No direct travel costs from place of residence to and from the normally assigned worksite will be allowable under this contract.

Domestic U.S. travel rates (i.e., per diem, mileage, etc.) can be found at the General Services Administration, Office of Government-wide Policy, Office of Transportation and Personal Property, Travel & Transportation Management Policy Division, Washington, DC 20405, (202) 501-1538, or at www.gsa.gov.

4.4 Invoicing

4.4.1 Invoice Documentation Requirements

Submission of an accurate invoice that includes all the requirements listed below, will ensure timely payment of the Contractor. Invoices will be carefully inspected by the COR. Invoices that are incorrect or which are lacking information will be formally rejected by the COR. The following parameters are required:

- Invoices are due the 10th working day of each month (the 9th if the 10th falls on a Saturday or the 11th if the 10th falls on a Sunday)
- Invoices must be submitted simultaneously to the DCA invoice email box at invoice.diversion@usdoj.gov and to the COR at carol.j.antoun@dea.gov
- The invoice must contain:
    - Separate, distinct invoice number
    - Contract Number
    - Specific Task Order Number
    - Performance period for the Task Order
    - Performance period for the billing period
    - Cumulative amount billed since beginning of performance period
    - Cumulative hours used since beginning of performance period
    - Summary page that lists each CLIN, position title, hourly rate, current hours billed, current amount billed, cumulative hours billed, and cumulative amount billed, sorted by CLIN
    - Employee labor supporting schedule reflecting each day worked by each employee, in employee alpha order
    - Summary report of resources devoted to each billing category – management, technology services, customer support services, ODC
    - Supporting documents (receipts) for all ODC costs
    - Supporting documents (receipts) for all Travel costs

- Time and Attendance Report

TGD has created a timekeeping system in which all contract employees must record their daily work. Failure of any employee to not record their hours may result in the employee not being paid for that day. From this system, the Contractor shall provide a report for the billing period that lists each employee, each work day, and the hours worked for that day. This report will be used by the COR to verify that the hours billed are the hours recorded by each employee. This report is due with the invoice.

4.4.2 Other Direct Costs

Other Direct Costs are those costs that cannot be billed to a specific labor category and may include things such as consulting services or duplication of materials. All anticipated ODC must be approved in advance by the COR and prior to the invoicing period.

4.5 COR Evaluations

4.5.1 Monthly Customer Satisfaction Surveys

The COR will evaluate the performance of the Contractor in terms of communication throughout the performance period, with Customer Satisfaction Surveys, that will include the completeness and quality of performance requirements and deliverables, as well as the timeliness of deliverables. All Findings and Recommendations reports, as well as the Activity/Progress Status Reports, must be technically and grammatically correct. Activity and progress reports must reflect work performed in the reporting period, problems encountered, milestones achieved, and/or deliverables submitted, work scheduled for the next reporting period, test results, comments, and funding status. All deliverable due dates (including those for services) must be met in accordance with the contract schedule.

4.5.2 Annual CPARS Evaluation

Under the FAR, government agencies are required to complete a detailed and complete evaluation of a contractor's performance in the Contractor Performance Assessment Reporting System (CPARS). The COR for this contract is responsible for preparing the CPARS rating on an annual basis and for the Contracting Officer's final review and approval. The rating will be prepared and submitted at the conclusion of each Option Period. In addition to the monthly Customer Satisfaction Surveys, the COR will base the rating on a number of measuring factors and records such as conformance with the Service Level Agreement Plan, Quality Control Plan, EVM Plan and to regulatory and policy statements and procedures. The COR will also survey government program managers regarding their assessment of the contractor's performance during the Option Period to include in the evaluation.