CLASS JUSTIFICATION AND APPROVAL FOR OTHER THAN FULL AND OPEN COMPETITION – APPLICATION FOR BRAND NAME DESCRIPTIONS 41 U.S.C. 3304(a)(1)

Justification and Approval No. FY26–0030

Pursuant to the requirements of the Competition in Contracting Act (CICA) as implemented by the Federal Acquisition Regulation (FAR), this Justification and Approval is prepared in accordance with FAR Subpart 6.103 FAR Class Deviation 25-11 for FAR Part 6[1], and in accordance with the requirements of RFO FAR 6.104, the justification for the use of the statutory authority under RFO FAR Subpart 6.103 is justified by the following facts and rationale required under RFO FAR 6.104-1 as follows:

1 Agency and Contracting Activity

The Department of Homeland Security (DHS), Office of Procurement Operations (OPO), in support of DHS, Office of the Chief Information Officer (OCIO) proposes to enter into multiple contracts on a basis other than full and open competition.

2 Nature and/or Description of the Action being Approved

DHS intends to procure, through procedures as established within FAR 12, FAR Class Deviation 25-21 for FAR Part 12[2], and FAR 15, FAR Class Deviation 26-08 for FAR Part 15[3], enterprise-wide, commercially available Cloud Service Provider (CSP) Anything as a Service (XaaS) services, professional services, marketplace solutions, and training services. XaaS refers to the vast number of products, tools, technologies delivered to users as a service over the internet such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). It also allows for the flexibility to include new and emerging service models such as Functions as a Service (FaaS), Database as a Service (DBaaS), or Container as a Service (CaaS). Similar commercial CSP services have been previously procured independently at DHS Components. However, referenced commercial CSP services

[1] FAR Class Deviation 25-11 for FAR Part 6 was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, Restoring Common Sense to Federal Procurement, signed April 15, 2025. Any subsequent citations to FAR Part 6 in this document will be cited as "RFO FAR" for brevity and are referring specifically to FAR Class Deviation 25-11 for FAR Part 6.

[2] FAR Class Deviation 25-21 for FAR Part 12 was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, Restoring Common Sense to Federal Procurement, signed April 15, 2025. Any subsequent citations to FAR Part 12 in this document will be cited as "RFO FAR" for brevity, and are referring specifically to FAR Class Deviation 25-21 for FAR Part 12

[3] FAR Class Deviation 26-08 for FAR Part 15 was issued as part of the Revolutionary FAR Overhaul (RFO), which was implemented in response to Executive Order 14275, Restoring Common Sense to Federal Procurement, signed April 15, 2025. Any subsequent citations to FAR Part 15 in this document will be cited as "RFO FAR" for brevity, and are referring specifically to FAR Class Deviation 26-08 for FAR Part 15

have not been previously procured on an enterprise (Department-wide) level, covering the entirety of the anticipated scope for all of DHS, as further detailed within section 3. below. DHS has titled this project Cumulus, as further reflected throughout this justification document.

In support of Cumulus, commercial CSP services shall be provided through multiple, single-award indefinite-delivery, indefinite-quantity (IDIQ) vehicles available for Department-wide use. Multiple, single-award IDIQ vehicles shall be directly established with several different CSPs, as represented within Table 1 immediately below, Brand Name Cloud Service Providers (CSPs).

Table 1. Brand Name Cloud Service Providers (CSPs)

Amazon Web Services (AWS)
Google Cloud (GC)
Microsoft Azure (MS)
Oracle Cloud Infrastructure (OCI)

Brand name CSP contracts under multiple, single-award IDIQ vehicles shall be made in accordance with a rolling schedule established within each solicitation and as identified within Table 2. Cumulus Rolling Award Schedule, immediately below. The rolling award schedule shall allow adequate time for effective negotiations resulting in significant discounts being provided to DHS off of CSP published commercial pricing. Further, as a part of the Cumulus project, DHS intends to competitively solicit for and formally execute, a multiple award IDIQ. Solicitation and award of the multiple award IDIQ will follow the establishment of the above noted single-award IDIQ vehicles as reflected within the below Table 2. Schedule.

Table 2. Estimated Cumulus Rolling Award Schedule

CSP	**Estimated Proposal Response**	**Estimated Award Date**
AWS	Fiscal Year (FY)26 – Quarter (Q)2	FY26 – Q2
OCI	FY26 – Q2	FY26 – Q3
GC	FY26 – Q2	FY26 – Q3
MS	FY26 – Q2	FY26 – Q3
Multiple Awardees	FY26 – Q3	FY26 – Q4

The solicitation resulting in the multiple-award IDIQ vehicle will include both on-ramping and off-ramping terms and conditions where on-ramping efforts will allow for, over time, the addition of CSPs that meet DHS requirements, offer emerging solutions highly beneficial to the DHS mission, and that are offered at a significant discount.

It is anticipated that all proposed Cumulus IDIQ vehicles awarded, directly executed by DHS, OPO, shall allow for firm fixed price (FFP) and firm fixed unit price (FFUP) contract line-item numbers (CLINs), to be established at the IDIQ Order Level based on IDIQ Order Level requirements.

Because of the anticipated competitive nature of the referenced multiple award IDIQ supporting the Cumulus project, no further information regarding aspects of that solution shall be presented within this justification as it shall be executed in accordance with CICA requirements. This justification and its content very specifically support those DHS efforts to award multiple, single award IDIQ vehicles directly to the brand name CSPs identified above.

The total estimated performance period and ceiling of the combined multiple, single-award Cumulus IDIQ vehicles is represented within Table 3. below:

Table 3. Estimated Cumulus Ordering Periods and Total Amounts*

Single IDIQ Contract Awards	Est. Ordering Period-Duration	Est. Total Amount
Current DHS CSP Spend	-	[redacted]
Base Ordering Period	One-Year	[redacted]
Optional Ordering Period One	One-Year	[redacted]
Optional Ordering Period Two	One-Year	[redacted]
Optional Ordering Period Three	One-Year	[redacted]
Optional Ordering Period Four	One-Year	[redacted]
Total Estimated Ceiling Amount		[redacted]

* Estimated (Est.) Total Amount reflects all single-award IDIQ vehicles to be awarded in total, inclusive of all IDIQ awardees (AWS, GC, MS, and OCI).

The total estimated performance period and ceiling of each of the single-award Cumulus IDIQ vehicles is represented within Table 4. below. Amounts specified are indicated in millions of dollars ($M) and rounded to the nearest million. Detailed cost estimate data is located in the Cumulus IGCE:

Table 4. Estimated Cumulus CSP Specific Ordering Periods and Ceiling Amounts

CSP	Base	Period One	Period Two	Period Three	Period Four
AWS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Azure	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
GC	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
OCI	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

DHS has long relied on CSP solutions to support its mission-critical operations across multiple management functions (Headquarters (HQ) and Components. Identified CSPs and their developed commercial solutions have been integral to DHS' efforts to enable hyper scaling, elasticity, high availability, high performance computing, and Information Technology (IT) capabilities Department-wide.

Within DHS, CSP solutions have been developed, implemented, and are fully operational Department-wide. Operational CSP solutions provide critical capabilities for compute, storage, database, network, artificial intelligence, cybersecurity, logging, and monitoring which underpin the ability for HQ and its Components to deliver mission success. As a result of DHS directed data center closure and migration activities, the vast majority of IT processing workloads exist with the identified CSP solutions covered by Cumulus requirements.

3 Description of Supplies/Services.

DHS requires commercial CSP services with on-demand, secure, scalable, flexible, automated, and cost-effective cloud computing facilities, services and resources that are accessible via a web Graphical User Interface (GUI) console or portal, CSP Application Programming Interfaces (APIs), CSP Command Line Interface (CLI), or CSP Software Development Kit (SDK) that allows DHS to rapidly and programmatically provision and/or de-provision CSP services and/or resources within the CSP environments.

Established DHS requirements necessitate Cumulus solutions that include at a minimum a service model provided for by a CSP that is a FedRAMP Marketplace approved environment officially listed by the General Services Administration (GSA) at "High, Moderate, and Low" ratings for XaaS cloud services within the continental United States. Further, CSP solutions considered in support of Cumulus must fully satisfy DHS established CSP

minimum requirements described in section 5.2 DHS Established Minimum Requirements identified below, and must provide both established and innovative capabilities necessary for the services and resources needed to fulfill critical Department-wide mission requirements.

The scope of this requirement includes all commercial XaaS services available in CSP specific government cloud and commercial cloud facilities, availability zones and regions equal to or exceeding services available to other government agencies and commercial customers. Per publicly available CSP specific information, not all CSP services are available in all regions.

4 Identification of Statutory Authority Permitting Other Than Full and Open Competition.

This is a justification for brand-name descriptions pursuant to 41 U.S.C.3304(a)(1) as implemented by RFO FAR 6. 103-1, entitled "Only One Responsible Source and No Other Supplies or Services Will Satisfy Agency Requirements" with specific references to RFO FAR 6.103-1(b) and RFO FAR 6.103-1(d).

5 Demonstration that the proposed contractor's unique qualifications or the nature of the acquisition requires use of the authority cited.

The authority represented within this justification for other than full and open competition includes RFO FAR Subpart 6.103-1(a), only one responsible source and no other supplies or services will satisfy agency requirements. The specific application of RFO FAR 6.103-1(d) for brand-name descriptions is pertinent to Cumulus requirements and the anticipated acquisition strategy immediately above. The inclusion of brand name CSPs in this immediate instance prevents full and open competition. Establishing multiple, single-award IDIQ vehicles including brand name CSPs, each satisfying Cumulus minimum requirements while offering unique capabilities that exceed minimum requirements, offers the Department a highly effective and efficient mechanism for timely and consistently securing commercial cloud hosted environments where environments are already developed, tested, and fully established.

Key advantages to the acquisition strategy include the ability to directly access CSP native features and functionalities offered by those brand name CSPs without restrictions that may be imposed by resellers. This ensures DHS can fully utilize the capabilities of CSP platforms to meet its operational needs. Managing CSP accounts directly allows for faster changes and issue escalation without the added complexity of coordinating through a reseller, improving efficiency and responsiveness. The Department will also receive access to detailed usage reports, which are often not provided by resellers, enabling greater transparency and

4

informed decision-making. Additionally, the Department gains early access to new, in-scope products and features, including beta programs and previews, which resellers may not be able to guarantee, allowing the Department to innovate with cutting edge technological advancements. By managing its own CSP environments, the Department reduces long-term dependency on third-party intermediaries, fostering greater control, agility, and self-sufficiency. Collectively, these benefits support DHS's mission to enhance efficiency, security, and innovation in its cloud adoption strategy.

5.1 DHS CSP Mission Critical Justification

The mission of the Department is critical to safeguarding the United States against evolving threats while ensuring resilience across key domains, including cybersecurity, border security, counterterrorism, and disaster response. The Department integrates advanced technologies, intelligence analysis, and interagency collaboration to protect critical infrastructure, secure the nation's borders, and mitigate risks to national security and public safety. The Department requires full ownership of real time, high performance, reliable, and secure CSP infrastructure, services, and solutions support to provide environments, systems, and applications to detect, deter, and respond to threats in real-time. These capabilities ensure the continuity of critical services and the protection of American citizens and assets in an increasingly complex and interconnected world.

The Department requires the flexibility to specify which CSPs and their services are required to meet mission needs which directly relates to the Department's ability to successfully manage programs and systems. The ability to meet Cumulus, Component, program and system requirements, cost of existing environments, potential environment cost savings determined by CSP competition, cost of migration and personnel retraining, total discount structure, total cost of ownership and impact to existing operations are all factors that the Department is exclusively and uniquely capable of evaluating to ensure mission needs are met. If unplanned cost, schedule, and performance risks are introduced, the risk of Department mission failure increases exponentially. Mission failure compromises national security, public safety, and protection of American citizens.

5.2 DHS Established Minimum Requirements

The acquisition strategy developed and the associated brand name CSPs referenced seek to provide unique mission critical capabilities across the Department with maximum effectiveness and efficiency. Brand name CSPs included within Table 1 above present CSP solutions that satisfy Cumulus minimum requirements in addition to unique CSP capabilities that can only be met by a specific brand name CSP. Established minimum requirements in this instance are not considered unduly restrictive, as they are based on the security and technical capabilities necessary to support the Cumulus scope in providing Department-wide CSP services without compromising mission success, data integrity, and mission and data

security. The brand name CSPs indicated in Table 1 above have been identified based on their publicly available cloud service offerings.

The particular brand names identified in Table 1 are critical to the Government's requirements, and market research indicates other companies' similar products, or products lacking the particular feature, do not meet, or cannot be modified to meet, the agency's minimum needs. The following established CSP minimum requirements were considered in identifying the brand name CSPs in Table 1 above:

- Provide DHS full ownership of all root accounts, linked accounts and payer / master organization accounts which contain DHS data and processing systems. DHS shall provide Components with root accounts, linked accounts, and payer / master organization accounts upon receipt from the CSPs. All meta data is the sole ownership of DHS and cannot be used for any purpose without expressed permission from DHS
- Provide DHS unrestricted ability to link and group accounts in a logical structure specified by DHS for centralized management of billing, secure configuration, account policies and identity management within a single CSP.
- Provide DHS unrestricted access to raw CSP usage and spend data in management billing accounts (AWS master payer account, Azure billing account, Google Cloud billing account, OCI billing page) via CSP Graphical User Interface (GUI) consoles and other XaaS cost tracking and optimizing tools via Application Programming Interface (API) to include regular access to and generation of Cost and Usage (CUR) Reports.
- Provide references to CSP developed product lists that include current and new products as they are added to the product list. This product list shall include all commercial, government, region specific products, as applicable, offered by the CSP. Any pricing discounts offered on the awarded CSP’s products shall be provided to the government.
- Availability of the full breadth of the CSP's offered cloud services in commercial and government cloud regions as Commercial Off The Shelf (COTS) technology ensuring availability, integrity, rapid development, confidentiality, provisioning, deployment, redundancy, and immediate use of approved services, on demand.
- Capability to scale rapidly and automatically to meet organizational mission demand, organic growth or maturation, operational requirements (routine and on-demand), and quickly provide the government with improved solutions associated with industry innovation.
- Capability to both horizontally and vertically scale to four thousand virtual instances in less than 10 minutes, support hundreds of petabytes of storage, support a minimum of six terabytes of storage for databases, and be able to scale across two or more data centers
- Large market presence in providing public cloud IaaS service offerings defined as a CSP that has more than three (3) years of market presence and demonstrates a minimum of $250 million in annual IaaS service revenue over the 12-month period reflected in the CSP’s most recent financial statement or records, excluding all managed and professional services, and a minimum of 100,000 virtual machines (VMs) currently in production, operating simultaneously, within its public commercial cloud.
- Provide CSP marketplace approved services that meet or exceed FedRAMP High, Moderate, and Low accreditation and cybersecurity protection requirements, as defined in NIST SP 800-53, Rev. 5, for sensitive government applications and systems.

- Provide redundancy across multiple data centers, geographically dispersed from each other, to prevent natural and man-made disasters from impacting operational status. All services shall be scaled over multiple data centers and provide for real-time automatic failover without interruption to the service the systems are supporting, should a disaster occur.
- Provide a minimum availability level of 99.9% for each of their services unless otherwise stated for a particular service in accordance with their commercially advertised Service Level Agreements (SLAs). Resources launched in multiple datacenters shall continue to operate and be available when one of the data centers is offline for 100% uptime redundancy.
- Unrestricted access to CSP GUI consoles and API endpoints required to create, provision, configure, and terminate all resource instances within 5 minutes of request using automated Infrastructure as Code (IaC), direct API calls, or manual GUI console workflows.
- Unrestricted functionality to integrate cloud services offerings through user-facing, self-service interfaces and service endpoints to enable system interoperability in a multi-cloud ecosystem through the exchange of information and identities.
- Provide a fully managed, gigabyte to petabyte-scale data warehouse service in the cloud, which allows for 100GB of data to scale to a petabyte or more. This service shall allow the user to run Business Intelligence (BI) tools against the data source to use the data to acquire new insights for the business. Complex query datasets shall be returned within minutes using SQL based tools to analyze the data.
- Provide DHS complete control over the entire virtual networking environment, including selection of its own IP address range, creation of subnets, and configuration of route tables and network gateways.
- Support a minimum of 1000 Security / Firewalling rules and a minimum of 1000 Access Control Rules to control traffic flow.
- Provide ability to bypass the public Internet and provide a direct connection to the commercial or government CSP from the DHS Data Center over a secure scalable on-demand cloud interconnection, providing a secure connection over a private link that improves performance, reduces costs, increases security, and ensures consistent throughput at network speeds up to 10Gbps.
- Provide a SaaS capability to deliver virtual desktops to the entire DHS organization. The number of desktops will be defined at the order level. The desktops shall support Government security standards, provide per user profiles, support Microsoft Windows Desktop and Linux Operating systems, and be capable of running any application that can run on these operating systems on a physical desktop.

Brand Name CSPs indicated in Table 1 provide FedRAMP offerings that satisfy all of the DHS established minimum requirements. The ability to satisfy all minimum defined requirements will ensure DHS has the capability to continue meeting its technical (e.g., NIST 800-53, Rev.5), policy (e.g., DHS 4300), and statutory (e.g., FISMA) requirements to protect sensitive information being deployed or hosted in CSP environments across the Department. The ability to satisfy all of the DHS established minimum requirements will also ensure complete ownership, continued access to and use of innovative enterprise CSP services

meeting mission objectives as presented within the Cumulus scope. The impact of not satisfying the aforementioned requirements will result in an inability to establish a centralized solution for securing critical CSP services that ensures the largest possible volume discounts, enhanced interoperability, governance, and consistent monitoring, application of and auditing of critical cybersecurity requirements and enhanced operational effectiveness across the Department. Department personnel calculated that in the first year of execution, the Department expects to realize at least $142M in savings leveraging the entire economy of scale of the Department's CSP services demand. Lack of a centralized CSP services procurement solution additionally leads to interoperability challenges and governance inefficiencies due to the fragmentation of network and environment attributes, implementations and data profiles.

Additionally, heterogeneous cloud architectures and footprints increase cybersecurity risk by complicating the enforcement of cybersecurity controls requiring significant customization to detect, plan, remediate, test, and monitor cybersecurity posture. Without complete ownership of CSP environments, DHS would be forced to rely on a third party to address time sensitive, safety and life critical vulnerabilities, and introduce defects and issues that could compromise mission critical SLAs, leading to mission failure.

5.3 CSP Specific Requirements

In addition to the DHS established Cumulus minimum requirements above, the following sections describe CSP specific requirements critical to successful mission delivery at the Department, which have been validated by market research to only be able to be met by a singular specific CSP. These requirements include but are not limited to specific brand name products, services, tools, workflows, architectures, interfaces and support that Department mission critical operational systems are built upon, tightly coupled with, depend on and are dependent upon. The critical differentiating factor between two or more unique CSP services that perform similar functions is the mechanism for their use. Each CSP has developed CSP unique Application Programming Interfaces (APIs), Command Line Interfaces (CLIs), and Software Development Kits (SDKs) to allow users and systems to access and use CSP specific services. These API, CLI, and SDK technologies are not interoperable between unique CSPs and would require extensive software, platform, and workforce modifications, testing, and accreditation as described in detail in sections 5.1 DHS CSP Mission Critical Justification, and 5.4 Migration Risks and Skillset Gaps to replace with another CSP's API, CLI, and SDKs to leverage another unique CSP. As a result, existing systems will incur high risks resulting in schedule and cost overruns, mission degradation and failure if required to migrate from a particular CSP with CSP specific requirements to another unique CSP with unique API, CLI, and SDK requirements.

5.3.1 AWS Specific Requirements

AWS is the only CSP that operates the following AWS specific services, which a large amount of Department-wide systems specifically require. The services below do not include the full breadth of available AWS services operational Department-wide. Market research indicates that other companies' similar products, or products lacking particular features, interfaces, and behaviors, do not meet, or cannot be modified to meet the Department's needs. No other brand name CSPs can natively host and provide the required AWS services described above along with Cumulus minimum requirements documented in 5.2 DHS Established Minimum Requirements.

- AWS CloudTrail
- AWS CloudWatch
- AWS DirectConnect
- AWS DynamoDB
- AWS Elastic Container Service (ECS)
- AWS Elastic Kubernetes Service (EKS)
- AWS Elastic Load Balancing (ELB)
- AWS Enterprise Cloud Compute (EC2)
- AWS File Server (FSx)
- AWS Lambda
- AWS OpenSearch Service
- AWS Oracle RDS
- AWS Relational Database Service (RDS)
- AWS Simple Storage Service (S3)
- AWS S3 Data Lake
- AWS Virtual Private Cloud (VPC)

5.3.2 Azure Specific Requirements

Microsoft Azure is the only CSP that operates the following Azure specific services which a large amount of Department-wide systems specifically require. The services below do not include the full breadth of available Azure services operational Department-wide. Market research indicates that other companies' similar products, or products lacking particular features, interfaces, and behaviors do not meet, or cannot be modified to meet the Department's needs. No other brand name CSPs can natively host and provide the required Azure services described above along with Cumulus minimum requirements documented in 5.2 DHS Established Minimum Requirements.

- Azure App Services
- Azure Availability Sets
- Azure Disks
- Azure Functions
- Azure Key Vault

- Azure Kubernetes Service (AKS)
- Azure Private Endpoints
- Azure Storage Accounts
- Azure Structured Query Language (SQL) Database (DB)
- Azure Virtual Machines
- Azure Virtual Networks
- Microsoft Entra ID
- Microsoft Exchange Administration services
- Microsoft Office 365
- Microsoft Teams

5.3.3 Google Cloud Specific Requirements

Google Cloud is the only Google Cloud that operates the following Google Cloud specific services which a large amount of Department-wide systems specifically require. The below services do not include the full breadth of available Google Cloud services operational Department-wide. Market research indicates that other companies' similar products, or products lacking particular features, interfaces, and behaviors do not meet, or cannot be modified to meet the Department's needs. No other brand name CSPs can natively host and provide the required Google Cloud services described above along with Cumulus minimum requirements documented in 5.2 DHS Established Minimum Requirements.

- Google Cloud Apigee X
- Google Cloud BigQuery
- Google Cloud Compute Engine
- Google Cloud Cloud Dialogflow
- Google Cloud Cloud Document AI
- Google Cloud Cloud Logging
- Google Cloud Cloud Run
- Google Cloud Cloud Run Functions
- Google Cloud Cloud Storage
- Google Cloud Cloud Workstations
- Google Cloud Distance Matrix
- Google Cloud Networking
- Google Cloud Notebooks
- Google Cloud reCAPTCHA Enterprise
- Google Cloud Workflows

5.3.4 OCI Specific Requirements

OCI is the only CSP that operates the following OCI specific services which a large amount of Department-wide systems specifically require. The below services do not include the full breadth of available OCI services operational Department-wide. Market research indicates that other companies' similar products, or products lacking particular features, interfaces, and

behaviors do not meet, or cannot be modified to meet the Department's needs. No other brand name CSPs can natively host and provide the required OCI services described above along with Cumulus minimum requirements documented in 5.2 DHS Established Minimum Requirements.

- OCI Exadata Database Service
- OCI Exadata Exascale
- OCI Functions
- OCI Kubernetes Engine
- OCI Object Storage
- OCI Virtual Cloud Networks
- OCI Virtual Machines

5.4 Migration Risks and Skillset Gaps

Migrating to different CSPs presents a multitude of technical challenges that would require significant planning for unplanned and increases in cost, schedule, and performance risk. A critical issue is that existing Department cloud hosted environment, network, system, interoperability cybersecurity and reporting architectures are tightly coupled to specific services offered exclusively by singular CSPs. These architectures and interfaces are incompatible with other CSP environments (even when making maximum use of open standards, architectures, and interfaces) due to specific unique CSP interface constraints at the platform level which would require extensive rearchitecting of existing mission critical workflows. Differences in storage formats, networking configurations, and security protocols necessitate significant refactoring or reconfiguration of applications to align with a different CSP's environment and unique interfaces. Migration is complex, especially for large system footprints, relationships, and datasets. Migrations introduce probabilities and impacts of risk and may involve downtime, data integrity risks, and compliance risk, especially when handling sensitive, confidential, For Official Use Only (FOUO) and / or Controlled Unclassified Information (CUI) data. Additionally, differences in service offerings, pricing models, and performance characteristics between CSPs can complicate cost optimization and performance tuning. Cybersecurity control identification, implementation, documentation and remediation activities required to obtain a system Authorization To Operate (ATO) also inherit significant risk as CSPs implement various CSP services differently. Significant effort is required to ensure risk is mitigated to an acceptable level to allow for system accreditation. Ensuring business workflow continuity during the migration process requires significant overhead, robust testing, validation, and rollback strategies to mitigate risks and minimize disruptions especially for highly available mission, safety, and life critical applications and systems. Migration activities between CSPs are estimated to require at least 12 months of transition per system with overlapping environments in multiple CSPs required to ensure business operations continuity. This overhead results in duplicate costs and personnel support costs.

CSP migration activities also affect all environments and systems dependent upon any environments and systems required to migrate. In addition to the risks described above, additional interoperability challenges, service usage, data transfer costs, cybersecurity accreditation activities and all verification and validation testing required to ensure feature parity that would not have been present without migration become added risks to mission critical environment and system owners. Individual task order requirement requests, CSP justification, and competition determination cannot be decided based on a singular environment or system but rather the entirety of the ecosystem that depends on a particular mission service. Department Components have invested hundreds of millions of dollars in specific CSPs to date to ensure mission success and availability. Market research and Component interviews have revealed that individual, single large system migrations can be estimated to cost up to $100M each if required to migrate to a new CSP.

Migrating to different CSPs requires incompatible development and support personnel skill sets and qualifications as each CSP requires different expertise, experience, and certifications to demonstrate comparable mastery of CSP functions critical to performing required support tasks. Market research has shown that a disproportionate amount of Lead System Integrator (LSI) cloud engineers are cross trained to effectively operate in more than one CSP concurrently due to the amount of specialization, experience and training required to be obtained and maintained. The Government would be placing unanticipated burden on mission owners, LSIs, system developers, operators, and users that would result in personnel transition actions, retraining, lost productivity and upskilling that would detract from originally planned program milestones.

Due to these factors, the total cost of ownership inclusive of migration, personnel retraining costs and adverse effects on dependent environments and systems will far outweigh any anticipated individual order level cost savings provided through competition.

5.5 Discount Structure

The Cumulus procurement strategy including direct awards to brand name CSPs will result in best value yielding the highest CSP discount structures possible, leveraging the total unified buying power of the Department, delivering on highly effective mission requirements while maximizing ordering efficiency and consistency Department-wide. Obtaining the maximum available discount structure is not possible when using third party reseller services for several reasons including but not limited to:

1. Third party reseller total buying power with the Department excluded is less than the total buying power of the Department as a whole. CSPs rely on the projected amount of expected spend when factoring in customer specific discount structures. As more agencies move towards CSP direct contract awards, third party reseller buying power is expected to further decrease.
2. Third party resellers while providing discounts to the Government through currently established awards, introduce additional contract administrative overhead,

maintenance, reporting, and operational activities required to be funded at a cost to the Department which decreases the total provided discount structure to the Department. It is fully anticipated that value added services provided for by third party resellers can and will be satisfied with in-house solutions further driving down contract costs that would be incurred by the Department if awarding to a third party reseller.

3. Third party resellers do not always provide access to the entirety of CSP discounting opportunities available to Department consumers due to the structure of how billing is calculated and what services are available in order to optimize solution architectures and to further decrease cost. Commercial agreements between resellers and their consumers can restrict the overall data available to all consumers based on lack of easy means to separate and aggregate data. By directly awarding to CSPs, the Department will have full access to all tools and opportunities for billing auditing, transparency, optimization and modernization.

6 Description of Efforts Made to Ensure that Offers are Solicited from as Many Potential Sources as is Practicable.

For those reasons represented within this justification, to specifically include Section 5. above, brand name CSPs shall be initially awarded on a rolling schedule. Additionally, in support of the Cumulus project, a competitive solicitation shall be published resulting in a multiple award IDIQ which includes on-ramping terms and conditions allowing for the future award of additional CSPs that meet DHS requirements and offer emerging solutions highly beneficial to the DHS mission.

DHS intends to post this Justification on SAM.gov pursuant to RFO FAR Subpart 6.301(b)(2), estimated in FY26-Q2.

7 Determination by the Contracting Officer that the Anticipated Cost to the Government will be Fair and Reasonable.

As represented above, the rolling award schedule shall allow adequate time for effective brand name CSP negotiations resulting in significant discounts being provided to DHS which will be directly applied to CSP published commercial pricing. Specifically, Cumulus solicitation requirements shall identify a minimum discount that supports DHS negotiation expectations established to drive down cost. Cumulus solicitations and resulting awards shall clearly note that DHS reserves the right to request further discounts at the order level based on order level requirements to ensure CSP cost to the Government is at all times determined to be both fair and reasonable.

8 Description of Market Research.

In support of the Cumulus effort an Integrated Project Team (IPT) was established supporting cross-agency and industry engagement activities, as well as requirements development.
A critical cornerstone of market research activity conducted in support of Cumulus, which has spanned nearly three years has been the multi-faceted communication and engagement strategy which has included most recently, Department-wide review of existing and anticipated Cloud requirements, External Agency (DoD, CIA, GSA, SSA, etc.) discussions regarding Cloud award review and lessons learned, industry engagement including for example, draft release of requirements, vendor one-on-one activities, and industry day events, and in IPT review and validation of extensive ECLIPS engagement information.

Further, in support of Cumulus additional industry engagement activities are planned prior to solicitation release, including publication (SAM.gov) of draft solicitation information and a virtual industry engagement event providing additional information pertaining to Cumulus.

9 Any Other Facts Supporting the Use of Other Than Full and Open Competition.

N/A

10 A Listing of the Sources, if Any That Expressed, in Writing, an Interest in the Acquisition.

A DHS Acquisition Planning Forecast System (APFS) record F2026072856 was posted January 20, 2026. As of the date of this document, responses from Deltek, IBM, and Efficio have been received, each of which requesting additional information pertaining to Cumulus.

11 A Statement of the Actions, if Any, the Agency May Take to Remove or Overcome Any Barriers to Competition Before Any Subsequent Acquisition for Supplies or Services Required.

DHS will continue market research efforts as required in exploring additional available CSPs, which may potentially satisfy all DHS requirements in the future via the aforementioned multiple award IDIQ.

12 Contracting Officer's Certification. I certify that the data supporting the recommended use of other than full and open competition is accurate and complete to the best of my knowledge and belief.

[redacted]

Contracting Officer
DHS, Office of Procurement Operations

13 Technical/Requirements Personnel Certification. I certify this requirement meets the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

[redacted]

Technical Representative
DHS, Office of the Chief Information Officer

14 Procuring Activity Advocate for Competition (PAAC) Certification. I certify that the data supporting the recommended use of other than full and open competition is accurate and complete to the best of my knowledge and belief.

[redacted]

Procuring Activity Advocate for Competition
DHS, Office of Procurement Operations

15 Head of the Contracting Activity (HCA) Certification. I certify that the data supporting the recommended use of other than full and open competition is accurate and complete to the best of my knowledge and belief.

[redacted]

Head of the Contracting Activity
DHS, Office of Procurement Operations

APPROVAL:

[redacted]

Chief Procurement Officer
DHS, Office of the Chief Procurement Officer