**SAMPLE – For Reference Only –** This sample is a redacted copy of a work statement accomplished under a NITAAC GWAC. A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach. The Table of Contents below is informational only and is provided to you for purposes of outlining the PWS/SOO/SOW. **This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references and regulations to their own PWS/SOO/SOW.**

Table of Contents

[1. Background 2](#_Toc11828347)

[1.1. Mission of the <AGENCY> 2](#_Toc11828348)

[1.2. Mission of the Chief Financial Officer (CFO) 2](#_Toc11828349)

[1.3. Office of Corporate Information Systems 2](#_Toc11828350)

[2. Collaboration 3](#_Toc11828351)

[3. Scope 3](#_Toc11828352)

[3.1. Acquisition Objectives 3](#_Toc11828353)

[3.2. Contractor Responsibilities 4](#_Toc11828354)

[3.2.1. Principle Place of Performance 4](#_Toc11828355)

[3.2.2. Government-Furnished Property and Data 4](#_Toc11828356)

[3.2.3. Telework and Flexi-place – Situational, Temporary or Permanent 4](#_Toc11828357)

[3.2.4. Teleworking During a Government Closure 5](#_Toc11828358)

[3.2.5. Continuity of Operations During a Government Closure 6](#_Toc11828359)

[3.2.6. Security Clearances 6](#_Toc11828360)

[3.2.7. Segregation of Duties 6](#_Toc11828361)

[3.2.8 Contract Type 6](#_Toc11828362)

[4. CYBER SECURITY SUPPORT SERVICES 6](#_Toc11828363)

[4.1. Deliverables 9](#_Toc11828364)

[5. PERFORMANCE MEASURES/EXPECTATIONS 10](#_Toc11828365)

**Performance Work Statement
Cyber-Security Support Services**

# Background

##  **Mission of the <AGENCY>**

XXX

##  Mission of the Chief Financial Officer (CFO)

The mission of the Office of the Chief Financial Officer (OCFO) is to assure the effective management and financial integrity of <AGENCY> programs, activities, and resources by developing and implementing and monitoring Department-wide policies and systems in the areas of budget administration, program analysis and evaluation, finance and accounting, internal controls, corporate financial systems, and strategic planning.

## Office of Corporate Information Systems

The Office of Corporate Information Systems (OCIS) is committed to fostering <AGENCY>’s mission through the provision of:

* Secure, accurate, and timely business transaction capabilities that enable the <AGENCY> complex to acquire and track needed assets, goods and services;
* Accurate information that facilitates knowledgeable decision making by improving transparency and accountability of all OCFO corporate data.
* The business systems software applications are currently composed of 26 distinct FISMA moderate or low reportable systems. The flagship systems include:
* **Standard Accounting and Reporting System (STARS)**. STARS is <AGENCY>’s implementation of the Oracle e-Business Suite (Federal Administrator, General Ledger, Accounts Payables, Purchasing, Accounts Receivables, and Fixed Assets);
* **Strategic Integrated Procurement Enterprise System (STRIPES)**. STRIPES is <AGENCY>’s implementation of Compusearch’s PRISM (Requisitions, Solicitations, Acquisition and Financial Assistance) life cycle modules;
* **iPortal.** iPortal is the single point of entry into the OCIS Systems using Oracle WebCenter Suite, Oracle Universal Content Management, Oracle Services Orientated Architecture (SOA), Oracle Access Manager (OAM);
* **Integrated Data Warehouse (IDW)**. IDW is the integration of <AGENCY>’s corporate business information utilizing Oracle Database and Oracle Warehouse Builder (OWB);
* **Entity Portfolio Assessment Tool (EPAT)**. EPAT uses Oracle’s Primavera Portfolio Manager (PPM);
* **Funds Distribution System (FDS) 2.0** uses Oracle Hyperion software for budget planning, execution and funds distribution processes and systems.
* Forms applications running on iPortal and IDW developed using Oracle Application Express (APEX); and
* Interfaces including Web interfaces that enable sharing or exchange of data with other business systems.

# Collaboration

All Contractors involved with the OCFO Program will work collaboratively with Federal staff and other Contractors and follow the direction of the Contracting Officer, Contracting Officer’s Representative (COR) or Alternate COR, in collaboration with the Federal Program Manager, or designee. This collaboration includes day-to-day activities, planning, development, prioritization, knowledge transfer and creating and sharing documentation.

The Contractors will need to work together to best achieve the OCFO vision for. Within Program, the following major roles and responsibilities include:

* **Program Management Consulting, Integration and Mission Support Services Contractors Program Management).** The Program Management Contractors are responsible for providing program management, consulting, integration, and mission support services to the OCFO
* **Operations and Maintenance (O&M) Contractor.** The O&M Contractor is responsible for the O&M of the OCIS systems currently in the O&M phase of the systems’ lifecycle, including upgrades, patches, and other enhancements. Additional systems may be added at the direction of the Contracting Officer in collaboration with the Federal Program Manager
* **Office of Corporate Information Systems (OCIS)**. The Office of Corporate Information Systems (OCIS) Federal Staff, which fall under the OCFO, are responsible for Federal Project Management oversight of the OCIS Program and OCFO support services. The Federal Program and Project Managers are responsible for the overall direction and management oversight of the various projects. The other Federal staff may assume various roles on their teams and provides additional support on key tasks
* **Other OCFO Contractors.** The Program Management Contractor will be responsible for collaborating and cooperating with all other OCFO Contractors, and will respond in the fashion directed by the COR, Alternate COR, or the Federal Program Manager
* **Office of the Chief Information Officer (OCIO).** The Office of the Chief Information Officer (OCIO) Application Hosting Environment (AHE) provides application hosting and housing services, and provides customers with a fully managed hosting solution. They typically provide infrastructure support from the Operating System down to the hardware; and
* **User Stakeholder Groups**. Individual communication with our various user stakeholder groups in the program and field offices occur as needed when implementing new services and software applications, as well as business process improvements.

# Scope

## Acquisition Objectives

The purpose of this contract is to acquire specialized technical support services to support the implementation and enforcement of cybersecurity requirements for the systems, applications, databases, computing environments and other supporting IT in the Office of the Chief Financial Officer (OCFO).

## Contractor Responsibilities

Support services provided by this acquisition include project management, consulting, administrative, and technical in support of the performance objectives in Section 4 of this PWS.

### **Principle Place of Performance**

The principle place of performance is the XXX, and the current office locations are the <LOCATIONS>. The Government may change the office location at its discretion.
All Key Personnel must work onsite at the XXX or other designated site in the XXX Metropolitan area, as agreed upon by <AGENCY>.

### Government-Furnished Property and Data

Will provide office space, computers and other required information technology hardware and software, office furniture, telephones, cell phones (on an as-needed basis) and office supplies at the XXX locations. may provide office space at other buildings in the XXX Metropolitan area, if office space is available and a need exists. Some travel may be required.

### Telework and Flexi-place – Situational, Temporary or Permanent

Depending on the nature of the work, and with concurrence of, the Contractor may allow certain Non-Key individuals to work remotely, via telework, on a situational, temporary or permanent basis.

Each Contractor employee authorized to telework shall comply with all of the following conditions:

Use only a secure computer/laptop with all necessary software and hardware when teleworking from home or some other alternate work location.
Perform services under this PWS as a teleworker and understand that the teleworking arrangement is a work alternative that must be requested and approved by the COR and the Contractor’s Project Manager prior to beginning a telework assignment.

Retain the same duties, obligations, and responsibilities assigned under this acquisition without change throughout the telework schedule.

Conform with the teleworker’s work schedule, overtime compensation (if any), leave, and other terms and conditions of employment with his/her employer as specified in the Contractor’s current collective bargaining agreement or personnel policy, as applicable, and meet the terms agreed upon with the Contractor’s Program Manager.

Develop an effective communications strategy with the Contractor’s Program Manager and work group, including required meetings held at the; and follow that approved strategy throughout the telework schedule.

Designate the Contractor employee’s home or some other alternate work location as the Contractor employee’s official telework location, subject to approval by the Contractor’s Program Manager.

Acknowledge that teleworking is not an entitlement and may be terminated by the COR or the Contractor’s Program Manager at any time.

Return any Government-furnished telework equipment, software, data, and supplies upon termination of the telework assignment or upon separation from this acquisition for any reason.

Immediately notify the Contractor’s Program Manager of any equipment malfunction and the impact of the malfunction upon the teleworker’s ability to continue the telework assignment; and obtain instructions from the Contractor’s Program Manager about working at another alternate work location.

Be responsible for the maintenance and repair of all the teleworker’s personal property, and for maintaining appropriate insurance coverage against loss or theft for all Government-furnished equipment/supplies in the possession of the teleworker.

Acknowledge that all work products, including documents, reports, and data created as a result of the teleworker’s work-related activities are owned by the Government and shall be properly secured and returned to the Government as instructed by the Contractor’s Program Manager.

Acknowledge receipt and compliance with the technology guidelines for securing equipment for telework assignments.

Acknowledge receipt and compliance with Information, Physical Access, and Personal Identity Information (PII) Security provisions applicable to the acquisition.

Acknowledge that the Contractor employee’s approved telework location is considered an extension of the Contractor’s worksite.

Under special circumstances other than a Government closure, the COR and the Contractor’s Program Manager may authorize a Contractor employee to telework under the above conditions.

### Teleworking During a Government Closure

During a period of Government closure, a Contractor employee with a secure computer/laptop must telework from home or some other alternate work location (including the Contractor’s facility) that is not a “Federally-controlled facility”, provided that approval has been received from the COR and the Contractor’s Program Manager. Since teleworking will be authorized only as a short-term remedy to an emergency situation, the Contractor agrees that there will be no additional charges to the Government. The Contractor shall provide the Government with a copy of their employee established telework agreements.

All Contractor employees teleworking during Government closure must comply with the same conditions listed in Section 3.2.3 above.

### Continuity of Operations During a Government Closure

The Contractor shall submit a plan entitled Continuity of Operations During a Government Closure to the COR for approval within 20 calendar days following an instruction from the COR to do so. The plan shall sufficiently specify what work tasks would be performed at non-Government location(s) (i.e., not a “Federally-controlled facility”) during a closure and which Contractor employees would be authorized to telework.

The Contractor shall implement its approved Continuity of Operations During a Government Closure plan when directed by the COR.

### Security Clearances

All personnel supporting this contract must obtain a public trust high determination.

### Segregation of Duties

The Contractor must ensure that the security control assessments are completed per Federal and cybersecurity guidelines. To support the integrity of these assessments, a segregation of duties will be required for the individuals assigned to the security control assessment and vulnerability scanning services tasks within this cybersecurity support services task order.

3.2.8 Contract Type

The contract type for this contract will be Time and Materials.

# CYBER SECURITY SUPPORT SERVICES

The Contractor shall provide cybersecurity technical expertise of NIST, and federal regulations, directives, and guidelines to the OCFO. This includes all aspects of a system’s security life cycle, from developing and maintaining Assessment and Authorization (A&A) documentation to performing independent validation and verification of controls to on-going operational security support.

The Contractor shall update and maintain the OCFO Risk Management Framework to current standards, guidelines, and approaches. The Contractor shall ensure that the OCFO’s cyber security program adheres to Federal (NIST, OMB, DHS, <AGENCY> etc.), executive orders, national security directives, and other regulations.

The Contractor shall coordinate with the OCFO systems owners to prepare, update, and maintain the necessary system security documentation for assessment and accreditation activities. The Contractor shall create/update/maintain templates to support the effective and efficient security documentation practices.

The Contractor shall conduct an independent security assessment of security controls for OCFO systems through interviews, document reviews, and testing of the system to ensure that appropriate controls are in place and operating as designed and intended. Assessments must be performed by qualified personnel, include thorough analysis and be accomplished in accordance with the OCFO Risk Management Framework, current NIST regulations, and other required and federal standards and regulations. Based on the makeup of the environments, servers, network devices, operating systems, application software, web servers and database servers, the Contractor shall identify the applicable NIST and other security guidelines and perform security evaluations. The Contractor must obtain Government approval on the applicability of external standards and the testing approach before they proceed. The assessment approach for OCFO systems is as follows:

* 1. Assessed for compliance to the NIST moderate or low baselines.
	2. Each year approximately, a third of the controls are assessed ensuring that all controls are assessed at least once every three year to support an authorization to operate.

The Contractor shall coordinate and conduct web application vulnerability assessment scanning on OCFO systems. The Contractor shall perform thorough analysis of the results and provide industry standard recommendations in the form of vulnerability scan reports. The Contractor shall coordinate with the system owner and teams to validate false positives. The Contractor shall provide a monthly vulnerability report to track the status of all vulnerabilities for OCFO systems. The Contractor shall coordinate with other scanning teams (infrastructure and database) to collect, correlate, and consolidate scan results. The overall scan results shall be presented on a vulnerability dashboard. The Contractor shall stay abreast of current security vulnerabilities and potential implications to the OCFO systems and inform OCFO of potential security threats to the systems and provide thorough analysis and industry standard recommendations on how to resolve or mitigate the threats introduced by the vulnerabilities.

The Contractor shall provide expert analysis and recommendations on risk (to include impact and likelihood) and mitigation options for security findings, gaps and vulnerabilities. This includes developing appropriate responses to audit report findings. If risks cannot be resolved, the Contractor shall work with the ISSM, and system owner to develop a Deviation Waiver Request (Risk Acceptance) based on thorough analysis and industry standards identifying the risk, impact/threat if exploited, existing countermeasures, risk level, and reason/justification for risk.

The Contractor shall update and maintain the OCFO continuous monitoring program. This includes identifying and implementing continuous monitoring mechanisms, strategies, and approaches. The Contractor shall provide and maintain a catalog of all continuously monitored system security controls, monitoring frequency, and monitoring approach (manual, automated etc.)

The Contractor shall provide a monthly Plan of Action and Milestones (POA&M) report to track the status of all POA&Ms for OCFO systems. If POA&Ms are due within the month, the Contractor shall work with the POA&M system owner to get resolution on the POA&M item or if the POA&M date needs to be extended, the Contractor shall require a valid justification from the POA&M system owner. The Contractor shall track the history of each POA&M to include the initial POA&M information and any modifications to the POA&M (i.e., justification(s) to the POA&M date).

The Contractor shall provide a quarterly software lifecycle report. The report should identify OCFO software components that are obsolete, end of life, or near end of life (within 18 months) based on information provided by the Department’s enterprise software lifecycle tool. Data provided by the tool should be augmented by manual research and review approaches to ensure adequate coverage for OCFO software components.

The Contractor shall maintain an up-to-date inventory of the following:

1. OCFO IT assets to include application software, databases, and supporting hardware to include versions and life cycle status (current, retiring, end-of-life etc.)
2. Privileged access authorizations.
	* Ports, protocols, and services.
	* Firewall rules.

The Contractor shall prepare responses in support of ad-hoc and federal data calls to include quarterly FISMA updates.

The Contractor shall support OCFO incident response activities. This includes analyzing, coordinating, tracking, and closing incidents. All incidents must be captured on the OCFO Incident Log.

The Contractor shall create, update, and maintain processes and procedures for cybersecurity functions and activities. The documentation shall be centrally stored on the OCFO portal.

The Contractor shall stay abreast of OCFO system change management activities and perform security testing and thorough analysis to ensure that none of the changes/modifications/updates introduce security risk into the environment.

The Contractor shall provide industry standard technical expertise to include research or updates on new or upgraded operating systems, patches, hotfixes, applications, databases, Commercial-off-the-Shelf (COTS) products, security tools, issue resolution, vulnerability evaluation, countermeasure implementation, auditing/intrusion detection tools, and all other security-relevant areas, as required.

The Contractor shall provide additional qualified support within notice of two weeks to support to support new and unanticipated cybersecurity support requirements, as required.

The Contractor shall ensure that within the Cybersecurity contract team, the following:
Require employee(s) performing vulnerability management functions possess demonstrable credentials to reflect knowledge, skills, and experience in operating web vulnerability assessment tools, and analyzing and interpreting results.

* 1. Require an employee possessing demonstrable credentials to reflect knowledge, skills, and experience on securing Linux/Unix based operating systems such as Red Hat / Oracle Enterprise Linux, and IBM AIX.
	2. Require an employee possessing demonstrable expertise to reflect knowledge, skills, and experience on securing database systems such as Oracle.
	3. Require an employee possessing demonstrable expertise to reflect knowledge, skills, and experience on securing corporate business systems supporting functions such as financial management, budget, procurement, travel, HR/payroll, and data warehousing,

The Contractor shall ensure all functions and activities are performed in accordance with all federal, <AGENCY>, state, and local regulations and guidelines.

## Deliverables

| **Deliverable** | **Due Date** |
| --- | --- |
| Project/Implementation Plan | Within 10 work days of award  |
| Revised Project Plan | Within 7 business days of technical monitor notification |
| Project Status Reports | Monthly |
| Meeting Minutes  | Within 1 day of meeting |
| Updated Security Documentation for 26 systems (Security plan, Configuration Management Plan, Contingency Plan, PIA/PNA, Control Assessment Plan, and other System related documentation) | Annually |
| Security Control Assessments | Annually, in accordance with mutually agreement upon assessment schedules. |
| Risk Assessment Report, Security Assessment Report and memo and other supporting materials | Within 2 weeks of completion of Security Control Assessment. |
| Security Impact Assessments | As required |
| Risk Assessments / Deviation Waiver Requests | As required |
| Security tasks/activities project schedule | Weekly |
| Vulnerability Reports | Monthly; As required |
| Vulnerability Dashboard | Monthly |
| POA&M Report | Monthly |
| OCFO IT Asset Inventory Updates | Quarterly; As required |
| Incident Log | Monthly |
| Unsupported Software Lifecycle Report | Quarterly; |
| Cybersecurity Metrics Scorecard | Monthly |
| Privileged Access Authorization Reviews | Quarterly; As required |

# PERFORMANCE MEASURES/EXPECTATIONS

The Performance Measures/ Expectations apply to Sections 4 of this PWS.

* Responds to requests for new work orders within 48 hours and delivers new or updated project plans within ten (10) working days of receiving the detailed requirements from the Contracting Officer, Contracting Officer’s Representative, Federal Project Manager, or designee. The Contractor will discuss impacts on other projects in their project plans. The Government must provide adequate requirements, and answer all relevant questions posed by the Contractor within two (2) days. If the Government takes longer than two (2) days to respond or provide clarification of the requirements, the ten (10)-day timeline for Contractor’s delivery of project plans will be extended by the amount of time it took the Government to respond. All project plans agreed upon with Contracting Officer, Contracting Officer’s Representative, Federal Project Manager, or designee will be accomplished within 5% of schedule.