**Disclaimer:** This is a sample document. Agencies are encouraged to tailor the contents to fit their individual needs.

Cloud Migration Services Performance Work Statement (PWS)

# 1.0 Background

A small, under-resourced agency (Agency X) is facing a variety of deadlines, on regulatory legislative requirements such as cloud first, zero trust security, and single sign-on mandates. IT resources have been stagnant or falling. Requests and responsibilities are constantly increasing. Legacy applications, end-of-service-life hardware, and onboarding of orphaned systems contribute to rising technical debt.

Moving to the cloud provides some relief by lowering technical debt, reducing large upfront costs of hardware procurement, providing system flexibility (scale up, scale down), adding resiliency, allowing for increased automation and the ability to run with a smaller IT team. Moving to an interoperable multi-cloud environment that supports the portability and compatibility of applications and data, or at least standing up the foundation for one, will lessen the chance that Agency X faces vendor or technological lock-in several years down the line.

Cloud migration presents benefits in increased efficiency and reduced costs. However, it does have a substantial learning curve and requires knowledgeable staff that can convince leadership, justify the migration, build a core team and navigate the procurement and implementation maze.

# 2.0 Scope

Agency X has a need to migrate and adopt modern cloud computing capabilities. This procurement will allow Agency X to:

* Define the recommended future state for identified areas of focus;
* Establish detailed guidance on tools and processes for cloud governance, security, and management as per best practices; and
* Identify and build in automated security controls, enforcement, and evidence-based verification in the cloud environment towards a continuous authority to operate (ATO) process for onboarding emerging technologies.

It will also establish and configure a cloud environment that aligns with cloud management and governance standards to provide continuity of operations for mission teams utilizing consolidated analytics products and services at Agency X.

This Performance Work Statement (PWS) defines the work to be performed for Agency X. The work described herein will satisfy each of the Overall Task Objectives listed below in Section 2.1 of this PWS.

## 2.1 Overall Task Objectives

### 

2.1.1 The PWS establishes the following Overall Task Objectives:

1. **Future State Recommendation:** Define the recommended future state for each identified area of focus.
2. **Training & Transition Plan:** Successfully train, transition and handoff Project Backlog as well as any developed artifacts to the Operations and Maintenance team.
3. **Cloud Environment:** Establish detailed guidance on tools and processes for cloud governance, security, and management in alignment with best practices.
4. **ATO Support:** Identify and build in automated security controls, enforcement, and evidence-based verification in the cloud environment. Work towards a continuous ATO process for onboarding emerging technologies.
5. **Enterprise Solution Architecture:** Develop implementation architecture and technical documentation for cloud and infrastructure solutions.
6. **DevSecOps:** Prototype best of breed methods for deployments, change management, version control, and security while adhering to agile practices.
7. **Prototype:** Develop a minimal viable architecture of the designed cloud environment, products and tools deployed in it via DevSecOps pipeline.

***Note:*** *It is important for the government to be more explicit about this and similar terms. Proof of concept, non-production pilot, production pilot (limited user scope), full-production roll-out, managed service could all fall under this term based on who is interpreting it. It's common in contracts we've seen to use Pilot or Production but there are huge nuances that are directly relevant to contracting that should be unpacked a bit further before finalization.*

1. **Flexible Application Platform:** Establisha Flexible Application Platform. This is a platform where end users can build, deploy, run, monitor, and scale applications without having to manage and run their own infrastructure.
2. **Continuity of Operations:** Establish and configure cloud environment per cloud management and governance standards to provide continuity of operations for mission teams utilizing consolidated analytics products/services at Agency X.
3. **Change Management:** Conduct existing system and resource capabilities assessment; identify gaps and propose plans to improve cloud adoption success.

### 2.1.2 Tasks

In order to achieve the Overall Task Objectives, the Contractor will perform the following tasks. The first column is the name of the task that will be performed, the second column provides a description of what the task itself entails, and the third column is the overall task objective that the task will satisfy.

|  |  |  |
| --- | --- | --- |
| **Task Name** | **Task Description** | **Task Objective** |
| **Create a Network Architecture diagram.** | Create and/or update Network Architecture diagram, ensuring it has the ability to support an interoperable multi-cloud multi-vendor environment as [defined by the Federal CIO](https://www.cio.gov/assets/resources/Multi-Cloud%20and%20Hybrid%20Cloud%20Guide_v4_Final.pdf#page=6). | **E**: Enterprise Solution Architecture  **A**: Future State Recommendation  **H:** Flexible Application Platform  **I:** Continuity of Operations |
| **Participate in sprints, planning, reviews, and MVP demonstrations.** | Follow Agile practices in executing the tasks from the Project Backlog through an appropriately paced Scrum / Sprint cadence, as well as through the estimation, allocation, and achievement of appropriate sprint velocity through the use of “[story points](https://www.mountaingoatsoftware.com/blog/what-are-story-points)” or similar estimation metric. Demonstrate the Minimum Viable Product to the Product Owner and other stakeholders at the end of the sprint. | **F.** DevSecOps  **G.** Prototype  **H:** Flexible Application Platform  **J:** Change Management |
| **Develop prototypes for Cloud Service configurations.** | Develop vendor- and technology-agnostic proof of concepts, minimum viable products, or prototypes in support of use cases identified, as necessary. | **G**: Prototype  **H:** Flexible Application Platform |
| **Demonstrate security control and assessment validations via hardening scripts.** | Implement hardening scripts and processes to demonstrate security validations to aid in the ATO process. | **D**: ATO Support  **H:** Flexible Application Platform |
| **Develop how-to guides on cloud management, operations and support.** | Establish guidance on tools and processes for cloud configuration enhancement, security and management as per best practices. | **B**: Training & Transition plans  **C**: Cloud Environment  **H:** Flexible Application Platform  **I:** Continuity of Operations |
| **Create a System Design Document.** | Establish System Design Document that provides detailed guidance on tools and processes involved in product implementation, cloud/application configurations, security and management procedures for consumption by external teams; For example: Operations & Maintenance team. | **C**: Cloud Environment  **D**: ATO Support  **E**: Enterprise Solution Architecture  **H:** Flexible Application Platform  **I:** Continuity of Operations |
| **Build in automation for processes and scripts in:**   1. **DevSecOps;** 2. **Cloud management;** | Prototype best of breed methods for automating manual processes and workflows. For Example: Infrastructure-as-Code (IaC) and build once and deploy multiple times methodologies. | **G**: Prototype  **C**: Cloud Environment  **E**: Enterprise Solution Architecture  **H:** Flexible Application Platform  **I:** Continuity of Operations |
| **Pilot automation in the following areas:**   1. **Compliance scanning;** 2. **Hardening;** 3. **Vulnerability scanning.** | Identify ways to build in security controls, enforcement and evidence verification in the cloud environment towards a continuous ATO process for onboarding emerging technologies. | **D**: ATO Support |
| **Create deployment plans.** | Prototype best of breed methods for deployments. | **F**: DevSecOps |
| **Pilot COTS and cloud native services.** | Assess and pilot products and services that are interoperable, allow for portability of data and applications, provide for compatibility of data and applications, and fit the needs of the cloud operations management and data science platform. | **M**: Enterprise Solution Architecture  **C**: Cloud Environment |
| **Perform gap analysis** | Identify Analytics Applications’ maturity for migration and/or Cloud adoption, and  Conduct readiness assessments. | **J:** Change Management  **I:** Continuity of Operations |
| **Enhancing Cloud Environment** | Develop prototypes for enhancing Cloud Service configuration with a focus on supporting a multi-vendor multi-cloud environment. Implementing Cloud operations best practices in order to enhance the Agency X cloud environment in the following architectural considerations:   * End-to-End Automation * High Availability * Security Hardening * Contingency planning * Load Balancing * Interoperability, Portability, Compatibility | **C.** Cloud Environment  **I:** Continuity of Operations |
| **Automate Cloud operations and maintenance** | Using DevSecOps principles of automation and Infrastructure as Code, develop vendor-agnostic prototypes in order to automate processes and procedures in Agency X operations and maintenance.  Build in automation for processes and scripts in:   * DevSecOps * Cloud management   Pilot automation in the following areas:   * Compliance scanning * Hardening * Vulnerability scanning   Create deployment plans. | **C.** Cloud Environment  **F**. DevSecOps  **I:** Continuity of Operations |
| **Assist in securing Cloud ATO validation and demonstration of security controls** | Document ATO Boundary, Configuration of Agency X’s cloud environment hardening per security guidelines, validation and demonstration scripts of compliance of security controls.  Create a System Design Document.  Demonstrate security control and assessment validations via hardening scripts. | **D.** ATO Support |
| **Support selection, analysis and onboarding of new cloud based products and services** | Ability to provide Product Market Analysis reports, Rapid prototyping and demonstration of tools, Product capabilities and requirements matrix.  Pilot COTS and cloud native services. | **G**. Prototype |

### 

### 2.1.3 Deliverables

In conjunction with performing the tasks outlined above, the Contractor will provide the following deliverables. The first column is the name and description of the deliverable, the second column provides the standard upon which performance of the deliverable will be measured, and the third column is the deliverable’s associated task in this PWS. The deliverables will be inspected and approved by the Government Engagement Lead aka Technical POC.

|  |  |  |  |
| --- | --- | --- | --- |
| **Deliverable Name** | **Performance and Quality Standards** | **Associated Task Name** | **Due Date** |
| **Project Backlog** | Agency X has a requirement for the contractor to establish and maintain the Project Backlog in accordance with Agile methods and practices. The Government will retain sole property and distribution rights to the Project Backlog throughout the course, and upon completion of the order.   Additionally, the contractor will achieve the following quality metrics:  1. Each Sprint will last no more than 4 weeks;  2. Each Sprint will result in completion of at least 85% of the story points; | Participate in sprints, planning, reviews, and MVP demonstrations. | After first sprint planning and ongoing throughout contract performance |
| **Health Check** | An evaluation of the current state against industry best practices. | Create Health Check | Document included in a quarterly business review. |
| **Future state - cloud configuration recommendation** | Conducting future state of the Agency X CloudOps and Cloud configuration via roadmap analysis and providing recommendations via pilots and documentation to achieving it. | Create Network Architecture diagram  Create a System Design Document | For each implemented product added to the ecosystem by the end of Product Increment. |
| **Conduct Training and Knowledge transfer** | Train Innovation Lab team in Cloud service operations, maintenance; Document Automated processes, tools and procedures; Provide how-to guides on troubleshooting, triage and scaling exercises. | Develop how-to guides on cloud management, operations and support. | For each newly implemented product or service added to the ecosystem by the end of the Product Increment. |
| **Propose shared responsibility and shared fate model** | Support providing an operational model for sharing a multi-vendor, multi-cloud environment responsibly within the organization. | RACI matrix;  Create project and team intake forms | For each newly implemented product or service added to the ecosystem by the end of the Product Increment. |
| **Enhance Cloud Governance standards** | Establish a cloud governance framework to facilitate efficient and secure deployment of applications and provisioning of infrastructure | Security Boundary Diagrams; Operations & maintenance documents; Cloud naming, tagging and versioning standards;  Cost Estimation guides  Standard operating procedure docs | At the end of each Product Increment along with Change Request submission. |
| **Infrastructure as Code** | Develop and maintain automation in the form of Infrastructure as Code (IaC) where feasible for quality control and reusability across the environment according to DevSecOps standards. IaC will be delivered to the Government after acceptance at the conclusion of each sprint. | IaC committed to the government software configuration management (SCM) repository. | Along with every deliverable involving code development at the end of a SAFe Agile Program Increment. |
| **Architecture Documentation** | Develop Information system’s current state and future state from best in class reference architectures. Architecture documentation will be delivered to the Government after acceptance at the conclusion of each sprint. | Commit the Architecture documents in the Government designated repository. For example, Agency X uses a Document Management (DM) system for artifacts. | At the end of each Program Increment along with Authority to Operate (ATO) package submission. |

### 2.1.4 Measuring and maintaining quality

This requirement is performance-based with specific performance criteria. To satisfy the government’s associated needs, the government prepared a Quality Assurance Surveillance Plan (QASP) (attached to RFQ) to ensure performance of contractual requirements. The Contractor will be held to the processes described in the contract and QASP and failure to adhere to the processes may result in a reduced CPARS rating per the QASP.

## 2.2 Operating constraints

### 2.2.1 Government constraints

The following are known constraints at Agency X:

1. Agency X’s Information security and privacy controls must be respected at every stage.
2. Agency X’s technical documentation will be generated in Agency X’s preferred document management system with version control.
3. Agency X cloud configurations and updates will be performed within ATO authorization boundary of Agency X’s cloud accounts.
4. Onboarding of new services and products will need to be aligned with Agency X’s ATO security controls.
5. DevSecOps procedures will be implemented in an agile environment to enable the Agency X personnel in conducting data science experiments with minimal cloud proficiency.
6. Security automation and Cloud configuration hardening will be implemented to demonstrate compliance with SP 800-53 Rev. 4 standard controls for a FISMA moderate sensitivity federal information system.
7. Cloud architecture deliverables must promote interoperability, portability, and compatibility to support a multi-vendor multi-cloud environment.
8. Agency X’s source code versioning control technologies and principles will be followed and designated repository systems used. Agency X’s source code repositories will be used for all software updates to track and manage changes to infrastructure as code.

Additionally, the contractor must collaborate with other teams at Agency X in the following ways:

* **Agency X’s Communications and Outreach team:** Support the generation and delivery of executive level briefings, talking points, emails, and other communication materials.
* **Agency X’s Program Management Office:** Ensure required deliverables are documented for leadership review.
* **Chief Information Security Officer:** Ensure cooperation with Agency X’s security policies and protocols to address security concerns.

# 3.0 Contractor roles and responsibilities

## 3.1 Key Personnel

### 3.1.1 Cloud Architect/Technical Lead/Subject Matter Expert (TSME)

The TSME must have a full understanding of the technical approach to be used by the Contractor's team and will be responsible for ensuring that the Contractor’s team follows that approach.

### 3.1.2 Cloud/DevOps Engineer

The Cloud/DevOps Engineer must have a full understanding of automating Cloud solutions end-to-end, adhering to DevSecOps principles of Infrastructure as Code, build once-deploy anywhere, rapid prototyping, Continuous Integration and Continuous Delivery (CI/CD).

### 3.1.3 Cloud Full-Stack developer

The Cloud Full-stack developer must have a full understanding of the cloud based application development and will be building internet and intranet web applications based on cloud native, open-source, serverless technologies.

### 3.1.4 Key Personnel Substitution

In order to substitute any Key Personnel, those substitutions must be accepted by the Government in writing, and will only be justified by the Government request, sudden illness, death, change of employment, or termination of employment for cause.

Contractor requests for a substitution of Key Personnel must include a detailed explanation of the justifying circumstances, and a list of qualifications for the proposed substitute or addition, including skills, experience, education, training, and security level. The Government’s failure to accept a proposed substitution will not constitute grounds for non-performance by the Contractor, or form a valid basis for any claim for money or any equitable adjustment. In the event of a Key Personnel’s departure from the contract the Contractor will, ideally, have a replacement identified and accepted by the Government so there is no gap in service. However, the Contractor must propose a Key Personnel replacement no later than ten (10) business days of the original Key Personnel’s departure date. The Government has ten (10) business days to accept or reject a proposed substitution.

## 3.1 Security Clearances

Contractor personnel must be required to obtain and maintain security badges and adhere to the applicable installation security requirements. Homeland Security Presidential Directive (HSPD-12) mandates the issuance of a common form of identification for all federal employees and contractors for use in accessing government-controlled facilities and information systems. As a result, Contractor employees that require access to Agency facilities (including IT systems) for six (6) months or more will be required to pass a National Agency Check with Credit (NACIC) background investigation and obtain the HSPD-12 Tier 2 level clearance, if necessary for performance, before receiving computer access. The Contractor must be responsible for the cost of complying with HSPD-12.

The Contractor must comply with PIV requirements and follow guidelines for returning PIV cards within five (5) business days of contractor personnel departure and before contract closeout.

# 4.0 Government roles and responsibilities

## 4.1 Makeup of team

The Government team consists of the Contracting Officer (CO) and the Contracting Officer’s Representative (COR).

1. CO: {NAME}

The Contracting Officer is responsible for award and contractual administration of the resulting contract. No modifications to the contract will occur unless issued via an SF30 modification form signed by the Contracting Officer.

2. COR: {NAME}

The Contracting Officer’s Representative is responsible for technical oversight and administration of the contract. Consult the COR Delegation of Authority Memorandum for additional information.

Note: If a change occurs to either the CO or COR, the Government will notify the contractor. Specifically for the COR, the contractor will receive a copy of a “COR Delegation of Authority” assignment letter when a COR is assigned, and the contractor will also receive a letter rescinding the COR delegation when appropriate.

## 4.2 Contracting personnel

### 4.2.1 Contracting Officer

Questions, comments, issues, or responses must be submitted through the methods outlined in this solicitation. Any other forms of communication will not be considered. After award, the CO will delegate most of the day-to-day tasks to the COR/TPOC.

### 4.2.2 Other members

A delegation letter for the COR, signed by both the CO and COR, outlining the contractual roles and responsibilities of the COR/TPOC as well as the names and email addresses of the entire team will be provided no later than the kickoff meeting that will follow the award.

## 4.3 Government furnished property and information

The Government will furnish any necessary data within ten (10) days from the time of award and throughout the POP. Anticipated Government Furnished Property (GFP) includes Government laptop computers. Anticipated Government Furnished Information (GFI) includes existing code base repositories, confluence documentation and architecture documents and system security plans.

In accordance with FAR 52.204-9 and agency specific guidance, the contractor must comply with personal identity verification requirements if contractor employees require access to agency controlled facilities or information systems to perform contract requirements.

# 5.0 Terms and conditions

## 5.1 Travel and Other Direct Costs (ODCs)

The Government does not anticipate travel in support of contract performance. Other Direct Costs (other than travel) are permitted and can be added to this task order with written consent of the CO.

## 5.2 Period of performance

The base period of performance (POP) for this order is 12 months from the date of award. There will also be four (4) option periods of 12 months, for a total period of performance of up to five (5) years[[1]](#footnote-1). The POP is expected to begin no later than fourteen (14) days after award.

## 5.3 Place of performance

The place of performance is fully remote at the Contractor’s facilities.

## 5.4 Contract Type

The government intends to award a Time & Materials (T&M) type contract. All rates must be fully burdened and hourly rates are fixed at the time of award.

# 6.0 Invoicing

# 6.1 Procedures for Payment

The selected vendor must submit invoices on a monthly basis and a final invoice at the end of the period of performance within 30 calendar days from contract completion. The procedures for payment are explained below.

# 6.2 Content of Invoice

The vendor will be provided with the following information when the acquisition has been awarded:

● Contract number

● Period of performance covered by the invoice

● Contract Line Item Number (CLIN) and title

● The IX number associated with the task order (if applicable)

● Invoiced amount and overall invoiced amount-to-date

For the labor CLIN, each invoice must list the labor category as awarded on the order, the hours worked per skill level/labor category, the rate per skill level/labor category and the extended amount for that invoice period. It must also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For purposes of this order and specific services, the Government will pay only for productive direct labor hours, which are those hours expended by contractor personnel in performing work under the scope of this contract. This does not include sick leave, vacation leave, holidays, jury duty, military leave, or any other kind of administrative leave.

If personnel have to obtain a background check prior to being able to perform under the terms of the order, the contractor is not permitted to bill until the contractor's personnel are fully able to perform the requirements of the PWS.

All of this information must be included on each invoice in addition to the requirements for a proper invoice specified in FAR 52.212-4 (g), the Prompt Payment clause, FAR 52.212-4(i)(2), Payments under Time and Materials and Labor Hours Contracts, FAR 52.232-7 and Progress Payments, FAR 52.232.16, Alternate I.

# 6.3 Invoice Submission

{Include agency specific instructions}

The contractor is required to submit invoices to the agency system and the COR **concurrently**.

The Contractor may invoice for items or services upon their delivery. Billing and payment must be accomplished in accordance with contract terms and agency payment procedures.

Once invoices are submitted by the Contractor, the government will make payment after verification that the goods or services listed on the invoice have been received and accepted.

# 6.4 Final Invoice

The contractor’s final invoice for this requirement must be identified and submitted after the task order has been completed and no further charges are to be billed. Final invoices must be submitted no later than thirty (30) calendar days after completion of any task orders. The contractor must submit a signed and executed Release of Claims with the final invoice.

# 7.0 Contractor Performance Information

(1) Evaluating Contractor Performance: The government is using the Contractor Performance Assessment Reporting System (CPARS) module as the secure, confidential, information management tool to facilitate the performance evaluation process. CPARS enables a comprehensive evaluation by capturing comments from both the government and the contractor. The website for CPARS is http://www.cpars.gov. Completed CPARS evaluations may then be used by the Federal acquisition community for use in making source selection decisions. CPARS assists acquisition officials by serving as the single source for contractor past performance data.

(2) CPARS Registration: Each award requiring an evaluation must be registered in CPARS. The awardee will receive several automated emails. Within thirty (30) days of award, the contractor will receive an email that contains user account information, as well as the applicable contract and order number(s) assigned. The contractor will be granted one user account to access all evaluations.

(3) Contractor CPARS Training: The contractor may sign up for CPARS training. A schedule of classes will be posted to the CPARS training site

(<https://www.cpars.gov/lc_role.htm>) and updated as needed.

(4) Contractor Representative (CR) Role: All evaluations will be sent to the contractor Representative (CR) named on your award. The CR will be able to access CPARS to review and comment on the evaluation. If your CR is not already in the CPARS system, the CO will request the name and email address of the person that will be responsible for the CR role on your award.

Once an evaluation is ready to be released, the CR will receive an email alerting them the evaluation is ready for their review and comment. The email will indicate the timeframe the CR has to respond to the evaluation; however, the CR may return the evaluation earlier than this date.

The government must provide for review at a level above the CO (i.e., contracting director) to consider any disagreement between the government and the contractor regarding the government’s evaluation of the contractor. Based on the review, the individual at a level above the CO will issue the ultimate conclusion on the performance evaluation. Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file.

# 8.0 Transparency Policy

The contractor is advised that the government reserves the right to publish documents associated with this acquisition on a publicly-available website, including any Requests for Quote or their amendments, as well as question and answer exchanges with the contractor with source-identifying information removed. The government reserves the right to publish any other relevant information that is not confidential or proprietary in nature, but will not publish any source-selection sensitive information that would otherwise implicate procurement integrity concerns.

Upon award of the acquisition, The government may publish the total price of the quote and certain non-source-identifying data. During the performance of task orders, the government may similarly publish data related to project management (e.g. user stories, milestones, and performance metrics) and top-line spending data.

# 8.1 Privacy Act

Performance of this contract may require that personnel have access to Privacy Information. The contractor personnel must adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and any other applicable rules and regulations.

# 8.2 Protection of Information

The contractor must be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this contract. The contractor must also protect all Government data by treating information as sensitive. All information gathered or created under this contract must be considered as controlled unclassified information (CUI). The use of this data is subject to the Privacy Act and must be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

All contractor key personnel, employees, agents, subcontractors and subcontractor personnel who will have access to documents or data during the performance of their duties under the contract must execute a Non-Disclosure Agreement and return it to the CO within five (5) calendar days of award and before being given access to such information or documents.

# 8.3 Organizational Conflicts of Interest

The contractor’s attention is directed to [Federal Acquisition Regulation (FAR) Subpart 9.5](https://www.acquisition.gov/far/part-9#FAR_Subpart_9_5), Organizational and Consultant Conflicts of Interest.

As part of its quote, the vendor must complete **Attachment D** - Organizational Conflict of Interest Statement to confirm that the firm and any subcontractors or teaming partners have no all actual or potential conflicts of interest relating to the work to be performed under this potential contract. As applicable, the contractor must list and describe any and all actual or potential conflicts of interest relating to the work to be performed under this contract. If the contractor believes the conflict can be avoided, neutralized, or mitigated, it must submit a mitigation plan to the Contracting Officer for review.

# 9.0 Data Rights and Ownership of Deliverables

The Government must hold unlimited rights in all deliverables in accordance with the FAR clause at 52.227-14, Rights in Data - General (May 2014).

Additionally, the government intends that any data or deliverable created as a result of the work performed under each task order be publicly accessible without restriction.

# 10.0 Provisions / Clauses

Since this will result in a task order from GSA Schedules, all provisions/clauses will flow from the base schedule contract to the task order. Agencies should include any agency-specific provisions/clauses they deemed necessary and incorporate any full-text provisions/clauses deemed applicable.

  

1. Per FAR 8.404(h)(3)(ii)(C), When the total performance period, including options, is more than three years, and the contract type is either T&M or LH, D&F shall be approved by the Head of the Contracting Activity (HCA). [↑](#footnote-ref-1)