Performance Work Statement (PWS)

Ginnie Mae Technology Operations

07/16/2026

DRAFT

Vision Statement 5

1 General Information 5

1.1 Scope of Work 5

1.2 Background 6

1.3 Constraints 11

1.4 Non-Personal Services 13

1.5 Period of Performance 13

1.6 Place of Performance 13

1.7 Hours of Operation 13

1.8 Special Qualifications 13

1.9 Post Award/Kickoff Conference 14

1.10 Status Meetings 14

1.11 Contractor Travel 14

1.12 Transition In 14

1.13 Transition Out 14

2.1 Definitions 15

3.1 Government Services 18

3.2 Facilities 18

3.3 Equipment 18

3.4 Materials and Information 18

3.5 Quality Assurance (QA) 18

4 Contractor-Furnished Items and Services 18

4.1 Facilities 18

4.5 Contractor Personnel 19

4.6 Identification of Contractor Employees 19

DRAFT

5 Specific Tasks.....19

5.1 Transition-In Services (Initial).....19

5.2 Program Management 23

5.3 Desktop as a Service (DaaS).....29

5.4 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Base Year..32

5.5 DevSecOps CI/CD Pipeline Operations and Support 37

5.6 Identity and Access Management (IAM):.....41

5.7 Infrastructure and Application Integrator (Optional) 43

5.8 Cloud Infrastructure and Application Operations and Maintenance (Optional).....45

5.9 Risk Application Operations Maintenance and Integrator Support (Infrastructure and Applications) (Transition from VMMR Contract) (Optional).....52

5.10 Securities Operations Application Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from MBSOA Contract) (Optional) 64

5.11 Financial Application Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from GFIT Contract) (Optional).....73

5.12 System and Cyber Security Support.....78

5.13 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year One (1) (Optional).....84

5.14 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year TWO (2) (Optional) 89

5.15 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year Three (3) (Optional) 94

5.16 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year Four (4) (Optional) 98

5.17 Transition Out Services.....103

6 Deliverables.....104

6.1 Quality Control Plan 106

6.2 Acceptance Criteria.....106

DRAFT

7 Related Documents 107

8 Performance Requirements Summary 107

DRAFT

Performance Work Statement (PWS)

Technology operations

Vision Statement

To achieve operational excellence through the operation and maintenance of mission critical systems that are secure and improve solutions and support.

The vision is to deliver consolidated, technology operations that empower the organization to achieve its mission and security of IT systems, fostering collaboration, and driving continuous improvement through solutions and support.

1 General Information

1.1 Scope of Work

The Department of Housing and Urban Development (HUD), Government National Mortgage Association (GNMA) has a requirement for IT technology operations and maintenance support services. Services shall include:

- Transition-In
- Project Management (PMP)
- Desktop as a Service (DaaS)
- Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from Digital Service Software Development Contract – Base Year)
- DevSecOps CI/CD Pipeline Operations and Support
- Identity and Access Management (IAM)
- Infrastructure and Application Integrator
- Cloud Infrastructure and Application O&M
- Risk Application Operations Maintenance and Integrator Support (Infrastructure and Applications) (Transition from VMMR Contract)
- Securities Operations, Applications Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from MBSOA Contract)
- Financial Application Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from GFIT Contract)
- System and Cyber Security Support

DRAFT

- Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from Digital Service Software Development Contract – OY1)

- Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from Digital Service Software Development Contract – OY2)

- Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from Digital Service Software Development Contract – OY3)

- Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from Digital Service Software Development Contract – OY4)

- Transition-Out

Detailed descriptions of specific tasks are provided in Section 5 – Specific Tasks.

1.2 Background

Modernization of Ginnie Mae's proprietary systems and securitization platform includes the continuation and implementation of major business applications which are in progress, and other MBS services related to implementing new securitization products and application infrastructure. These major IT initiatives are critical, highly specialized, and necessary to support Ginnie Mae's role in supporting the housing market and economic recovery.

The vital goal of the Technology operations Program is to consolidate all technology, infrastructure and applications operations and maintenance under one effort. Consolidating technology, infrastructure and application operations and maintenance will achieve greater efficiency, reduce costs, improve service quality, strengthen security and compliance, improve consistency and strategic alignment (Simplified IT) in IT service delivery across the organization. This includes:

1. Operational Efficiency
    a. Streamlined Processes: Reduces duplication of effort, eliminates redundant processes, and standardizes workflows.
    b. Centralized Management: Simplifies oversight and coordination, making it easier to manage resources, schedules, and priorities.
2. Cost Savings
    a. Reduces Cost: Consolidates support from across many to one (unified support) to reduce overall costs.
    b. Reduced Administrative Overhead: Minimizes contract management complexity and associated administrative expenses.
3. Improved Service Quality

    a. Consistent Service Levels: Enables the establishment of uniform SLAs, performance metrics, and reporting standards across all environments.
    b. Faster Issue Resolution: Centralized support teams can address incidents and problems more quickly and effectively.
4. Enhanced Security and Compliance
    a. Unified Security Posture: Standardizes security controls, monitoring, and compliance practices across all systems and applications.
    b. Simplified Auditing: Eases the process of compliance reporting and audit preparation by consolidating documentation and processes.
5. Strategic Alignment
    a. Business-IT Alignment: Ensures technology operations are aligned with organizational goals and priorities across all applications and services.
    b. Agility and Innovation: Facilitates the adoption of new technologies and best practices across the enterprise.
6. Resource Optimization
    a. Better Utilization: Allows for more flexible allocation of personnel and technical resources based on organizational needs.
    b. Knowledge Sharing: Promotes cross-training and sharing of expertise among teams.
7. Improved Vendor Management
    a. Single Point of Accountability: Establishes clear ownership and accountability for service delivery.
    b. Simplified Communication: Reduces the complexity of managing multiple vendor relationships.

1.2.1 Technical Environment Background Information:

There are existing conditions within Ginnie Mae's current environment which will have a direct impact on overall acquisition. The Ginnie Mae platform currently supported is a mix of modernized and legacy applications. All legacy applications are currently moving through modernization. This effort will provide a supporting role to those modernization efforts but will not perform application or infrastructure modernization. This effort will assume operations and maintenance of some existing applications and applications that have been developed or modernized under the Ginnie Mae Digital Services (Software Development) effort.

1.2.1.1 Technology Highlights

- Endpoints: 1800 to include 600 servers and 500 workstations
- Security Operations Technologies: Sailpoint, Okta, Centrify, Trellix, Crowd Strike, Palo Alto Prism, Threat Connect, Tenable IO, Splunk Security Information and Event Management (SIEM)/SOAR, DLP, SKYHigh., AWS Security Tools, AWS Shield, Service Now, Datadog, Beyond Trust, Morpheus, RSA, Akamai WAF, Akamai API Security
- GSS is hosted in AWS GovCloud, and all Technology and Security tools have FEDRAMP SaaS Accreditation
- External Cloud integrations with Salesforce, ARRIA, BOX, ServiceNow, Appian, Informatica Cloud, Adobe Cloud, SAS Cloud, Jira Cloud, GIT, Veracode Cloud,

DRAFT

EKS, Oracle EPBCS, Oracle Fusion Middleware, Cloud based data services, NiceOne, Adobe LMS, Arris, Databricks, Mulesoft
- Technology and Application Operations is 24x7x365
- Technology and Application Maintenance/Changes cannot be performed during the first 8 business days unless approved by the CISO, CTA and Business Stakeholder
- 1 production GSS and 1 non-production GSS
- 9 Major Applications and multiple minor applications
- Average of 10-15 major infrastructure projects completed each year.
- Average of 35-45 software development projects supported each year.
- Average of 1500 application changes supported each year.

1.2.1.2 Ginnie Mae Major Applications

Ginnie Mae's current infrastructure technology portfolio consists of 9 key systems (Major Applications) and one General Support System (GSS) and are as follows:

System Name	Brief Description	Operating Environment
RFS – Reporting and Feedback System	Consists of business applications that support the post-settlement collection and processing of monthly pool and loan level investor reporting data, which is used for creation/generation of data disclosures, Ginnie Mae's analytics and internal reporting, and monitoring of Issuers compliance with program requirements. ***System of Systems: Includes 23 Business Applications***	Dev, SIT, UAT, TRN, TST, PROD, DR
WebServices – GinnieMae.gov	Provides comprehensive information on Ginnie Mae's program guidelines, policies, training materials, and critical data disclosures to support the needs of the Investor Community, Issuer Base and other counterparties, and the general public.	Dev, SIT, UAT, PROD, DR
MGM – MyGinnieMae Portal	Provides a secure portal for Issuers and Ginnie Mae Operations staff to access Ginnie Mae's suite of business applications. In addition, it consists of a multiple business applications that support Issuer management, pool issuance and bond administration. ***System of Systems: Includes Portal + 24 Additional Business Applications***	Dev, SIT, UAT, TRN, TST, PROD, DR
GinnieNet	Facilitates the electronic processing and management of HMBS issuance and related transactions. Provides access to Document	Dev, SIT, UAT, PROD, DR

DRAFT

	Custodians to certify or reject MBS submissions.	
GFAS / SLDB – Ginnie Mae Financial Account System	Tracks, records, and reports Ginnie Mae's accounting information to ensure accurate handling of government revenues, fundings, and expenditures. Manages detailed transaction data related to Ginnie Mae's defaulted portfolio, and it supports the preparation of financial statements.	Dev, SIT, UAT, PROD, DR
IPMS – Integrated Pool Management System	Contains the master record of pools issued and ownership as well as the certificate/positions for payment; it facilitates the collection of P&I from Issuers; it records the certification and approval of loan and pool documents to issue new MBS; it performs updates needed to complete pool transfers.	Dev, UAT, PROD, DR
GMC – Ginnie Mae Central	Provides a platform that facilitates the communication and review between their program participants and reviewers to streamline compliance reviews for Insurance, Financials, and Compliance & Monitoring of Issuers.	Dev, UAT, PROD, DR
VMMR / EMAD	Mission critical application for Ginnie Mae's quarterly financial reporting modeling production, annual credit subsidy production, quarterly counterparty risk management surveillance production and bi-annual guaranty fee adequacy and capital adequacy assessment.	Dev, UAT, PROD, DR
ServiceNow	Provides Enterprise IT, Customer, Security, Governance and Risk Service Management and Business Workflow Services.	Dev, UAT, Prod
AWS GSS	Provides the cloud IT infrastructure, network backbone and cyber security resources where all Ginnie Mae systems and applications reside. AWS-GSS is deployed on AWS GovCloud and supports 8 system boundaries.	GSS Production and GSS Non-Production

1.2.1.3 Ginnie Mae IT Environment

Ginnie Mae utilizes several environments as part of the overall systems development and integration process. Not all Major Applications have all listed environments. The environments and associated descriptions are listed below:

DRAFT

Demonstration (DEMO): Contains sample configuration and transaction data. The DEMO environment is leveraged to conduct additional testing for new function functionality. It is also used to apply patches released by PeopleSoft for testing prior to migrating to other environments.

Development (DEV): The development (DEV) environment is used by Vendors and Ginnie Mae to conduct development and integration testing prior to official system testing in SIT and UAT. Code is promoted here from the developer's local machine and tested to ensure correctness. Once code is successfully integrated and tested here, it is considered ready for system testing.

Disaster Recovery (DR): The disaster recovery environment is configured to support Ginnie Mae applications in the event the primary hosting facility is rendered inoperable. The disaster recovery environment will include a dedicated production environment including dedicated servers for each production (PROD) application. Connectivity will be secured through a secure VPN internet connection.

Production (PROD): This is the production environment for Ginnie Mae. Only software that has passed system testing and been fully accepted and baselined by Ginnie Mae can be promoted to production. These are considered the critical servers hosting live data and systems for use by the public and require the highest uptime.

Quality Assurance (QA): The QA environment is for testing upgrade procedure against data, hardware, and software that closely simulate the Production environment and where intended users test the resulting application.

Staging (STG)(PreProd): This environment mirrors the production environment and its purpose is to enable Quality Assurance tests after the DEV environment before moving to the PROD environment.

System Integration Testing (SIT): The SIT testing environment is where pieces of Ginnie Mae application code are uploaded and tested for interoperability with other applications. The code is integrated after normal software testing is conducted and approved.

Test (TST): The Test environment is reserved for testing single pieces of Ginnie Mae application code. Prior to moving the code through SIT and UAT testing, the code must be tested and approved in this environment.

Training (TRN): The Training Environment is designated for educating end users on how to operate Ginnie Mae applications. The Training environments are also paired with QA environments in some instances. These environments are typically closed off from PROD environments and enable users to experiment and learn.

User Acceptance Testing (UAT): The UAT Environment is where Ginnie Mae applications are tested to confirm that the functionality is working properly for end users.

DRAFT

Code will have already passed through the TST and SIT environments to reach this stage of the Software Development Lifecycle.

1.3 Constraints

The services identified in this PWS will adhere to the rules, regulations, laws, standards, and conventions identified by HUD as well as within the Federal Government. Constraints include the following:

1. Federal Information Security Modernization Act of 2014 (FISMA 2014), Public Law No: 113-283 (12/18/2014), S.2521 - 113th Congress (2013-2014): Federal Information Security Modernization Act of 2014 | Congress.gov | Library of Congress
2. Clinger-Cohen Act of 1996 (40 USC 1401) 40 U.S. Code Subtitle III - INFORMATION TECHNOLOGY MANAGEMENT | U.S. Code | US Law | LII / Legal Information Institute
3. Paperwork Reduction Act (44 USC §§3501 -3521) 44 USC CHAPTER 35, SUBCHAPTER I: FEDERAL INFORMATION POLICY
4. Office of Management, and Budget Circular A-I23 https://www.whitehouse.gov/omb/information-for-agencies/circulars/
5. Department of Housing and Urban Development regulations, Chief Information Officer Handbooks and Policies 2400 series, 3150 series, 3200 series, 3300 series, 3400 series and 3500 series. https://www.hud.gov/hudclips/handbooks/cio
6. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
7. National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev.5, *Security and Privacy Controls for Information Systems and Organizations* SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC and all future revisions
8. NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: *A System Live Cycle Approach for Security and Privacy*, SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy | CSRC
9. NIST SP 800-160 Vol. 1 Rev. 1, *Engineering Trustworthy Secure Systems*, SP 800-160 Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems | CSRC and SP 800-160 Vol. 2 Rev. 1, *Developing Technology operations- Resilient Systems: A Systems Security Engineering Approach,* SP 800-160 Vol. 2 Rev. 1, Developing Technology operations-Resilient Systems: A Systems Security Engineering Approach | CSRC.
10. NIST SP 800-30 https://csrc.nist.gov/pubs/sp/800/30/r1/final
11. Ginnie Mae Technology Management Division Policies and Procedures
12. Ginnie Mae Chief Information Security Officer Sub-policies and procedures

13. Executive Orders Executive Orders – The White House and OMB "Memoranda" for Information Technology and Security Memoranda – OMB – The White House and Cybersecurity and Infrastructure Security Agency (CISA) "Binding Operational Directives (BODs)" and "Emergency Directives (Eds)" Cybersecurity Directives | CISA
14. GAO directives - https://www.gao.gov/technology operationssecurity - https://www.gao.gov/fiscam -
15. Federal Managers' Financial Integrity Act of 1982 (31 USC 3512)(Public Law No: 97-255) Text - H.R.1526 - 97th Congress (1981-1982): Federal Managers Financial Integrity Act of 1982 | Congress.gov | Library of Congress
16. E-Government Act of 2002, 44 U.S.C. 3601et seq.)- https://www.federalregister.gov/
17. Homeland security Presidential Directive-12
18. Federal Manual 0-8530.-1M, Federal Computer Network Defense (CND) Service Provider Certification and Accreditation Process https://www.cool.osd.mil/usmc/ia_documents/DoD_8570.01M.pdf
19. FSO Evaluator's Scoring Metrics: Certification and Accreditation of Computer Network Defense Service Providers
20. Federal Directive 8570.1, Information Assurance Training, Certification, and Workforce Management https://www.cool.osd.mil/usmc/ia_documents/DoD_8570.01M.pdf
21. Federal 8570.01M, Federal Information Assurance Workforce Improvement Program https://www.cool.osd.mil/usmc/ia_documents/DoD_8570.01M.pdf
22. Computer Network Defense (CND)
23. Ginnie Mae's Information Assurance Manual
24. Federal Security Technical Implementation Guides (STIGs)

1.3.1 Project Planning and Management

All HUD IT projects, including all information systems acquired, developed, enhanced, or maintained shall follow the policy, procedures, standards, and guidelines set forth within the IT Management Framework using the Project Planning and Management (PPM) Life Cycle located at HUD's PPM Life Cycle Website:

http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/ppm/PPMV20HOME

PPM was designed based on the best practices from Capability Maturity Model Integration (CMMI) for systems development and PMBok for project management. While at its foundation, PPM is designed as a Waterfall methodology, HUD encourages tailoring the PPM to use the many modern solution development methodologies available to enable the planning, development and delivery of usable functionality within 6-to-9-month increments.

Contractors are encouraged to propose a preferred methodology whether their solution(s) are for custom development, including prototypes or pilots, Commercial Off the Shelf (COTS)/ Government Off the Shelf (GOTS) configuration, or Software as a Services. Working with the HUD Project Manager(s), the Contractor shall tailor PPM to

take advantage of Contractor proposed expertise in using other methodologies in a manner that will provide HUD the best value and address all of the work necessary for successful project completion, on time, within budget, and delivering intended functionality.

The decisions of PPM tailoring are captured in the Project Tailoring Agreement (PTA), which documents the specific agreement for creating, combining, referring or omitting specific artifacts applicable to the project, as well as adjusting project control gate reviews to be consistent with the tailoring. All tailoring of PPM must be approved by HUD's Deputy Chief Information Officer (DCIO) for Business & IT Modernization. As a default, any project without an approved project tailoring agreement is required to follow all PPM phases and artifacts as presented.

1.4 Non-Personal Services

The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances shall the Government assign tasks or prepare work schedules for individual Contractor employees. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services.

If the Contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the Contracting Officer (CO) immediately. These services shall not be used to perform the work of a policy, decision making, or management nature, i.e. inherently Government functions. All decisions relative to programs supported by the Contactor shall be the sole responsibility of the Government.

1.5 Period of Performance

The period of performance shall be for one (1) 12-month base period and nine (9) 12-month option periods.

1.6 Place of Performance

The services to be performed under this contract shall be performed at the Contractor's facility.

1.7 Hours of Operation

N/A

1.8 Special Qualifications

The Contractor shall possess and maintain ISO/IEC 20000 and IT Infrastructure Library (ITIL) certifications relevant to IT Service Management (ITSM).

DRAFT

1.9 Post Award/Kickoff Conference

The Contractor shall attend any post award conference convened by the contracting activity or contract administration office in accordance HUD Acquisition Regulation (HUDAR) clause 2452.237-79 - Post Award Conference.

1.10 Status Meetings

The Contracting Officer, Contracting Officer's Representative (COR) and other Government personnel, as appropriate, may meet periodically with the Contractor to also review Contractor performance, requirement status, etc. At these meetings, the Contracting Officer will apprise the Contractor of how the Government views the Contractor's performance or progress of the requirement. The Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government. Post Award Conference and subsequent meetings may be held via teleconference at the Contracting Officer's discretion

1.11 Contractor Travel

N/A

1.12 Transition In

The Contractor shall, upon the Contracting Officer's written notice, furnish Transition-In services as required. As a successor, the Contractor shall have sufficient personnel on board during the **180 calendar days Transition-In period** to ensure a smooth transition with the incumbent Contractor and the Government. The Contractor shall provide an orderly transition of work acceptance and accomplishment such that any impact on the program is minimized. During the Transition-In period, the Contractor shall become familiar with the requirements to commence full performance of services by the end of the contract transition-In period. Transition-in is not required if the successor Contractor is the incumbent Contractor.

1.13 Transition Out

To minimize any decrease in productivity and to prevent possible negative impacts on additional services, the Contractor shall have sufficient personnel on board during the **180 calendar days Transition-Out period**. The incumbent Contractor shall ensure a smooth transition with the successor Contractor during the Transition-Out period, prior to completion of contractual performance. The incumbent Contractor shall aid the successor in the development of plans, procedures, and methods for the assumption of all on going work. The Contractor shall provide an orderly transition of work acceptance and accomplishment, such that full control by the successor Contractor is achieved by the end of the new contract Transition-In period. Definitions and Acronyms

2.1 Definitions

Business Day - Every official day of the week which are days between and including Monday to Friday. This does not include public holidays and weekends.

Contracting Officer (CO*)* - A person with authority to enter into, administer, and/or terminate contracts and make related determinations and findings on behalf of the Government. Note: the only individual who can legally bind the Government.

Contracting Officer's Representative (COR) - An employee of the U.S. Government appointed by the Contracting Officer to perform contract administration activities regarding technical issues. This individual has authority to provide technical direction to the Contractor if direction is within the scope of the contract, does not constitute a change and has no funding implications. This individual does NOT have the authority to change the terms and conditions of the contract.

Contractor - A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

Defective Service - A service output that does not meet the standard of performance as Technology operations associated with the Performance Work Statement.

Deliverable - Anything that can be physically and electronically delivered but may include non-manufactured things such as meeting minutes or reports.

Demonstration (DEMO) - Contains sample configuration and transaction data. The DEMO environment is leveraged to conduct additional testing for new function functionality. It is also used to apply patches released by PeopleSoft for testing prior to migrating to other environments.

Development (DEV) - The development (DEV) environment is used by Vendors and Ginnie Mae to conduct development and integration testing prior to official system testing in SIT and UAT. Code is promoted here from the developer's local machine and tested to ensure correctness. Once code is successfully integrated and tested here, it is considered ready for system testing.

Disaster Recovery (DR) - The disaster recovery environment is configured to support Ginnie Mae applications in the event the primary hosting facility is rendered inoperable. The disaster recovery environment will include a dedicated production environment including dedicated servers for each production (PROD) application. Connectivity will be secured through a secure VPN internet connection.

Government Furnished Property (GFP*)* - Government-furnished property means property in the possession of, or directly acquired by, the Government and subsequently furnished to the Contractor for performance of a contract. Government-furnished property includes spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes Contractor-acquired property

if the Contractor-acquired property is deliverable under a cost contract when accepted by the Government for continued use under the contract.

Performance Standard - The Contractor's performance level required by the Government.

Performance Work Statement (PWS) - A statement of work for performance-based acquisitions that describe the required results in clear, specific, and objective terms with measurable outcomes.

Production (PROD) - This is the production environment for Ginnie Mae. Only software that has passed system testing and been fully accepted and baselined by Ginnie Mae can be promoted to production. These are considered the critical servers hosting live data and systems for use by the public and require the highest uptime.

Quality Assurance (QA) - Policies and procedures adopted by the Government to ensure that supplies and services acquired under Government contracts conform to the contract's quality requirements.

Quality Assurance (QA) - The QA environment is for testing upgrade procedure against data, hardware, and software that closely simulate the Production environment and where intended users test the resulting application.

Quality Assurance Surveillance Plan (QASP) - A plan describing how the agency will survey, observe, test, sample, evaluate and document the Contractor's performance in meeting critical performance standards identified in the contract.

Quality Control (QC) - All measures taken by the Contractor to ensure that the quality of an end product of service shall meet contract requirements.

Staging (STG)(PreProd) - This environment mirrors the production environment and its purpose is to enable Quality Assurance tests after the DEV environment before moving to the PROD environment.

Subcontractor - Any person, other than the prime Contractor, who offers to furnish or furnishes any supplies, material, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with.

System Integration Testing (SIT) - The SIT testing environment is where pieces of Ginnie Mae application code are uploaded and tested for interoperability with other applications. The code is integrated after normal software testing is conducted and approved.

Test (TST) - The Test environment is reserved for testing single pieces of Ginnie Mae application code. Prior to moving the code through SIT and UAT testing, the code must be tested and approved in this environment.

Training (TRN) - The Training Environment is designated for educating end users on how to operate Ginnie Mae applications. The Training environments are also paired with

QA environments in some instances. These environments are typically closed off from PROD environments and enable users to experiment and learn.

User Acceptance Testing (UAT) - The UAT Environment is where Ginnie Mae applications are tested to confirm that the functionality is working properly for end users. Code will have already passed through the TST and SIT environments to reach this stage of the Software Development Lifecycle.

2.2 Acronyms

AQL - Acceptable Quality Level
CND – Computer Network Defense
CIO or OCIO - Office of the Chief Information Officer of HUD
CISA – Technology operations security and Infrastructure Security Agency
CISO – Chief Information Security Officer
CO - Contracting Officer
COR - Contracting Officer's Representative
CTA – Chief Technology Architect
DEMO - Demonstration
DEV - Development
DR - Disaster Recovery
FISMA – Federal Information Security Management Act
GAO - U.S. General Accountability Office
HUD - U.S. Department of Housing and Urban Development
IA – Information Assurance
IAM – Information Assurance Manager
IT - Information Technology
NIST – National Institute of Standards and Technology
OCPO - Office of the Chief Procurement Officer
OIG - Office of Inspector General
OMB - Office of Management and Budget
POAM – Plan of Action and Milestones
PM - Project Manager
POC - Point of Contact
PPM - Project Planning and Management
PROD - Production
QA - Quality Assurance
QASP - Quality Assurance Surveillance Plan
QCP - Quality Control Plan
SIT - System Integration Testing
SA&A – Security Authorization and Accreditation
STG - Staging
STIG - Federal Security Technical Implementation Guides
TBD - To be determined
TRN - Training
TST – Test
UAT - User Acceptance Testing
U.S.C - United States Code

DRAFT

3 Government-Furnished Property and Services

The Contractor shall ensure accurate control and accountability of all Government-Furnished Property (GFP) in accordance with the terms and conditions of this contract. The Government will furnish, at no cost to the Contractor, the GFP shown below.

3.1 Government Services

No Government services will be provided.

3.2 Facilities

The Government will not provide facilities.

3.3 Equipment

The Government will provide HUD or Ginnie Mae issued laptops when required, but all other IT equipment required will be furnished by the Contractor.

3.4 Materials and Information

The Government will provide documentation or access to information via the Government provided document storage location(s). Copies of the required materials may be provided to the Contractor in hard copy or soft copy. Access to all existing technology operations tools, environments, programs, services, software and licenses will be provided by the Government. The Contractor will be given access after completing successful onboarding. All materials will remain the property of the Government and will be returned to the Government through the COR upon request or at the end of the contract period of performance.

3.5 Quality Assurance (QA)

The Government shall evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable quality level.

4 Contractor-Furnished Items and Services

The Contractor shall furnish, all facilities, equipment, and supplies required to perform the work under this contract that are not listed under Government-Furnished Property and Services.

4.1 Facilities

The Contractor shall furnish all facilities.

4.2 Equipment

The Contractor shall furnish all equipment.

4.3 Material

The Contractor shall furnish all materials.

4.4 Contractor Responsibilities

The Contractor shall only conduct business with designated Government personnel listed as points of contact (POCs). Names of authorized personnel shall be provided to the Contractor by the Government, in writing, and updated as necessary throughout the contract period.

U.S. Government records, copies of original results and reports, verified original data, corrected data and corrected supporting final reports which are maintained by the Contractor remain the property of the U.S. Government. These files/results must be surrendered to the COR.

4.5 Contractor Personnel

See HUDAR clause 2452.237-70 - Key Personnel in the Key Personnel section of the contract.

4.6 Identification of Contractor Employees

All Contractor/subcontractor personnel shall wear company picture identification badges to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone, or via electronic mail, Contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, Contractor/subcontractors occupying collocated space with their Government program customer shall identify their workspace area with their name and company affiliation, or at a minimum, "Contractor" after name.

5 Specific Tasks

5.1 Transition-In Services (Initial)

The Contractor shall provide Transition-In support services that shall provide uninterrupted and continuing services of all existing maintenance services. The Contractor shall submit a draft Transition-In Plan five (5) business days after the contract award. The plan shall include:

DRAFT

- A description of all activities necessary to ensure continuity of operations and limits disruption to services and daily operations until operational responsibility is completely assumed.
- A description of the technical approach, organizational resources, resource allocations and management controls to be employed to meet the cost, performance and schedule requirements to transition-in the services required by the Contract.
- The technical approach, planned transition activities, Transition activity timelines and milestones, Transition resource requirements, Transition security requirements, Transition risks and mitigation or avoidance strategies, Transition communication plan
- A Work Breakout Structure (WBS) in Microsoft Project format addressing schedule and work products.
- Knowledge transfer to ensure continuity of technology operations. This includes documenting processes, procedures, and configurations, and providing training for incoming personnel to ensure a smooth transition.

The Contractor shall submit a final Transition-In Plan within fifteen (15) business days of receiving GNMAs comments on the draft plan.

The Contractor shall participate in weekly planning sessions with GNMA and the incumbent Contractor(s) and provide updates during the meeting to its transition plan(s) to address any specific changes because of these discussions. The incumbent Contractor shall transition all required information.

The Contractor shall coordinate with the incumbent Contractor to complete the necessary forms or documentation for the transference of Services, Service Accounts and all maintenance services needed to support the requirements and tasks.

The Contractor shall send an email to the COR within 5 business days after the completion of the transference of each of the services. The email shall include the transference account information, account POC, account number, provider information, period of performance, cost of service, confirmation from provider of the completed transference. The transition period will not exceed 180 days.

The Contractor shall submit a Transition-In Completion Report 10 Business Days after Transition-In is complete via email to the COR. The report shall include the final status of all the transition tasks and activities to include the completion date as annotated in the Transition In Plan and work breakdown structure.

5.1.1 System Review/Fit Gap Analysis

The Contractor shall review application tools, platforms and configurations to determine if setup, configuration and deployments meet Original Equipment Manufacturer (OEM) and technology best practices and deployment guidelines. If not, the Contractor shall identify the need to re-configure/re-design/update deployments to meet best practices and deployment guidelines. The Contractor shall review and determine if gaps exist in

the current application architecture and review and recommend alternative products to fill the identified gaps. If, during the system review and fit/gap analysis, it is determined that an existing application platform or product cannot be configured to meet certain entity-specific mandatory requirements or best practices, the Contractor shall provide a plan to scope, design, develop, test, and implementation of an approved replacement to accommodate the entity-specific mandatory functionality and/or best practices.

The Contractor shall review the following existing technology operations program to include:

- Documenting the Current State
    - Review existing technology operations, processes, tools and services.
    - Collect all relevant documentation (SOPs, runbooks, architecture diagrams, asset inventories).
- Defining Recommended Future State
    - Clarify the organization's desired outcomes, performance metrics, and compliance requirements.
    - Identify any new or changed requirements.
- Capability Assessment.
    - Assess the current's tools, technologies, processes, and operations.
    - Map these capabilities against the organization's current and future requirements.
    - Identify where the current environment fully meets or exceeds the organization's needs.
    - Document best practices or recommended enhancements to the current environment.
- Gap Identification
    - Identify current capabilities, tools or process that do not meet requirements
    - Highlight missing skills, unsupported technologies or process differences
    - Assess the potential impact of each gap on service delivery, continuity and performance
    - Identify the risks associated with each gap, including potential service disruptions or compliance failures
- Remediation Recommendation
    - Develop plans and recommendations to address each identified gap (e.g., training, process, changes, tool acquisition or update/replacement)
    - Provide a recommended schedule / notional timeline to address / close each identified gap.
- Finalize Report
    - Review findings and recommended remediation plans with the Government for validation.
    - Deliver a comprehensive Fit/Gap Analysis Report that summarizes the fits, gaps, impacts, risks and recommended actions.
- Transition Plan
    - Update the Transition Plan to incorporate any fit/gap findings and approved remediation actions into the overall transition plan.

DRAFT

- Track closure/resolution of all gaps as part of the transition milestones and regular status reporting

The fit/gap analysis shall include proof of concept sessions to review the approved solutions against requirements and business processes and identify the fits and gaps. The Contractor shall review the results of the fit/gap analysis to assess the level of effort required to meet the gaps and shall support and generate all activities necessary to conduct the fit/gap analysis for the system, including:

a. Review of functional and other requirements.
b. Identification of potential business process impact areas.
c. Conducting proof of concept sessions and demonstrating the new system capabilities and workflow.
d. Creating fit/gap analysis and comparison reports.
e. Providing specific recommendations and developing the level of effort to configure and enhance (if required through an extension) the system.

The Contractor shall submit a Fit/Gap Analysis Report via email to the COR ten (10) business days after completion of transition-in activities. The report shall include:

a. an executive summary with detailed findings and recommendations.
b. All identified Application, and Services / Products / Deployments and Validation of Configuration as per OEM Best Practices.
c. Requirements review results (identifying the fits and gaps).
d. Products, functions and services impacted by the gap.
e. Functional and technical gaps and how the Contractor recommends the Government can fill the gap.
f. External requirements, including licensing, services, methods to address ensuring / maintaining operations and maintenance of/for the system.
g. Review infrastructure, applications and services configurations to determine if alternative configurations are required.
h. Identify application and services impact. The Contractor shall incorporate into the design and implement a best practice, zero impact approach for all environments.
i. Technology operations roadmap recommendation.
j. Application and Service O&M migration strategy and plan.
k. Inventory Report of all technology operations applications, tools, platforms and configurations that identifies if setup, configuration and deployments meet Original Equipment Manufacturer (OEM) best practices and deployment guidelines.

<u>Performance Standards</u>

a. Standard: Submit a draft Transition-In plan 5 business days after contract award
AQL: Five (5) business day deviation from standard

b. Standard: Submit a final Transition-In plan 15 business days after receiving Government Comments
AQL: Five (5) business day deviation from standard

DRAFT

c. Standard: Send a Transference of Services email within 5 business days after completion of the transference of each service
AQL: Five (5) business day deviation from standard

d. Standard: Submit a Transition-In Completion 10 business days after completion of transition-in activities
AQL: Five (5) business day deviation from standard

e. Standard: Submit a Fit/Gap Analysis Report via email to the COR ten (10) business days after completion of transition-in activities.
AQL: Five (5) business day deviation from standard

Deliverables
A001 Draft Transition-In Plan
A002 Final Transition-In Plan
A003 Transference of Services Emails
A004 Transition-In Completion Report
A005 Fit/Gap Analysis Report

5.2 Program Management

The Contractor shall provide program management support under this effort. This includes management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The Contractor shall identify a Program Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this effort.

The Contractor shall facilitate Government and contractor communications; use the best industry standards and proven methodologies to track and document requirements and activities to allow for continuous monitoring and evaluation by the Government; and ensure all support and requirements performed are accomplished in accordance with the PWS. The Contractor shall notify the Contracting Officer Representative (COR) and Technical Point of Contract (TPOC) of any technical, financial, personnel, and general managerial problems encountered throughout the period of performance (PoP).

All labor hours and work will be documented and accounted for through Service Now ticketing. The Vendor shall ensure all work completed has associated Service Now tickets recording work completed and hours associated with each ticket and assignment.

The Contractor shall recommend the overall communication management structure to provide collaborative, responsive interfacing with the Government and a mechanism to facilitate rapid problem resolution and approval of contractor recommendations by the required authorities. The Contractor shall ensure that Information Technology Infrastructure Library (ITIL) methodologies are incorporated into the Program management structure and guide the overall execution of the requirements.

DRAFT

The Contractor shall develop and submit to the COR a draft Program Management Plan (PMP) 10 business days after the contract Post Award/ Kick-off Conference. At a minimum, the plan shall include the following:

- Description of proposed management approach, timelines, and tools to be used in the execution of the contract services;
- Detailed Standard Operating Procedures (SOPs) for all tasks including milestones, tasks, and subtasks required;
- Overall Work Breakdown Structure (WBS); and
- The PMP must comply with the HUD PPM process and Ginnie Mae's IT governance program.
- A communications plan annotating:
    - Key Stakeholders
    - Primary Client Contact
    - Contact Information
    - Contractor Team Personnel
    - Roles and Responsibilities
    - Contact Information
    - Management Structure
    - Escalation Path for issue Resolution
    - Communications Method
    - Communications Type
    - Meeting Schedule
    - Risk Management Plan annotating:
    - How Risks will be identified, managed and mitigated
    - Key Stakeholders and responsibilities
    - Monitoring and Review Processes

A final PMP shall be submitted to the COR within ten business days of receipt of COR comments.

Performance Standards

a. Standard: Submit to the COR a draft Program Management Plan (PMP) 10 business days after the contract Post Award/ Kick-off Conference
AQL: Five (5) business days deviation from standard

b. Standard: A final PMP that incorporates 100% of the requested information and revisions shall be submitted to the COR within 10 business days of receipt of COR comments
AQL: Five (5) business days deviation from standard

Deliverables

A006 Draft Program Management Plan
A007 Final Program Management Plan

DRAFT

5.2.1 Project Management

The Contractor shall:

1. Oversee the management of Technology O&M under this requirement, system lifecycle management (conception, design, deployment, operations and maintenance).
2. Attend weekly Ginnie Mae project management meetings.
3. Attend weekly Ginnie Mae Change control meetings.
4. Attend weekly Ginnie Mae technology governance meetings.
5. Manage on average 10-15 major infrastructure projects per year.
6. Support on average 35-45 application software development projects per year.
7. Manages all daily assignments and priorities in support of this requirement.
8. Coordinate with all necessary Infrastructure and Applications Teams.
9. Assist in the coordination of all O&M projects performed under this effort. (Upgrades, Changes, Implementations, Deployments, Compliance, Cloud, Enhancements, Changes, Tech Refresh, etc.).
10. Coordinate change management.
11. Maintain a variety of program deliverables (e.g. Risk Register, Action Items, Issues Log, external and internal Program Status Reports, etc.).
12. Coordinating meetings between all stakeholders.
13. Prepare and deliver meeting agenda, notes and minutes.
14. Identify and escalate program issues to COR and Ginnie Mae Program Manager.
15. Work with functional leaders to establish project/initiative objectives, scope and charter that addresses business challenges.
16. Lead multiple O&M projects, lead, coordinate with and guide vendor/customer/partner project managers to accomplish internal project objectives.
17. Identify internal resources and where needed negotiate allocations with functional managers, customers, partners and vendors.
18. Develop a detailed project plans to monitor and track project progress and include in the monthly status reporting.
19. Utilize the Ginnie Mae provided project management platform to track project progress and status reporting.
20. Coordinate with EPMO and ITPMO for Integrated Project Plans.
21. Measure project performance using appropriate tools and techniques.
22. Report and escalate effectively and in a timely manner to technology operations management as needed.
23. Successfully managing the relationship with the internal clients and all stakeholders.
24. Identify internal resources and where needed negotiate allocations with functional managers, internal support partners, customers, and vendors.
25. Weekly Integration Project status meetings with up to 10 individual partners/providers.

DRAFT

5.*2.2* Monthly Status Reporting

The Contractor shall develop and submit to the COR a Monthly Status Report (MSR) via email by the first business day of each month for the prior month. All Monthly Reporting can be rolled up into the MSR. At a minimum, the MSR shall include the following:

- Activities during the report period, by task (include a brief description of each task, on-going activities, new activities, activities completed; and progress to date on all activities); each task shall have its own section
- Problems and corrective actions taken to include any technical, financial, personnel, or problems with performance to include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses, and status (security clearance, etc.)
- Potential risks to tasks
- Government actions required.
- Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Accumulated invoiced cost for each Line Item Number (LIN) up to the previous month.
- Projected cost of each LIN for the current month.
- Contractor risks and issues related to managing the contract.
- Asset Management reports annotating all assets to include cloud services, software, licenses, warranty, support, and services required/supporting this program.
- Monthly monitoring and reporting from management platforms, services, service platforms and other tracking of Ginnie Mae's systems and its environment of operation with respect to costs, services, performance, and utilization of systems
- Service Level matrix reporting to include progress and response times for all incidents and issues responded to and encountered.
- Travel Reporting
- Performance Metrics and KPI Reporting
- Annually include Skills Assessment Reporting
- Monthly and Quarterly Access Audit Reporting
- Monthly Compliance Reporting
- Audit Evidence Analysis and Review shall be included in the October Monthly Report
- Meeting Agenda’s, notes and minutes for all meetings of the prior month
- New and existing project plans

Performance Standards

a. Standard: Submit a Monthly Status Report (MSR) to the COR via email by the first business day of each month for the prior month

AQL: Five (5) business days deviation from standard

Deliverables

A008 Monthly Status Report

5.*2.3* Performance Metrics

The Contractor shall develop, establish and track Key Performance Indicators (KPI's) to measure the effectiveness and efficiency of the technology operations KPI's will demonstrate availability, effectiveness and efficiency as it relates to people, process and technology. The Contractor shall track and report on KPI's to include detection rates, response times, incident resolution times, and compliance with service level agreements (SLA's). Metrics will be reviewed monthly to assess technology operations performance and identify areas of improvement. KPI and SLA reporting will be included in the MSR. SLA's are available in Appendix A.

The Contractor shall:

- Mean Time to Detect (MTTD): Measure the average time taken to detect an incident from the moment it occurs.
- Mean Time to Respond (MTTR): Measure the average time taken to respond to a detected incident.
- Incident Resolution Rate: Track the percentage of incidents that are successfully resolved within a specified time frame.
- False Positive Rate: Measure the percentage of alerts that are incorrectly identified.
- Number of Incidents Detected: Track the total number of operational incidents detected over a specific period. (Monthly)
- Compliance Adherence: Monitor adherence to regulatory requirements and internal policies, including the number of violations and audit findings.
- Participate in regular performance reviews to evaluate technology operations, including incident handling, issue detection, and overall effectiveness.
- Implement processes for continuous improvement based on performance metrics, audit results, and feedback. This includes updating technology operations procedures, technologies, and training programs to enhance overall effectiveness.

Contractor performance measures will include:

- Compliance with approved maintenance windows.
- Completion of preventive maintenance activities.
- Percentage of recurring operational tasks completed on schedule.
- Compliance with approved standard operating procedures.
- Percentage of first-pass success rate for routine operational activities.
- Completion of required monthly health checks.
- Number and Percentage of unauthorized production changes.
- Completion of annual technology and skills assessments for contractor personnel.
- Completion of annual training and personnel improvement plans.

5.2.4 Skills Assessment and Improvement

The Contractor shall assess the skills of the technology, infrastructure and application operations delivery personnel on an annual basis focusing on maintaining and improving the contractor's ability to support the ongoing and evolving technology

DRAFT

environment and operational maturity of the program. The Contractor shall create and submit an individualized improvement plan based on assessment results. The plan shall include:

- **Technical Skills Development**
  - Identify gaps in current technical knowledge related to assigned technologies, platforms, and operational responsibilities.
  - Establish a training plan to address identified deficiencies within defined timeframes.
- **Certification and Professional Development**
  - Maintain required certifications for assigned positions.
  - Identify new certifications or advanced training aligned with emerging technologies, cloud services, cybersecurity, AI, automation, or Service Management.
- **Technology Currency**
  - Complete annual training on new versions of supported operating systems, cloud platforms, enterprise applications, networking technologies, and infrastructure components used by the Government.
  - Demonstrate proficiency with newly implemented technologies before assuming operational responsibility.
- **Cybersecurity Competency**
  - Maintain knowledge of current cybersecurity threats, Federal cybersecurity guidance, Zero Trust principles, vulnerability management, incident response, and secure system administration practices.
  - Complete annual cybersecurity awareness and role-based security training.
- **Operational Excellence**
  - Improve proficiency in ITIL processes including Incident, Problem, Change, Configuration, Asset, Knowledge, and Service Request Management.
  - Develop skills that improve operational efficiency, automation, and service quality.
- **Automation and Process Improvement**
  - Identify opportunities to improve operational processes through scripting, orchestration, AI-assisted operations, or workflow automation.
  - Include measurable objectives for implementing efficiency improvements.
- **Performance Objectives**
  - Establish measurable annual goals tied to individual job responsibilities.
  - Include milestones and expected completion dates for each development objective.
- **Knowledge Transfer**
  - Participate in mentoring, cross-training, and knowledge-sharing activities.
  - Document operational procedures and contribute to the organization's knowledge base.
- **Cross-Functional Training**
  - Develop proficiency in adjacent technology areas to improve operational resiliency and surge support capabilities.

    - Participate in rotational assignments or cross-training exercises where appropriate.
- **Leadership and Communication**
    - Improve written and verbal communication skills.
    - Develop project management, customer engagement, and team leadership competencies appropriate to the individual's role.
- **Performance Review and Progress Tracking**
    - Review progress against the improvement plan at least semi-annually.
    - Update the plan as technologies, requirements, or organizational priorities change.
- **Emerging Technology Readiness**
    - Include training on technologies expected to be adopted during the contract period, such as cloud-native operations, AI-enabled IT operations (AIOps), infrastructure automation, observability platforms, and DevSecOps practices, when applicable.

The Contractor shall:

- Conduct periodic skill assessments to identify strengths and areas for improvement.
- Complete and provide an annual skills assessment report as part of the MSR.
- Skills assessment and improvement reporting will be included in the Monthly MSR and will include any identified gaps and improvement plans.

5.3 Desktop as a Service (DaaS)

The Contractor shall provide operations and maintenance for virtual desktop environments delivered via AWS AppStream 2.0 and AWS Workspaces and/or other associated services.

The Contractor Shall:

5.3.1 Provisioning and Configuration

- Deploy and configure DaaS application environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Active Directory or AWS Directory Service for user authentication and access control.

5.3.2 User Management

- Onboard and offboard users, assigning appropriate desktop resources and permissions.
- Manage user access, entitlements, and group policies.
- Provide support for user profile issues, password resets, and connectivity problems.

5.3.3 Application Management

- Package, update, STIG and maintain applications delivered through AppStream 2.0 and / or Workspaces.

- Ensure application compatibility and performance within the virtual desktop environment.
- Develop, install, configure and maintain tools to support effective DaaS Services.
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new DaaS software requirements
- Conduct performance testing and diagnosis monitoring to validate proper installation and functionality of tools and services quarterly.

5.3.4 Monitoring and Performance Optimization

- Monitor the health, performance, and usage of AWS Workspaces and AppStream 2.0 instances using Datadpg, AWS CloudWatch and other monitoring tools.
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for DaaS
- Configure, maintain and respond to alerts

5.3.5 Security and Compliance

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution, and incident response for all DaaS Services
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or providers and track resolution progress.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Document root cause analysis and implement corrective action
- Maintain all A&A for DaaS

5.3.6 Patch Management and Updates

- Apply operating system and application patches / updates to all virtual desktops and application images.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the DaaS following patching or updates

DRAFT

- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.

5.3.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Maintain Infrastructure as Code (IaC) Scripts for deploying DaaS
- Provide, support and maintain a disaster recovery solution for DaaS
- Test and document recovery procedures to ensure business continuity.

5.3.8 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status. Include performance reporting as part of the Monthly Status Report.
- Create and/or Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.3.9 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.3.10 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS features and updates for potential adoption to enhance the DaaS environment.

<u>Performance Standards</u>

a. Standard: Submit to the COR Standard Operating Procedures, Deployment and Troubleshooting Guides and Training Material 45 business days after the transition of services.
   AQL: Five (5) business days deviation from standard

b. Standard: Submit to the COR Root Cause Analysis Reports withing 2 Business Days of resolution.
   AQL: Two (2) business days deviation from standard

<u>Deliverables</u>

A009 Standard Operating Procedures, Deployment and Troubleshooting Guide
A010 Training Material
A011 Root Cause Analysis Report

DRAFT

5.4 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Base Year

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the Ginnie Mae Digital Services Contract for all applications and services currently in the final stage of O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). Perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae Digital Services (Software Development) Contract to include MuleSoft, DataBricks, WebServices (Drupal), Adobe LMS, Arria, Ginnie Direct (REMIC), Collateral Portfolio Management (Rocktop), and XXXX.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include:
        - Application Monitoring and Availability
        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring

DRAFT

        - Application Security Reporting
        - Application Release Management
    - Maintain and optimize the AWS GovCloud and all SaaS infrastructure
    - Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
    - Implement/maintain robust security measures to protect sensitive data and systems.
    - Provide monitoring, troubleshooting, and continuous improvement of infrastructure operations.
    - Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations

The Contractor Shall:

5.4.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.4.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.4.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.4.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).

DRAFT

- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
  Proactively identify and resolve performance issues or outages

5.4.5 Security, Compliance and Incident Response

- Implement security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Support SOC operations and respond to all incidents, support all investigations for supported systems.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements

DRAFT

- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.4.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.4.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.4.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.4.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.

DRAFT

- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.4.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.4.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status. All performance reports shall be included in the MSR.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.4.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices once per quarter.

5.4.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

<u>Performance Standards</u>

a. Standard: Submit to the COR Backup and Recovery Procedures 45 business days after the transition of services.
   AQL: Five (5) business days deviation from standard

b. Standard: Submit to the COR Flow Diagrams within 5 Business Days of ARB Approval.
   AQL: Five (5) business days deviation from standard

DRAFT

Deliverables
A012 Backup and Recovery Procedures
A013 Flow Diagrams

5.5 DevSecOps CI/CD Pipeline Operations and Support

The contractor shall provide comprehensive DevSecOps support for a GNMA environment hosting multi-cloud integrated applications. The contractor shall ensure secure, and automated development, deployment, and operations processes while enabling seamless integration across multiple cloud platforms (e.g., AWS, Git, ServiceNow, Jira, Azure, Google Cloud Platforms). The focus will be on embedding security into every stage of the software development lifecycle (SDLC) and ensuring compliance with government regulations for all CI/CD pipelines.

The contractor shall:

- Validate the current CI/CD Pipeline, Implement and manage DevSecOps pipelines to automate secure application development, testing, and deployment.
- Ensure the security, reliability, and scalability of applications and infrastructure in AWS GovCloud and other cloud environments.
- Integrate security practices into CI/CD workflows and multi-cloud operations.
- monitor, troubleshoot, and continuous improvement of DevSecOps processes.
- Perform Operations and Maintenance of CI/CD Pipelines
- Support Software Development teams deployment and utilization of the CI/CD Pipelines

5.5.1 CI/CD Pipeline Validation, Implementation and Automation

The Contractor Shall:

- Review existing pipeline, validate, design, implement, and manage secure CI/CD pipelines using: AWS CodePipeline, Angular, Java Spring Boot, Jenkins, Nexus, JFrog, SonarQube, Veracode, Jira, GitLab CI/CD, GitHub, Redhat OpenShift, or Azure DevOps.
- Automate build, test, and deployment processes to ensure rapid and reliable delivery of applications.
- Design and implement CI/CD pipelines and infrastructure-as-code (IaC) templates for infrastructure and application deployment.
- Provide automation scripts and templates for cloud resource provisioning.
- Integrate security tools into pipelines (e.g., static application security testing (SAST), dynamic application security testing (DAST), and software composition analysis (SCA)).

DRAFT

5.5.2 Pipeline Security (CI/CD Pipeline)

The Contractor Shall:

- Embed security checks into CI/CD workflows, including vulnerability scanning, code analysis, and dependency management.
- Integrate security scanning and compliance checks into development workflows.
- Use SonarQube, Veracode, Checkmarx, Snyk, or OWASP ZAP to identify and remediate security issues during development.
- Ensure all CI/CD tools are patched, updated and maintained.
- Provide Vulnerability management and remediation of all pipeline tools.

5.5.3 Artifact Management (CI/CD Pipeline)

The Contractor Shall:

- Manage secure storage and distribution of build artifacts using AWS CodeArtifact, JFrog Artifactory, or Docker Hub.
- Ensure version control and integrity of artifacts.

5.5.4 Infrastructure as Code (IaC) (CI/CD Pipeline)

The Contractor Shall:

- IaC Validation, implementation and support
    - Validate, develop, implement and manage infrastructure as code templates using Terraform Enterprise.
    - Automate provisioning and configuration of AWS GovCloud resources and multi-cloud environments.
- Secure IaC Practices
    - Validate, develop, implement and manage security best practices in IaC templates, including least privilege access, encryption, and secure networking configurations.
    - Use tools like Checkov, Terraform Sentinel, or AWS Config to validate IaC templates for compliance and security.
    - Maintain, update, manage all IaC templates

5.5.5 Security Operations for DevSecOps / CI/CD Pipeline

The Contractor Shall:

- Application and Infrastructure Security:
    - Implement security controls to protect applications and infrastructure, including encryption, firewalls, and secure coding practices.

DRAFT

    - Work with the SOC to ensure monitoring for security threats and responding to incidents using AWS Security Hub, GuardDuty, and CloudTrail.
    - Support SOC operations and respond to all incidents, support all investigations for supported systems.

- Identity and Access Management (IAM):
    - Manage IAM roles, policies, and permissions to enforce least privilege access for DevSecOps workflows.
    - Implement AWS Organizations and Service Control Policies (SCPs) to manage multi-account environments securely.
- Compliance Management:
    - Ensure DevSecOps processes comply with government regulations
    - Conduct regular audits and provide compliance documentation.
- Vulnerability Management:
    - Perform regular vulnerability scans and penetration testing on applications and infrastructure.
    - Use Nessus, Qualys, AWS Inspector or similar tools to identify and remediate vulnerabilities.

5.5.6 Multi-Cloud Integration Support (CI/CD Pipeline)

The Contractor shall:

- Interoperability Design and Implementation:
    - Design and implement solutions to enable seamless integration between AWS GovCloud and other cloud platforms (e.g., Azure, Google Cloud).
    - Use integration tools such as AWS AppFlow, Azure Logic Apps, or Google Cloud Pub/Sub or alternative authorized tools to facilitate data exchange.
- Data Integration and Management:
    - Develop and manage data pipelines to ensure secure and efficient data transfer across cloud environments.
    - Ensure data consistency, integrity, and security during integration.
- API and Service Integration:
    - Integrate and manage APIs to enable communication between applications hosted in AWS GovCloud and across multiple cloud platforms and external service providers.
    - Implement integration solutions for shared services such as identity management, logging, and monitoring.
- Migration Support:
    - Migrate workloads and applications between AWS GovCloud and other cloud environments.
    - Minimize downtime and ensure data integrity during migrations.

DRAFT

5.5.7 Continuous Monitoring and Improvement (CI/CD Pipeline)

The Contractor Shall:

- Proactive Monitoring:
  - Monitor DevSecOps pipelines, applications, and infrastructure using AWS CloudWatch, Prometheus, Datadog or alternative authorized monitoring tools..
  - Detect and resolve issues in real-time to ensure uninterrupted operations.
- Performance Optimization:
  - Analyze DevSecOps workflows and recommend improvements to enhance efficiency and scalability.
  - Implement automation tools to reduce manual effort and improve operational workflows.
- Cost Optimization:
  - Monitor cloud spending and provide recommendations for cost-saving measures, such as reserved instances, savings plans, and eliminating unused resources.
  - Use AWS Cost Explorer and AWS Budgets or other alternative authorized tools to track and manage costs.
- Innovation and Research:
  - Evaluate emerging DevSecOps tools and technologies and recommend solutions to improve operations.
  - Develop proofs of concept (POCs) for new tools and services.
- Training and Knowledge Transfer:
  - Provide training to internal teams on DevSecOps tools, processes, and best practices.
  - Develop documentation and knowledge bases to support ongoing operations.

DRAFT

Performance Standards

a. Standard: Create IaC Templates within 5 business days of the final requirements approval. As Required

   AQL: Five (5) business days deviation from standard

b. Standard: Create Automation Scripts within 5 business days of the final requirements approval. As Required

   AQL: Five (5) business days deviation from standard

Deliverables
A014 IaC Templates
A015 Automation Scripts

5.6 Identity and Access Management (IAM):

The Contractor shall perform Identity and Access Management (IAM) operations using BeyondTrust for Privileged Access Management (PAM), Okta for Multi-Factor Authentication (MFA), and SailPoint for Identity Governance.

5.6.1 Privileged Access Management (Beyond Trust)

- Onboard Privileged Accounts and Assets: Add new privileged accounts and systems to BeyondTrust for centralized management.
- Monitor and Audit Privileged Sessions: Review session logs and recordings for privileged access; investigate anomalies.
- Enforce Password Rotation and Vaulting: Ensure privileged credentials are regularly rotated and securely stored.
- Approve and Track Privileged Access Requests: Manage workflow for privileged access requests, including approvals and documentation.
- Integrate with Okta for MFA: Confirm that all privileged access requires Okta MFA authentication.

5.6.2 Multi-Factor Authentication (Okta)

- Maintain MFA Enrollment: Ensure all users, especially privileged users, are enrolled in Okta MFA.
- Update MFA Policies: Review and update MFA policies to reflect changes in risk or compliance requirements.
- Monitor Authentication Events: Analyze Okta logs for failed MFA attempts or suspicious activity.
- Support User Access Issues: Provide helpdesk support for MFA enrollment, resets, and troubleshooting.

5.6.3 Identity Governance (SailPoint)

- Automate User Provisioning and Deprovisioning: Use SailPoint to provision new users and remove access for terminated users.
- Conduct Access Reviews and Certifications: Schedule and execute periodic access reviews for all users, focusing on privileged accounts.
- Enforce Role-Based Access Controls (RBAC): Maintain and update roles and entitlements to ensure least privilege.
- Generate Compliance Reports: Produce reports on access rights, changes, and review outcomes for audit purposes.
- Integrate with Okta and BeyondTrust: Ensure SailPoint is syncing with Okta and BeyondTrust for unified identity lifecycle management.

5.6.4 Integration and Workflow Management

- Automate Identity Lifecycle Events: Ensure changes in user status (e.g., onboarding, role change, termination) are reflected across SailPoint, Okta, and BeyondTrust.

DRAFT

- Synchronize Access Policies: Regularly review and align access policies across all platforms.
- Incident Response:Respond to alerts from any system (e.g., unauthorized privileged access, failed MFA) and document actions taken.

5.6.5 Operations and Maintenance

- Patch and Update IAM Systems: Apply updates and patches to BeyondTrust, Okta, and SailPoint to maintain security and functionality. Maintain all systems with compliant versions to include operating systems, applications and architecture
- Monitor System Health: Check system dashboards and logs for errors, outages, or performance issues.
- User Support and Training: Provide ongoing training and support for users and administrators on IAM processes and tools.

5.6.6 Compliance and Audit Support

- Maintain Audit Logs: Ensure logs from all systems are retained and accessible for compliance audits.
- Prepare for Audits: Gather evidence of controls, access reviews, and incident responses for internal/external audits.
- Review Regulatory Requirements: Update IAM processes as needed to meet new or changing compliance standards.
- Support SOC operations and respond to all incidents, support all investigations for supported systems.

5.6.7 Continuous Improvement

- Collect Feedback: Solicit feedback from users and stakeholders to identify process improvements.
- Evaluate New Features: Assess new features or integrations from BeyondTrust, Okta, and SailPoint for potential adoption.
- Update Documentation: Maintain up-to-date documentation for IAM workflows, policies, and procedures.

<u>Performance Standards</u>

a. Standard: Submit to the COR Identity Governance Report on the first business day of each month for the prior month

   AQL: Five (5) business days deviation from standard

<u>Deliverables</u>
A016 Identity Governance Compliance Reporting

DRAFT

5.7 Infrastructure and Application Integrator (Optional)

The Contractor shall provide support for the integration of applications and infrastructure deployed in AWS and other cloud environments (e.g., Azure, Google Cloud Platform, Oracle Cloud).

The Contractor Shall:

5.7.1 Cloud Infrastructure Architecture & Design

- Assess current infrastructure and application landscape.
- Design target cloud infrastructure architectures (IaaS, PaaS, SaaS) for scalability, security, and cost optimization
- Develop architecture diagrams, design documentation, and implementation roadmaps.
- Implement solutions to integrate applications and infrastructure across multiple cloud platforms
- Ensure interoperability between cloud environments and seamless data flow.

5.7.2 Application and Infrastructure Migration

- Develop migration strategies and detailed migration plans for infrastructure components and applications.
- Conduct migration readiness assessments and risk analysis.
- Execute migration of workloads, applications, and data to and between cloud environments (e.g., AWS, Azure, GCP).
- Validate successful migration through testing, acceptance criteria, and stakeholder sign-off.
- Minimize downtime and ensure data integrity during migrations.

5.7.3 API and Cloud Integration Services

- Integrate cloud infrastructure and applications and tools with current cloud platforms, services, systems and other cloud platforms.
- Develop and implement APIs, connectors, and automation scripts for interoperability.
- Develop and manage APIs to enable communication between applications and services across multiple clouds.
- Configure identity and access management integrations (e.g., SSO, federation).
- Support the design and implement data pipelines and services to enable secure and efficient data transfer across cloud environments.
- Ensure data consistency and integrity during integration.

5.7.4 Security and Compliance Enablement

DRAFT

- Implement cloud security tools, controls, encryption and configurations in accordance with organizational and regulatory requirements to protect cloud resources in support of SOC operations.
- Coordinate SOC access to all security tools and services
- Work with SOC to monitor for security threats and respond to incidents in support of Security Operations
- Work with SOC to develop and document security architectures, policies, and procedures.
- Work with SOC to conduct security assessments and provide recommendations for remediation.
- Ensure Compliance with relevant security requirements and regulations
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.

5.7.5 Knowledge Transfer and Training

- Develop and deliver training sessions and materials for contract application teams on new cloud architectures, integrations, and tools.
- Conduct knowledge transfer workshops
- Develop documentation and knowledge bases to support ongoing operations.

5.7.6 Continuous Improvement

- Performance Optimization
  - Analyze system performance and recommend improvements to enhance efficiency.
  - Implement automation tools to reduce manual effort and improve scalability.
- Innovation and Research:
  - Evaluate emerging technologies and recommend solutions to improve cloud operations.
  - Develop proofs of concept (POCs) for new tools and services.

<u>Performance Standards</u>

a. Standard: Submit to the COR Infrastructure and Application Architecture Diagrams and Designs within 10 Business Days of the Request.
   AQL: Five (5) business days deviation from standard

b. Standard: Submit to the COR Migration Plans within 10 Business Days of the Request.
   AQL: Five (5) business days deviation from standard

<u>Deliverables:</u>
A017 Infrastructure and Application Diagrams and Designs
A018 Migration Plans

DRAFT

5.8 Cloud Infrastructure and Application Operations and Maintenance (Optional)

The contractor shall perform infrastructure operations and maintenance for the existing cloud environment. The contractor shall ensure the secure, reliable, and efficient operation and maintenance of AWS accounts and associated cloud infrastructure, supporting business continuity, compliance, and optimal resource utilization.

The contractor shall provide operations and maintenance support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the Ginnie Mae Cloud Services (CAMO) Contract for all applications and services currently being supported under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud).

The Contractor shall perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure under the “CAMO” responsibility which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications and infrastructure transitioning from the Ginnie Cloud Services Consolidation (CAMO) Contract to include all AWS Services, Servier Operating and Data Services, Application and Database support, Infrastructure, Network, Cloud, Connectivity, Backup and Recovery, Disaster Recovery and Business Continuity, Maintenance Management, Configuration and Change Management, Patch Management, Monitoring and reporting.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include:
        - Application Monitoring and Availability
        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Networking and Network management
        - Network Operations
        - Helpdesk Operations
        - Cloud Connectivity
        - Applying Code Changes
        - Applying Configuration Changes

        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
    - Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
    - Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
    - Implement/maintain robust security measures to protect sensitive data and systems.
    - Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.
    - Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
    - Ensure Availability and Performance

The Contractor Shall:

5.8.1 AWS Account Administration

- Manage AWS account structures, including Organizations, Organizational Units (OUs), and Service Control Policies (SCPs).
- Provision and deprovision AWS accounts as required.
- Maintain and update account contact information and billing details.
- Provide required access and data to support FinOps Team

5.8.2 Resource Provision and Management

- Provision, configure, and decommission AWS infrastructure resources (e.g., EC2, S3, RDS, VPC, IAM).
- Monitor resource utilization and optimize for cost and performance in support of cloud FinOps.
- Maintain tagging standards for resource tracking and cost allocation.

5.8.3 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.

DRAFT

- Integrate with Identity and Access Management Solution for user authentication and access control.

5.8.4 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.8.5 Network, Application and Data Management

- Maintain applications, infrastructure and data as per established RACI
- Manage, maintain, operate, patch, secure Ginnie Mae TIC infrastructure
- Ensure application, infrastructure and data compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications, infrastructure and data as needed.
- Maintain compliance of all deployed applications, infrastructure and data
- Test, validate, secure and maintain all new requirements
- Manage all physical and virtual connections as required

5.8.5.1 Network Management

- Design and configure Virtual Private Clouds (VPCs), subnets, and routing tables for secure, segmented network architecture. (e.g., production, staging, development).
- Define IP address ranges and CIDR blocks to avoid overlap and support growth.
- Implement network security controls such as security groups, network ACLs, and firewalls. Create and manage security groups and network ACLs to restrict inbound/outbound traffic.
- Configure, monitor and manage firewalls and web application firewalls (WAF) for perimeter and application-layer protection.
- Implement network segmentation and micro-segmentation for sensitive workloads.
- Setup and manage VPNs, Direct Connect, or ExpressRoute for secure hybrid connectivity.
- Configure and maintain site-to-site and client VPNs for remote access.
- Deploy and configure and manage load balancers (e.g., AWS ELB, Azure Load Balancer) for high availability and failover.
- Set up DNS zones and records using Route 53, Akamai DNS, AWS DNS.
- Integrate and manage CDNs for global content delivery and caching.
- Manage all Certificate Services

DRAFT

- Monitor network traffic and performance using cloud-native tools (e.g., AWS VPC Flow Logs, Azure Network Watcher).
- Enable and analyze VPC Flow Logs, Network Watcher, or equivalent for traffic monitoring and troubleshooting.
- Enforce network segmentation and micro-segmentation to limit lateral movement.
- Manage DNS, load balancers, and content delivery networks (CDNs) for optimized access and availability.
- Set up alerts for unusual traffic patterns, latency, or connectivity issues.
- Support regular network penetration testing and vulnerability assessments.
- Regularly review and update network policies to address emerging threats and business needs.
- Regularly review and update network security policies and firewall rules.
- Document network topology, configurations, and changes for audit and compliance.
- Ensure compliance with regulatory requirements (e.g., FISMA, PCI DSS) for network controls.

5.8.5.2 Application Management

- Deploy, configure, and update applications using cloud-native services (e.g., AWS ECS/EKS, Elastic Beanstalk, Azure App Service, GCP App Engine).
- Configure environment variables, secrets, and application settings securely (e.g., AWS Secrets Manager, Azure Key Vault).
- Implement blue/green or canary deployments for zero-downtime releases.
- Monitor application health, performance, and availability with tools like CloudWatch, Datadog, Application Insights.
- Set up health checks, synthetic monitoring, and alerting for application endpoints.
- Analyze logs for errors, exceptions, and performance bottlenecks.
- Implement automated scaling and load balancing to ensure application resilience and performance.
- Configure auto-scaling policies based on CPU, memory, or custom metrics.
- Implement load balancing and failover strategies for high availability.
- Design applications for statelessness and horizontal scaling.
- Manage application secrets, environment variables, and configuration settings securely.
- Apply patches and updates to application components to address vulnerabilities.
- Apply security patches and updates to application runtimes and dependencies.
- Conduct regular vulnerability scans and code reviews.
- Enforce least privilege for application roles and service accounts.
- Integrate CI/CD pipelines for automated application deployment and rollback.
- Maintain application documentation, runbooks, and support procedures.

DRAFT

- Maintain up-to-date runbooks, troubleshooting guides, and architecture diagrams.
- Provide Tier 2/3 support for application incidents and escalations.
- Document application dependencies and integration points.

5.8.5.3 Data Management

- Provision and manage cloud storage solutions (e.g., S3, Blob Storage, Cloud SQL) for structured and unstructured data
- Provision and configure databases (e.g., RDS, Cloud SQL, Cosmos DB), object storage (e.g., S3, Blob Storage), and file storage.
- Set up storage classes and lifecycle policies for cost optimization.
- Implement data backup, replication, and disaster recovery strategies.
- Schedule automated backups and snapshots for databases and storage.
- Test backup restoration procedures regularly to ensure data recoverability.
- Implement cross-region replication for disaster recovery.
- Enforce data encryption at rest and in transit using cloud-native encryption services.
- Configure IAM policies, roles, and access controls for data resources.
- Monitor and audit data access using cloud-native tools (e.g., AWS CloudTrail, Azure Monitor).
- Define and apply data retention, archival, and lifecycle management policies.
- Define and enforce data retention, archival, and deletion policies.
- Classify data according to sensitivity and regulatory requirements (e.g., PII, PHI).
- Ensure compliance with data privacy laws (e.g., FISMA,GDPR) through proper handling and documentation.
- Monitor data access and usage for compliance and security (e.g., audit logs, access controls).
- Monitor database and storage performance metrics; tune queries and indexes as needed.
- Optimize storage costs by moving infrequently accessed data to lower-cost tiers.
- Review and clean up unused or obsolete data resources.
- Regularly review and optimize data storage costs and performance.
- Maintain data flow diagrams, data dictionaries, and access logs.
- Generate regular reports on data usage, access, and compliance status.

5.8.6 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS

DRAFT

- Manage all cloud resources such as EC2 instances, EXS Clusters, S3 buckets, RDS databases, Lambda functions, and Elastic Load Balancers.
- Monitor the performance and availability of AWS GovCloud resources using tools like AWS CloudWatch, AWS Config, Datadog and AWS Trusted Advisor.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.8.7 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as FedRAMP, ITAR, FISCAM, and FISMA.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Implement security controls and policies to meet regulatory requirements.

DRAFT

5.8.8 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.8.9 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.8.10 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.8.11 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

DRAFT

5.8.12 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.8.13 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status. All reporting shall be included in the MSR.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.8.14 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.8.15 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.9 Risk Application Operations Maintenance and Integrator Support (Infrastructure and Applications) (Transition from VMMR Contract) (Optional)

The Contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the VMMR (Risk Modeling Contract) for all applications and services currently in the O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). The Contractor shall perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae Modeling Services Contract (VMMR) to include VM, MR and EMAD.

- O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include:
    - Application Monitoring and Availability
    - Access Requests and User Management
    - Application Upgrades
    - Application Functionality (End User Experience/Customization)
    - Maintenance and Patching
    - DaaS requirements
    - Applying Code Changes
    - Applying Configuration Changes
    - Database Administration
    - Database Maintenance and Patching
    - Database Configuration
    - Database Encryption
    - Data Export and Integrations
    - Database Exports
    - Database User Monitoring
    - Audit/PBC Support
    - Security Scan Remediation
    - Vulnerability Management and Remediation
    - Application SA&A
    - Application Continuous Monitoring
    - Application Security Reporting
    - Application Release Management
- Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
- Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
- Implement/maintain robust security measures to protect sensitive data and systems.
- Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.
- Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
- Ensure Availability and Performance

5.9.1 VM Application Operations

The Contractor Shall:

5.9.1.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

DRAFT

5.9.1.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.9.1.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.9.1.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)

DRAFT

- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.9.1.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA's
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.9.1.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout

DRAFT

- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.9.1.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.9.1.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.9.1.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.9.1.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

DRAFT

5.9.1.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.9.1.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.9.1.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.9.2 MR Application Operations

The Contractor Shall:

5.9.2.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.9.2.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.9.2.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance

DRAFT

- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.9.2.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.9.2.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications

DRAFT

- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA's
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.9.2.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.9.2.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.9.2.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.

DRAFT

- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.9.2.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.9.2.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.9.2.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.9.2.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.9.2.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.

DRAFT

- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.9.3 EMAD Application Operations

The Contractor Shall:

5.9.3.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.9.3.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.9.3.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.9.3.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.

DRAFT

- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.9.3.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

DRAFT

5.9.3.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.9.3.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.9.3.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.9.3.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.

DRAFT

- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.9.3.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.9.11 Reporting and Documentation

- 5.Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.9.3.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.9.3.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.10 Securities Operations Application Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from MBSOA Contract) (Optional)

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the MBSOA Contract for all applications and services currently in the O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). The Contractor shall perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and

DRAFT

Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae MBSOA Contract to include RFS, GMC, MGM, WebServices and all other supporting applications and infrastructure. Transition and provide O&M Services for current applications transitioning from the Ginnie Mae MBSIBA Contract to include MGM, EWODS, IPMS Portable Applications, GinnieNet and all other supporting applications and infrastructure.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include to the following:
        - Application Monitoring and Availability
        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
- Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
- Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
- Implement/maintain robust security measures to protect sensitive data and systems.
- Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.

DRAFT

- Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
- Ensure Availability and Performance

5.10.1 MBSOA Application Operations

The Contractor Shall:

5.10.1.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.10.1.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.10.1.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.10.1.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS

DRAFT

- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.10.1.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.

DRAFT

- Implement security controls and policies to meet regulatory requirements.

5.10.1.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.10.1.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.10.1.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.10.1.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.

DRAFT

- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.10.1.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.10.1.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.10.1.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.10.1.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.10.2 MBSIBA Application Operations

The Contractor Shall:

5.10.2.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.10.2.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.

DRAFT

- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.10.2.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.10.2.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing

DRAFT

- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.10.2.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA's
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.10.2.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

DRAFT

5.10.2.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.10.2.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.10.2.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.10.2.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

DRAFT

5.10.2.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.10.2.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.10.2.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.11 Financial Application Operations, Maintenance and Integrator Support (Infrastructure and Applications) (Transition from GFIT Contract) (Optional)

The Contractor Shall:

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the GFIT Contract for all applications and services currently in the O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). The Contractor shall perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae MBSOA Contract to include GFAS, SLDB, Oracle EPBCS and all other supporting applications and infrastructure.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include to the following:
        - Application Monitoring and Availability

        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
    - Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
    - Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
    - Implement/maintain robust security measures to protect sensitive data and systems.
    - Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.
    - Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
    - Ensure Availability and Performance

5.11.1 GFIT Application Operations

The Contractor Shall:

5.11.1.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.11.1.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.

DRAFT

- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.11.1.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.11.1.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)

DRAFT

- Proactively identify and resolve performance issues or outages

5.11.1.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA's
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.11.1.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.11.1.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements

DRAFT

- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.11.1.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.11.1.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.11.1.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.11.1.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.11.1.12 User Support and Training

DRAFT

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.11.1.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.12 System and Cyber Security Support

5.12.1 RIGHTS TO AUDIT AND RECORDS

This provision requires a contractor or service provider to maintain records relating to its performance of the contract and provide Ginnie Mae with copies of, or access to, those records.

Contractor agrees to retain all records, processes documentation, controls, flowcharts, and accounts related to Agency under this Agreement for a period of at least three (3) years from the completion date of any Work. Such records, processes documentation, controls, flowcharts, and accounts shall itemize the names of employees, hours worked, services performed, materials used, and any other costs or expenses.

The Contractor shall permit Agency or Ginnie Mae Contractor to review all records and accounts related to costs and expenses invoiced to AGENCY which pertain to the non-fixed price transactions under this Contract. The contractor agrees to cooperate with all inspections (i.e. Contract Audit Reviews (CARs), OMB A-123, Appendix A, Operational Risk Assessments (RCSA), Vendor Risk Assessment (VRM), and Continuity of Operations (COOP) activities) and to resolve all findings to Ginnie Mae's satisfaction at no additional cost to the Government. The contractor agrees that the government may deduct any monetary discrepancies from any invoice submitted by the contractor to correct all monetary findings. Agency's signature on timecards or other documents evidencing Work performed or materials purchased shall not preclude Agency from receiving an adjustment to amounts paid to Contractor based on an audit or other review by or on behalf of Agency.

Such records shall include, accounting records, written policies and procedures; flowcharts, subcontract files (including proposals of successful and unsuccessful bidders, bid recaps, etc.); all paid vouchers including those for out-of-pocket expenses; other reimbursement supported by invoices; ledgers; cancelled checks; deposit slips; bank statements; journals; original estimates; estimating work sheets; contract amendments and change order files; back charge logs and supporting documentation; insurance documents; payroll documents; timesheets; memoranda; and correspondence."

The Vendor shall perform an SSAE18 and all future revision Audits through an external auditor provided by the Vendor on all Ginnie Mae environments and provide results of the audit in a report. Audit criteria will be determined by the Ginnie Mae. The Vendor shall be subject to a SSAE audit issued under Statement on Standards for Attestation Engagements (SSAE) Type II Engagement Report on policies and procedures placed in operation and tests of 18 operating effectiveness of controls with AICPA SOC 1 Report (Financial Reporting) for each year of the contract term. An independent public accounting firm shall conduct the SSAE audit report.

The Vendor shall provide the auditor with access to all systems, information and people required to perform a SSAE Type II with an AICPA SOC I review. As part of the audit process, the Vendor shall provide the SSAE auditor with corrective action plans for addressing any findings noted in a SSAE Audit Remediation Report. A draft of the SSAE report will be submitted to Ginnie Mae by August 1st of the year ordered. Each audit including follow up work shall be completed by August 30th of the year ordered. A final SSAE Audit Report shall be completed by May 30th of the year ordered. Ginnie Mae and HUD's Office of Inspector General (OIG) shall have access to all work papers related to the SSAE audit. Additionally, the vendor shall:

1. Work in conjunction with independent auditors to install auditor software to extract metrics.
2. Supply auditors with requested documents and system extracts. Typical requests include: log samples, standard operating procedures, proof of successful backup and recovery, current asset inventory, security documentation, security configuration and settings, security profiles, etc.
3. Ensure Vendor technicians, security and technical leads are available for interviews with audit personnel.
4. Follow up on requests for information made during audit interviews.
5. Assist the Government in drafting responses, including technical rationale, for or against changes proposed by auditors. Complete an Audit Remediation Plan
6. Provide ongoing status of audit remediation activities. Complete an Audit Remediation Report when all findings have been remediated or mitigated.

Performance Standards

a. Standard: Submit to the COR SSAE Audit Request Beginning Option Year 1 and Yearly After on the First day of the Option Period.
   AQL: Five (5) business days deviation from standard

b. Standard: Submit to the COR the Draft SSAE Audit Report NLT May 15.
   AQL: Five (5) business days deviation from standard

c. Standard: Submit to the COR the Final SSAE Audit Report NLT May 25.
   AQL: Five (5) business days deviation from standard.

d. Standard: Submit to the COR the SSAE Audit Remediation Plan NLT June 5.
   AQL: Five (5) business days deviation from standard

DRAFT

e. Standard: Submit to the COR the Final SSAE Audit Remediation Report NLT 5 days after completion of remediation.
   AQL: Five (5) business days deviation from standard.

Deliverables:

A019 SSAE Audit Request
A020 Draft SSAE Audit Report
A021 Final SSAE Audit Report
A022 Draft SSAE Audit Remediation Plan
A023 Final SSAE Audit Remediation Report

5.12.2 IT, RISK and FISMA Audit Support

An IT audit is an in-depth evaluation of an organization's information technology infrastructure, IT systems, controls, policies, and procedures. It's designed to ensure that IT systems are secure and follow all applicable security standards and policies. The overall audit process helps ensure that the organization meets privacy and security compliance measures and can identify potential vulnerabilities before they can be exploited. Due to the nature of Ginnie Mae's business, we have multiple FISMA and Financial System audits on an annual basis. The Contractor shall support the Ginnie Mae IT Audit Team. The contractor shall support 6 independent IT audits per year.

The Contractor Shall:

- Provide evidence as requested to the Audit Support Team.
- Provide ongoing support to the Audit Support Team.
- Remediate any findings and provide proof of remediation.
- Support control demonstrations to external auditors.
- Follow Ginnie Mae Audit Support Policy to include tracking of all findings in ServiceNow.

5.12.3 Security Assessment and Authorization

The contractor shall support Security Assessment and Authorization activities and continuously monitor the compliance of all applications and infrastructure. The Contractor shall develop and maintain A&A documentation and supporting artifacts for the NIST RMF to include FedRAMP Control Matrix, System Security Plan, Control Implementation Matrix, COOP/DR Plan, IS Contingency Plan, Configuration Management Plan, System Impact Analysis, Risk Acceptance Plan, FIPs 199 System Categorizations, EAuth, Business Impact Analysis, Privacy Impact Assessments, Interconnection Security Agreements (ISA), Security Assessment Report, vulnerability reports, and Plan of Action and Milestones (POA&Ms) as they apply in order to achieve and maintain a favorable accreditation decision. Templates will be provided.

The contractor shall:

DRAFT

a. Provide information security guidance and technical assistance for all Assessment and Authorization activities.
b. Coordinate with the Ginnie Mae Security Team in obtaining certification and accreditation of systems, risk assessment and remediation management.
c. Provide SA&A compliance and monitoring.
    a. Create/Update/Maintain SA&A artifacts including System Security Plans, System Categorization, System Boundary Diagrams, Network and Dataflow Diagrams, Risk Assessments, IT/IS Contingency Plans, Configuration Management Plans, Security Testing and Evaluation, Incident Response Plans, etc.
    b. Complete System Categorization: FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems.
    c. Create/Update/Maintain System Boundary Diagram: Detailed graphic layout of the system authorization boundary.
    d. Create/Update/Maintain Network Diagram and Dataflow: A network diagram is a visual representation of network architecture. It maps out the structure of a network with a variety of different symbols and line connections. Data flow diagram (DFD) illustrates how data is processed by a system in terms of inputs and outputs. As its name indicates its focus is on the flow of information, where data comes from, where it goes and how it gets stored.
    e. Create/Update/Maintain Risk Assessment (RA): Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.
    f. Create/Update/Maintain Configuration Management Plan (CMP): a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.
    g. Create/Update/Maintain System Security Plan (SSP): Provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.
    h. Create/Update/Maintain (Information) System Contingency Plan (CP): Provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and

DRAFT

responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

i. Create/Update/Maintain Security Testing and Evaluation (ST&E): Documents the current state of the Major Application or the General Support System in accordance with FIPS 199, NIST SP 800-53 rev. 4, SP 800-37 rev. 1, SP 800-160 and OMB A130, A123, and FFMIA, and all future revisions.

j. Create/Update/Maintain Incident Response Plan (IRP): In accordance with NIST Special Publication 800-61 rev. 2, provide instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats.

d. Work with the SOC to perform security scanning of all layers and remediate or mitigate issues and prepare for independent testing and validation.

e. Remediate and mitigate any open issues.

f. The contractor shall provide documentation relating to all activities being performed related to SA&A.

g. All SA&A Activities will be entered, managed, monitored, reported in the Ginnie Mae GRC platform.

Standards

a. Standard: Submit to the COR the SA&A Documentation as requested.

AQL: Five (5) business days deviation from standard

Deliverables

A024 SA&A Documentation

5.12.4 Disaster Recovery and Business Continuity

The contractor shall support and maintain disaster recovery and business continuity services across all platforms ensuring the organization's cloud infrastructure, applications, and data can withstand, respond to, and recover from disruptive events, minimizing downtime and data loss while maintaining critical business operations. The contractor shall maintain and support Disaster Recovery (DR) and Business Continuity (BC) of all applications and infrastructure.

5.12.4.1 Business Impact Analysis (BIA)

The Contractor Shall:

- Validate existing documentation, Identify and document critical business functions, applications, and data dependencies.
- Assess the potential impact of various disruption scenarios (e.g., cloud outages, cyber incidents, supply chain disruptions, data corruption).
- Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all major systems and data.

DRAFT

5.12.4.2 BC/DR Planning and Documentation

- Validate, update and maintain a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) tailored to the cloud and application environments.
- Document recovery strategies for infrastructure, applications, and data, including failover, fallback, and manual workarounds.
- Establish clear roles, responsibilities, and communication protocols for BC/DR teams.

5.12.4.3 High Availability and Redundancy

- Validate, Architect, maintain cloud infrastructure and applications for high availability (e.g., multi-AZ, multi-region, load balancing).
- Implement redundancy for critical components to eliminate single points of failure.
- Regularly review and update high availability and redundancy configurations.

5.12.4.4 Backup and Recovery Operations

- Validate, update, maintain, implement automated, regular backups for all critical data, configurations, and system states.
- Ensure backups are encrypted, versioned, and stored in geographically diverse locations (e.g., cross-region replication).
- Document and routinely test backup restoration procedures to validate data integrity and recovery readiness.

5.12.4.5 Disaster Recovery Testing and Exercises

- Schedule and conduct regular disaster recovery drills and tabletop exercises.
- Simulate various disaster scenarios (e.g., data loss, service outage, ransomware) to test response and recovery procedures.
- Document test results, lessons learned, and corrective actions.
- Complete Pre-DR testing and failover prior to all formal DR Testing Events.
- Complete Disaster recovery testing semi-annually. If a pass is not received, additional testing will be required until a pass is received.
- Provide a Disaster recovery test plan and hold tabletop exercises to validate the plan.
- Provide a Disaster recovery completion and validation report.

5.12.4.6 Incident Response Integration

- Integrate BC/DR procedures with the organization’s incident response plan.
- Define escalation paths, notification procedures, and decision-making authorities for BC/DR events.
- Maintain up-to-date contact lists for key personnel and stakeholders.

5.12.4.7 Compliance and Audit Support

- Ensure BC/DR plans and activities align with organizational policies and regulatory requirements (e.g., FISMA, FEDRamp, NIST).

DRAFT

- Maintain comprehensive documentation of all BC/DR procedures, tests, and updates.
- Provide evidence of BC/DR readiness for audits and compliance assessments.

5.12.4.8 Continuous Improvement

- Review and update BC/DR strategies in response to changes in business processes, technology, or the threat landscape on an annual basis.
- Solicit feedback from stakeholders and incorporate improvements into BC/DR planning.
- Monitor industry best practices and emerging risks to enhance resilience.

Standards

a. Standard: Submit to the COR the Business Continuity Disaster Recovery Plan 30 days after transition-in is complete.
   AQL: Five (5) business days deviation from standard

b. Standard: Submit to the COR the DR Test Plan 30 days prior to Semi-Annual DR Test.
   AQL: Five (5) business days deviation from standard

c. Standard: Submit to the COR the DR Completion Report 5 days after DR Test completion.
   AQL: Five (5) business days deviation from standard

Deliverables

A025 Business Continuity Disaster Recovery Plan
A026 DR Test Plans
A027 DR Completion Report

5.13 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year One (1) (Optional)

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the Ginnie Mae Digital Services Contract for all applications and services currently in the final stage of O&M under that vehicle. The contractor will ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). The Contractor shall perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure

DRAFT

responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae Digital Services (Software Development) Contract.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include to the following:
        - Application Monitoring and Availability
        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
- Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
- Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
- Implement/maintain robust security measures to protect sensitive data and systems.
- Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.
- Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
- Ensure Availability and Performance

The Contractor Shall:

5.13.1 Provisioning and Configuration

DRAFT

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.13.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.13.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.13.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.

DRAFT

- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.13.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA's
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.13.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates

DRAFT

- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.13.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.13.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.13.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.13.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).

DRAFT

- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.13.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.13.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.13.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.14 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year TWO (2) (Optional)

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the Ginnie Mae Digital Services Contract for all applications and services currently in the final stage of O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). Perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae Digital Services (Software Development) Contract.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include to the following:
        - Application Monitoring and Availability

        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
    - Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
    - Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
    - Implement/maintain robust security measures to protect sensitive data and systems.
    - Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.
    - Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
    - Ensure Availability and Performance

The Contractor shall:

5.14.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.14.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms

DRAFT

- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.14.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.14.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.14.5 Security, Compliance and Incident Response

DRAFT

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA's
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.14.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.14.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline

DRAFT

- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.14.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.14.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.14.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.14.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.14.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.

DRAFT

- Develop and deliver user training materials and sessions for onboarding and best practices.

5.14.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.15 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year Three (3) (Optional)

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the Ginnie Mae Digital Services Contract for all applications and services currently in the final stage of O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). Perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae Digital Services (Software Development) Contract.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include to the following:
        - Application Monitoring and Availability
        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports

        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
    - Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
    - Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
    - Implement/maintain robust security measures to protect sensitive data and systems.
    - Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.
    - Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
    - Ensure Availability and Performance

The Contractor Shall:

5.15.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.15.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.15.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

DRAFT

5.15.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.
- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.15.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or SaaS providers and track resolution progress.

DRAFT

- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.15.6 Patch Management and Updates

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.15.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.15.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.15.9 Cost Management and Optimization

DRAFT

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

5.15.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.15.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.15.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.15.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.16 Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Option Year Four (4) (Optional)

The contractor shall provide comprehensive support for infrastructure and application operations in an AWS GovCloud environment that hosts multi-cloud integrated applications. The contractor shall transition operations and maintenance of applications and services developed and implemented under the Ginnie Mae Digital Services

DRAFT

Contract for all applications and services currently in the final stage of O&M under that vehicle. The contractor shall ensure the reliability, security, and performance of the infrastructure while transitioning and enabling seamless integration with other cloud platforms (e.g., Azure, Google Cloud Platform, Oracle Cloud). Perform all operations and maintenance as annotated in the Infrastructure and Application RACI for Identified Applications and Infrastructure which includes the breakdown of SaaS provider responsibilities and application/infrastructure responsibilities. Operations and Maintenance may differ pending the services provided as part of a SaaS solution.

The contractor shall:

- Transition and provide O&M Services for current applications transitioning from the Ginnie Mae Digital Services (Software Development) Contract.
    - O&M Services include the following for both Production (Production and DR) and Non-Production (DEV,SIT,UAT,PreProd) Environments to include to the following:
        - Application Monitoring and Availability
        - Access Requests and User Management
        - Application Upgrades
        - Application Functionality (End User Experience/Customization)
        - Maintenance and Patching
        - DaaS requirements
        - Applying Code Changes
        - Applying Configuration Changes
        - Database Administration
        - Database Maintenance and Patching
        - Database Configuration
        - Database Encryption
        - Data Export and Integrations
        - Database Exports
        - Database User Monitoring
        - Audit/PBC Support
        - Security Scan Remediation
        - Vulnerability Management and Remediation
        - Application SA&A
        - Application Continuous Monitoring
        - Application Security Reporting
        - Application Release Management
- Maintain and optimize the AWS GovCloud and all SaaS infrastructure to ensure high availability and compliance with government regulations.
- Support multi-cloud integration efforts to enable interoperability and data flow between AWS GovCloud and other cloud environments.
- Implement/maintain robust security measures to protect sensitive data and systems.
- Provide proactive monitoring, troubleshooting, and continuous improvement of infrastructure operations.

DRAFT

- Support FinOps ensuring reduction in costs, remediation for performance and applying approved recommendations
- Ensure Availability and Performance

The Contractor Shall:

5.16.1 Provisioning and Configuration

- Deploy and configure SaaS applications and associated data infrastructure environments according to user and organizational requirements.
- Set up user profiles, application stacks, and network settings.
- Integrate with Identity and Access Management Solution for user authentication and access control.

5.16.2 User Management

- Onboard and offboard users, assigning appropriate resources and permissions.
- Provision and deprovision user accounts in the application, IAM and integrated SaaS platforms
- Manage user access, roles, permissions, entitlements, and group policies to enforce least privilege and separation of duties
- Integrate with Identity providers (e.g. OKTA, SailPoint, BeyondTrust).
- Audit Access logs and review for unauthorized or suspicious activity. Report any suspicious activity to the Security Operations Center
- Provide support for user profile issues, password resets, and connectivity problems.

5.16.3 Application Management

- Maintain applications as per established RACI
- Ensure application compatibility and performance
- Coordinate with stakeholders to deploy new or updated applications as needed.
- Maintain compliance of all deployed applications
- Test, validate, secure and maintain all new SaaS software requirements

5.16.4 Monitoring and Performance Optimization

- Monitor the application health, availability, performance, and usage using built in dashboards and third party tools (Datadog, Cloudwatch and other monitoring tools).
- Analyze usage patterns and optimize resource allocation to control costs and improve user experience.
- Proactively identify and resolve performance bottlenecks or outages.
- Monitor and ensure availability
- Maintain monitoring solution and dashboards for SaaS
- Manage all cloud resources such as **EC2 instances**, **EXS Clusters**, **S3 buckets**, **RDS databases**, **Lambda functions**, and **Elastic Load Balancers**.

DRAFT

- Monitor the performance and availability of AWS GovCloud resources using tools like **AWS CloudWatch**, **AWS Config**, **Datadog** and **AWS Trusted Advisor**.
- Perform routine maintenance, including patching, updates, and backups, to ensure system reliability.
- Identify and resolve performance bottlenecks and infrastructure issues.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Setup, configure, maintain and respond to alerts (CPU, Memory, latency, error rates, job run, job completion, etc.)
- Anaylze logs for AWS, SaaS, application and audit trails.
- Track usage metrics and analyze trends to optimize application performance and licensing
- Conduct regular performance reviews and optimize resources (e.g., EC2 instance types, auto-scaling policies)
- Proactively identify and resolve performance issues or outages

5.16.5 Security, Compliance and Incident Response

- Implement and enforce security best practices, including access control, encryption, logging, multi-factor authentication, and least privilege access.
- Monitor for security events using AWS Security Hub, GuardDuty, DataDog and other SaaS security dashboards.
- Regularly review and update security groups, IAM roles, and network configurations.
- Ensure compliance with organizational and regulatory requirements for data protection and user privacy.
- Provide vulnerability management, mitigation, remediation, resolution for all SaaS Services and applications
- Log capture to support Security and Operational Needs
- Respond to and resolve incidents, service requests, and user-reported issues in accordance with established SLA’s
- Escalate issues to application support teams or SaaS providers and track resolution progress.
- Document root cause analysis and implement corrective action
- Maintain Audit Logs
- Maintain all A&A requirements
- Ensure compliance with government regulations such as **FedRAMP**, **ITAR**, **FISCAM**, and **FISMA**.
- Support SOC operations and respond to all incidents, support any and all investigations for supported systems.
- Conduct regular audits and provide documentation to demonstrate compliance.
- Implement security controls and policies to meet regulatory requirements.

5.16.6 Patch Management and Updates

DRAFT

- Apply operating system and application patches / updates to all applications and AWS resources and SaaS connectors.
- Coordinate with SaaS vendors and/or providers to schedule and communicate application updates and maintenance windows
- Provide, support and maintain automated testing of the applications following patching or updates
- Schedule and communicate maintenance windows to minimize user disruption.
- Test and validate new features or patches in non-production environments before production rollout
- Test and validate all production rollouts.
- Communicate changes to all stakeholders and users

5.16.7 Backup and Recovery

- Implement backup strategies for user data and application configurations.
- Ensure SaaS data backup polices are in place and meet business requirements
- Maintain Infrastructure as Code (IaC) Scripts for deploying applications
- Maintain Application CI/CD pipeline
- Provide, support and maintain a disaster recovery solution for the Application
- Test and document recovery procedures and backup plans to ensure business continuity.

5.16.8 Integration Management

- Maintain and monitor integrations between AWS services (e.g., Lambda, SQS, SNS, API Gateway) and SaaS solutions (e.g., Salesforce, ServiceNow).
- Update and test integration connectors or APIs as needed.
- Configure and manage **Virtual Private Clouds (VPCs)**, subnets, security groups, and network access control lists (ACLs).
- Ensure secure and reliable connectivity between AWS GovCloud and other cloud environments using **VPNs**, **Direct Connect**, or **Transit Gateways**.
- Handle integration failures (e.g., retries, error handling, notification).
- Document integration flows and dependencies.

5.16.9 Cost Management and Optimization

- Coordinate reporting with the Cloud FinOps Office to Monitor AWS and/or SaaS usage and costs.
- Coordinate Optimization and resource allocation adjustment recommendations with the Cloud FinOps Office (e.g., right-sizing, reserved instances, auto-scaling).
- Review SaaS FinOps cost reporting for licensing and usage to avoid over-provisioning.
- Optimize resource utilization through rightsizing, auto-scaling, and cost-saving measures as identified by the FinOps (e.g., reserved instances, savings plans).
- Implement approved recommendations for savings.

DRAFT

5.16.10 Change and Release Management

- Manage change requests for application features, integrations, and infrastructure.
- Coordinate releases using CI/CD pipelines (e.g., AWS CodePipeline, Jenkins).
- Communicate release schedules and changes to stakeholders.
- Maintain rollback procedures for failed deployments.
- Maintain CI/CD pipelines

5.16.11 Reporting and Documentation

- Generate regular reports on usage, performance, incidents, and compliance status.
- Maintain up-to-date documentation for standard operational procedures, image creation and configurations, deployment and troubleshooting guides.

5.16.12 User Support and Training

- Provide Tier 1 and Tier 2 support for end-users, resolving incidents and service requests.
- Develop and deliver user training materials and sessions for onboarding and best practices.

5.16.13 Continuous Improvement

- Collect user feedback and monitor service metrics to identify areas for improvement.
- Evaluate new AWS and SaaS capabilities, features and updates for potential adoption to enhance the Application environment.

5.17 Transition Out Services

The Contractor shall submit a draft Transition-Out Plan 180 calendar after contract award updated annually via email to the COR. This plan shall facilitate accomplishing a seamless transition from the incumbent to incoming Contractor/Government personnel at the expiration of the contract.

The Contractor shall submit a final Transition-Out Plan via email to the COR and implement the final plan 180 days prior to contract expiration.

The Contractor shall address the following in the Transition-Out Plan:

- Identify how it shall coordinate with the incoming Contractor and/or Government personnel to transfer knowledge
- Program management processes
- Communications Plan
- Points of contact for all providers (services and maintenance agreements)
- Location of technical and program management documentation
- Status of ongoing initiatives and services

DRAFT

- Appropriate contractor-to-contractor coordination to ensure a seamless transition
- Transition of Key Personnel knowledge
- Schedules and milestones
- Actions required by the Government
- Knowledge transfer requirements

Establish and maintain communication with the incoming Contractor/Government personnel for the period of the transition via weekly status meetings.

Performance Standards

a. Standard: Submit a draft Transition-Out Plan six (6) months after contract award updated annually
AQL: Five (5) business days deviation from standard

b. Standard: Submit a final Transition-Out Plan via email to the COR and implement the final plan 180 days prior to contract expiration
AQL: Five (5) business days deviation from standard

Deliverables
A028 Draft Transition-Out Plan
A029 Final Transition-Out Plan

6 Deliverables

The Contractor shall complete all work and submit all deliverables as specified herein. The Government reserves the right to make changes to delivery dates.

Number	Name	Frequency	Quantity
A001	Draft Transition In Plan	Once	1
A002	Final Transition In Plan	Once	1
A003	Transference of Services Emails	Once	1
A004	Transition In Completion Report	Once	1
A005	Fit/Gap Analysis Report	Once	1
A006	Draft Program Management Plan	Once	1
A007	Final Program Management Plan	Once	1

DRAFT

A008	Monthly Status Report	Monthly	1
A009	Standard Operating Procedures, Deployment and Troubleshooting Guides	TBD	1
A010	Training Materials	TBD	1
A011	Root Cause Analysis	TBD	1
A012	Backup and Recovery Procedures	TBD	1
A013	Flow Diagrams	TBD	1
A014	IaC Templates	TBD	1
A015	Automation Scripts	TBD	1
A016	Identity Governance and Compliance Reporting	Monthly	1
A017	Infrastructure and Application Diagrams and Designs	TBD	1
A018	Migration Plans	TBD	1
A019	SSAE Audit Request	Annually	1
A020	Draft SSAE Report	Annually	1
A021	Final SSAE Report	Annually	1
A022	SSAE Remediation Plam	Annually	1
A023	SSAE Final Remediation Report	Annually	1
A024	SA&A Documentation	TBD	1
A025	BC/DR Plan	Once	1
A026	DR Test Plan	Bi-annual	1
A027	DR Completion Report	Bi-annual	1

DRAFT

A028	Draft Transition Out Plan	Once, updated annually	1
A029	Final Transition Out Plan	Once	1
A030	Quality Control Plan	Once	1

6.1 Quality Control Plan

The Contractor shall establish and maintain a complete quality control program that shall ensure services are performed in accordance with this contract. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-reoccurrence of defective services. The Contractor's quality control program is the means by which they assure themselves that their work complies with the requirements of the contract. The Contractor shall provide the associated Quality Control Plan to the Government as directed.

The Contractor shall develop, maintain, enforce, and document a Quality Control Plan (QCP). The QCP shall ensure the Government receives a level of quality that is consistent with the requirements specified in this contract. The QCP shall be sufficiently detailed to provide the Contractor's methodology for identifying and recruiting qualified personnel. The QCP shall also provide the Contractor's methodology for resolving problems identified by the Government during reviews conducted in accordance with its Quality Assurance Surveillance Plan (QASP).

The QCP shall also provide the Contractor's methodology for establishing an internal feedback system for support personnel and for resolving problems identified by that feedback system.

The QCP shall demonstrate and validate that the services or deliverables to be provided under the contract are completed with a level of quality that meets the minimum performance threshold established in the Government's QASP. The QCP shall address Quality Management Approach, Quality Assurance, Quality Control, and Quality Standards.

The Contractor's QCP shall be delivered to the COR within 30 days after contract award (or with the Contractor's proposal if it is an evaluation factor). The QCP shall be submitted to the COR within 10 business days when changes are made thereafter.

6.2 Acceptance Criteria

Each contract deliverable shall meet the following inspection and acceptance criteria in addition to any "*Inspection and Acceptance*" contract terms and conditions:

All deliverables shall be submitted in a draft format agreed upon by the Contractor and the Government. Upon review and acceptance by the Government, the Contractor shall address all Government comments and submit a final draft within five (5) business days

of Government notification. All deliverables shall be emailed to the COR as per the annotated schedule in the Microsoft Office Format and uploaded to the Government Provided BOX platform.

7 Related Documents

The Contractor shall abide by all applicable regulations, publications, manuals, policies, and procedures in the performance of this contract.

8 Performance Requirements Summary

The summary chart below lists the contract's primary requirements, the associated performance standards, the expected target performance, and the methods of surveillance. While some contract requirements may not be listed in the chart below, requirements not appearing on the PRS chart do not negate the Contractor's obligation to perform all requirements as specified in the contract. Additionally, HUD reserves all rights and remedies under the provisions and clauses of the contract when performance of any contract requirement, whether or not listed below, is unacceptable.

HUD will develop a Quality Assurance Surveillance Plan to be used to provide contract oversight. In conjunction with the Contractor's Quality Control Plan and various other methods of assessing performance, the COR and PM may perform on-site reviews and/or other types of verification to determine that the specified target performance requirements have been met. Regular review of Contractor performance is critical to the overall success of the contract. On a monthly basis, the COR will evaluate the quality of the product or services.

Statements	**Standards/AQLs**	**Incentive/Remedy**
5.1 Transition-In Services	a. Standard: Submit a draft transition plan 5 business days after contract award AQL: Five (5) business day deviation from standard b. Standard: Submit a final transition plan 15 business days after receiving Government Comments AQL: Five (5) business day deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.

DRAFT

		c. Standard: Send a Transference of Services email within 5 business days after completion of the transference of each service AQL: Five (5) business day deviation from standard d. Standard: Submit a Transition-In Completion 10 business days after completion of transition-in activities AQL: Five (5) business day deviation from standard e. Standard: Submit a Submit a Fit/Gap Analysis Report 10 business days after completion of transition-in activities AQL: Five (5) business day deviation from standard	
5.2.2	**Program Management**	a. Standard: Submit to the COR a draft Program Management Plan (PMP) 10 business days after the contract Post Award/ Kick-off Conference AQL: Five (5) business days deviation from standard b. Standard: A final PMP shall be submitted to the COR within 10 business days of receipt of COR comments. AQL: Five (5) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.
5.2.3	**Monthly Status Reporting**	a. Standard: Submit a Monthly Status Report (MSR) to the COR via email by the first	%5 deduction from the associated CLIN for each business day not submitted in

DRAFT

		business day of each month for the prior month. AQL: Five (5) business days deviation from standard.	accordance with the established performance standard.
5.3	**DaaS**	a. Standard: Submit to the COR Standard Operating Procedures, Deployment and Troubleshooting Guides and Training Material 45 business days after the transition of services. AQL: Five (5) business days deviation from standard b. Standard: Submit to the COR Root Cause Analysis Reports withing 2 Business Days of resolution. AQL: Two (2) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.
5.4	**Technology Operations, Maintenance and Integrator Support (Infrastructure and Applications) Transition from Digital Service Software Development Contract Base Year**	Standard: Submit to the COR Backup and Recovery Procedures 45 business days after the transition of services. AQL: Five (5) business days deviation from standard Standard: Submit to the COR Flow Diagrams within 5 Business Days of ARB Approval. AQL: Five (5) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.

DRAFT

5.5	**DevSecOpd CI/CD Pipeline Operations and Support**	a. Standard: Create IaC Templates within 5 business days of the final requirements approval. As Required AQL: Five (5) business days deviation from standard b. Standard: Create Automation Scripts within 5 business days of the final requirements approval. As Required AQL: Five (5) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.
5.6	**Identity and Access Management (IAM)**	a. Standard: Submit to the COR Identity Governance Report on the first business day of each month for the prior month AQL: Five (5) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.
5.7	**Infrastructure and Application Integrator**	a. Standard: Submit to the COR Infrastructure and Application Architecture Diagrams and Designs within 10 Business Days of the Request. AQL: Five (5) business days deviation from standard b. Standard: Submit to the COR Migration Plans within 10 Business Days of the Request. AQL: Five (5) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.
5.12.1	**Right to Audit and Records**	a. Standard: Submit to the COR SSAE Audit Request Beginning Option Year 1 and Yearly After on the First day of the Option Period.	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established

DRAFT

	AQL: Five (5) business days deviation from standard b. Standard: Submit to the COR the Draft SSAE Audit Report NLT May 15. AQL: Five (5) business days deviation from standard c. Standard: Submit to the COR the Final SSAE Audit Report NLT May 25. AQL: Five (5) business days deviation from standard. d. Standard: Submit to the COR the SSAE Audit Remediation Plan NLT June 5. AQL: Five (5) business days deviation from standard e. Standard: Submit to the COR the Final SSAE Audit Remediation Report NLT 5 days after completion of remediation. AQL: Five (5) business days deviation from standard.	performance standard.
5.12.3 SA&A	a. Standard: Submit to the COR the SA&A Documentation as requested. AQL: Five (5) business days deviation from standard	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.
5.12.4 BC/DR	a. Standard: Submit to the COR the Business Continuity Disaster Recovery Plan 30 days after transition-in is complete.	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established

DRAFT

		AQL: Five (5) business days deviation from standard b. Standard: Submit to the COR the DR Test Plan 30 days prior to Semi-Annual DR Test. AQL: Five (5) business days deviation from standard c. Standard: Submit to the COR the DR Completion Report 5 days after DR Test completion. AQL: Five (5) business days deviation from standard	performance standard.
5.17	**Transition-Out Services**	a. Standard: Submit a draft Transition-Out Plan six (6) months after contract award updated annually. AQL: Five (5) business days deviation from standard. b. Standard: Submit a final Transition-Out Plan via email to the COR and implement the final plan 90 days prior to contract expiration. AQL: Five (5) business days deviation from standard.	%5 deduction from the associated CLIN for each business day not submitted in accordance with the established performance standard.

DRAFT