JUSTIFICATION FOR AN EXCEPTION TO FAIR OPPORTUNITY

Acquisition Title:	Okta Operations and Maintenance (O&M) Services
Agency:	HRSA
Acquisition Year (FY):	FY 2026
Author:	[redacted]

2. Description of Action:

Nature:	☒ New Requirement	☐ Follow-on Order	
	☐ Modification to Existing Delivery/Task Order/Contract Number:		
Order Against:	Multiple Award ID/IQ Contract Number:		HHSN316201200018W
Pricing:	☒ Firm-Fixed Price	☐ Time & Materials	☐ Cost Type
Funds:	☐ OMA	☒ Other Funds:	

3. Description of Applicable Contract Provisions:

HRSA intends to issue a task order under the NIH NITAAC CIO-SP3 Government-Wide Acquisition Contract (GWAC) in accordance with RFO 16.507 ordering procedures. Ordering procedures are governed by FAR Subpart 16.5 and, for HHS, by HHSAR Part 316 and HHS Class Deviation CD-2026-05 implementing the Revolutionary FAR Overhaul (RFO) Part 16 ordering procedures. RFO 16.507 requires that all GWAC awardees receive a fair opportunity to be considered for each order unless an exception to fair opportunity applies. The applicable exception to fair opportunity is RFO FAR 16.507-6(b)(2) – Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized. The task order will incorporate all applicable terms and conditions of the base IDIQ contract, including provisions governing performance, security, and service delivery. These include requirements for compliance with HSPD-12, FIPS 201, and Federal Identity, Credential, and Access Management (ICAM) policies, as well as applicable cybersecurity requirements under FISMA and NIST Special Publications. The contractor will also be required to adhere to HHS-specific security and privacy policies, including safeguarding Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII).

Contract provisions will address the operation and maintenance of the Okta Federated Identity Hub, including service availability, system performance, incident response, identity federation (e.g., SAML and OpenID Connect), and access control. The contractor shall ensure continuity of operations, maintain system security, and support authentication and authorization services across HHS and HRSA systems. Additionally, the task order will include provisions for performance monitoring, reporting requirements, and adherence to defined Service Level Agreements (SLAs) to ensure reliable and secure delivery of mission-critical identity and access management services

4. Description of Supplies or Services:

The estimated value of the proposed action, including all options, is: [redacted]

The estimated value of the proposed action, including all options, is $[redacted] This total consists of [redacted] for base tasks and [redacted] for all optional tasks, plus the applicable NITAAC/NIH contract access fee of 0.65% ([redacted] for optional tasks).

This requirement is for continued Access Management Services (AMS) and HSPD-12 System Integration Services, with primary emphasis on the operation, maintenance, and enhancement of the Okta Federated Identity Hub for the Department of Health and Human Services (HHS) and the Health Resources and Services Administration (HRSA). The contractor shall provide comprehensive operations and maintenance (O&M) support for the Okta platform (Software-as-a-Service), including administration of the Okta tenant; configuration and sustainment of single sign-on (SSO); management of identity federation services (e.g., SAML and OpenID Connect integrations); and support for authentication and authorization services across HRSA and HHS applications. Services also include user provisioning and deprovisioning, identity lifecycle management, system monitoring, incident response, troubleshooting, and implementation of security patches, upgrades, and enhancements.

In support of the broader Identity, Credential, and Access Management (ICAM) environment, the contractor shall maintain integration between the Okta Federated Identity Hub and the HHS Card Management System (CMS) to enable Personal Identity Verification (PIV)-based authentication in accordance with HSPD-12 and FIPS 201 requirements. The contractor shall also support implementation of Federal cybersecurity requirements, including multi-factor authentication (MFA) and Zero Trust architecture initiatives.

While Okta is a commercial platform, the services to be procured are peculiar to the existing HRSA implementation, including its configurations, integrations, and dependencies with the HSPD-12 infrastructure and enterprise applications. These elements constitute a highly specialized environment that is not readily transferable without significant cost, time, and operational risk.

The anticipated period of performance is a 12-month base period (July 25, 2026 through July 24, 2027). If necessary, services may be extended under FAR 52.217-8 to ensure continuity of operations. The scope of work remains consistent with the base requirement, focusing on sustaining and enhancing the existing Okta and HSPD-12 environment. Any optional tasks included in this action will support incremental enhancements, such as integration of additional SaaS and custom applications, expansion of enterprise authentication capabilities, and alignment with evolving Federal ICAM and cybersecurity requirements.

5. Authority and Rationale:

The Contracting Officer shall give every awardee a fair opportunity to be considered for a delivery/task order exceeding the micro purchase threshold unless one of the following statutory exceptions applies. FAR 16.505(b)(2). Mark the applicable exception:

☐ The agency need for the supplies or services is so urgent that providing a fair opportunity would result in unacceptable delays [FAR 16.505(b)(2)(i)(A)];

☒ Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services are unique or highly specialized [FAR 16.505(b)(2)(i)(B)];

☐ The order must be issued on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order [FAR 16.505(b)(2)(i)(C)];

The authority cited for this action is RFO FAR 16.507-6(b)(2), which permits an exception to the fair opportunity process when only one awardee is capable of providing the required services at the level of quality required because the services are unique or highly specialized. This justification supports the issuance of a sole-source task order to Deloitte Consulting, LLC under the NIH NITAAC CIO-SP3 Government-Wide Acquisition Contract (GWAC) without providing fair opportunity to other contract holders, as implemented by HHSAR Part 316 and HHS Class Deviation CD-2026-05.

This requirement is highly specialized because it involves the continued operation, maintenance, and enhancement of HRSA's production Okta Federated Identity Hub, which serves as the enterprise authentication and identity federation platform supporting secure access to HRSA and HHS applications. Although Okta is a commercial identity platform, HRSA's implementation is a mature production environment that has been extensively customized and integrated with numerous enterprise systems and security services. The requirement encompasses agency-specific Okta tenant configurations, complex SAML and OpenID Connect identity federation integrations, direct integration with the HHS HSPD-12 Card Management System (CMS) to support PIV-enabled authentication in accordance with HSPD-12 and FIPS 201, and advanced security capabilities including multi-factor authentication (MFA), Okta FastPass, FAL2-compliant token encryption, and Zero Trust identity governance aligned with OMB M-22-09.

The specialized nature of this requirement is not the use of these technologies themselves, but the expertise required to safely operate and sustain HRSA's existing production implementation. The environment consists of numerous production application integrations, established federation trust relationships, authentication workflows, security policies, certificate mappings, and agency-specific identity governance processes that have evolved over several years of operational support. Maintaining these services requires detailed knowledge of how the environment has been configured, validated, secured, and integrated across the HRSA enterprise while ensuring continuous availability of authentication services.

Deloitte has operated and continuously enhanced HRSA's production Okta Federated Identity Hub since its implementation and possesses the specialized operational expertise necessary to administer this environment without disrupting mission-critical services. This expertise extends beyond general Okta administration and includes detailed knowledge of HRSA's authentication architecture, application-specific federation configurations, PIV authentication processes, identity lifecycle management, security controls, and operational procedures required to maintain compliance with Federal Identity, Credential, and Access Management (ICAM), HSPD-12,

FIPS 201, and Zero Trust requirements.

Market research determined that no other NITAAC CIO-SP3 contract holder or other commercially available source currently possesses equivalent operational knowledge of HRSA's production environment or can reasonably assume responsibility for these services within the required period of performance. While several vendors demonstrated experience providing enterprise identity and access management services and Okta implementation support, none were identified as currently operating or maintaining HRSA's Okta Federated Identity Hub or its integration with the HHS HSPD-12 Card Management System. Conducting a fair opportunity competition would not provide sufficient time for a successor contractor to acquire the detailed operational understanding necessary before assuming responsibility for HRSA's continuously operating production authentication environment. A successor contractor would be required to inventory and validate existing application integrations, reconstruct authentication workflows, rebuild identity federation trust relationships, re-establish CMS/PIV integrations, validate security policies, and replicate HRSA-specific identity governance configurations in a live production environment before independently assuming operational responsibility.

These activities introduce significant technical, operational, cybersecurity, schedule, and cost risks. Errors in authentication configuration or federation trust relationships could disrupt user access to HRSA and HHS production systems, interrupt single sign-on capabilities, degrade multi-factor authentication services, and create compliance gaps with HSPD-12, FIPS 201, and Federal Zero Trust requirements. Additionally, delayed implementation of security updates, certificate renewals, or authentication policy changes could increase cybersecurity exposure and adversely affect the availability of mission-critical applications relied upon by HRSA employees, contractors, grantees, and external partners.

The Government estimates that transitioning these services to a new contractor would require substantial duplication of effort to analyze, validate, and reconstruct the existing production environment, resulting in an estimated increase in implementation costs of approximately 30 percent, as well as significant schedule delays before the contractor could safely assume operational responsibility. These costs represent duplication of work already performed and do not provide additional value to the Government.

Accordingly, Deloitte's specialized qualifications are directly related to successful performance of this requirement. Deloitte is the only contractor capable of providing the required services at the level of quality necessary to maintain uninterrupted operation of HRSA's enterprise authentication environment during the required period of performance. Award to any other contractor would result in unacceptable schedule risk, increased costs, substantial duplication of effort, and increased operational and cybersecurity risk to mission-critical authentication services.

The current task order expires on July 24, 2026. If a follow-on order is not awarded by that date, there is a significant risk of interruption to operations and maintenance support for the Okta Federated Identity Hub, which serves as HRSA's enterprise authentication and identity federation platform. The Okta Federated Identity Hub provides centralized authentication, single sign-on (SSO), multi-factor authentication (MFA), and identity federation services supporting HRSA and HHS applications used by Federal employees, contractors, grantees, and external partners. These applications depend on the platform for secure user authentication, authorization, and access control. Without continuous operational support, HRSA would lose the ability to:

- Respond to authentication and identity-related production incidents.
- Maintain or renew federation trust relationships and certificates.
- Implement critical security patches and software updates.
- Onboard new applications or modify existing identity integrations.
- Support user provisioning, deprovisioning, and privileged access changes.
- Implement changes required to maintain compliance with Federal cybersecurity directives, including HSPD-12, FIPS 201, OMB M-22-09, and Zero Trust requirements.

A disruption to the Okta Federated Identity Hub could result in authentication failures, loss of single sign-on functionality, inability of users to access mission-critical systems, increased cybersecurity risk, and interruption of business operations across HRSA. Depending on the affected integration, outages could prevent users from accessing enterprise applications that support grants management, program administration, financial management, human resources, and other essential agency functions.

Because the Okta Federated Identity Hub operates continuously in a production environment, any lapse in contractor support after July 24, 2026 would significantly increase the risk of service interruptions, delayed incident response, and degradation of enterprise authentication services. Maintaining uninterrupted contractor support is therefore essential to ensuring the availability, security, and reliability of HRSA's identity and access management environment.

Therefore, issuance of this sole-source task order to Deloitte Consulting, LLC under RFO FAR 16.507-6(b)(2) represents the only technically sound, cost-effective, and lowest-risk approach available to the Government.

☐ It is necessary to place the order to satisfy a minimum guarantee [FAR 16.505(b)(2)(i)(D)]; or

N/A

☐ A statute expressly authorizes or requires that the purchase be made from a specified source. [FAR 16.505(b)(2)(i)(E)].

N/A

6. Agency Actions to Take or Remove Barriers That Led to Fair Opportunity Exception (If applicable):
Describe the actions, if any, the agency may take to remove or overcome any barriers that led to the restricted consideration prior to any subsequent acquisition for the supplies of services is made. If no such actions have been taken, explain why.

The current limitation to fair opportunity is driven by the highly specialized and tightly integrated nature of HRSA's Identity, Credential, and Access Management (ICAM) environment, including the Okta Federated Identity Hub and its dependencies with the HSPD-12 Card Management System (CMS) and enterprise applications. These integrations, configurations, and operational dependencies create barriers to competition due to the complexity and risk associated with transitioning to a new provider within the required timeframe. To reduce these barriers in future acquisitions, the Government will take the following actions, as feasible: (1) Documentation and Knowledge Transfer: Improve and maintain comprehensive technical documentation of the Okta environment, including configurations, integrations, and identity workflows, to facilitate potential transition to other vendors. (2) Modularization of Services: Evaluate opportunities to modularize ICAM components (e.g., separating Okta O&M, CMS integration, and application onboarding) to enable more discrete competition. (3) Standardization of Interfaces: Promote use of standardized, interoperable interfaces and architectures to reduce vendor dependency and increase portability of services. (4) Early Market Engagement: Conduct early and ongoing market research, including Requests for Information (RFIs) or Sources Sought notices, to identify and develop a broader pool of capable vendors. (5) Acquisition Planning: Consider future acquisition strategies that allow for phased transition approaches or competitive re-competes when operational risks can be mitigated. At this time, immediate actions to remove these barriers have not been implemented due to the need to ensure uninterrupted operation of mission-critical authentication services and the unacceptable risk associated with transitioning the current environment during this period of performance. However, the Government will continue to assess and implement strategies to reduce vendor dependency and enhance competition in future procurements.

7. Fair and Reasonable Price/Cost Determination: I hereby determine that the anticipated price/cost for this contract action will be fair and reasonable.

I hereby determine that the anticipated price for this contract action will be fair and reasonable. In accordance with FAR 15.404-1(b), the Contracting Officer will utilize price analysis techniques to ensure price reasonableness. These techniques include a comparison of the proposed pricing to the Independent Government Cost Estimate (IGCE), historical prices paid for similar services under prior HHS/NITAAC task orders, and, where applicable, market research and industry benchmarks for comparable identity and access management services, including Okta-related operations and maintenance. The IGCE has been developed based on prior contract performance, current labor categories, level of effort, and prevailing market rates. The Government will evaluate the contractor's proposed labor mix, hours, and rates for consistency with the IGCE and historical data to ensure alignment with current market conditions. The Contracting Officer will ensure that the final negotiated price represents a fair and reasonable cost to the Government.

Signature:	[redacted]	Date:	06/22/2026
Name:			
Title:			

8. Any other facts supporting the justification:

Document prepared in accordance with FAR 16.505(b)(2)(ii), RFO FAR 16.507-6, HHSAR Part 316, and HHS Class Deviation CD-2026-05. Post award, this justification must be posted to SAM.gov within 14 days of order placement and remain posted for a minimum of 30 days per FAR 16.505(b)(2)(ii)(D).

9. Technical / Requirements Certification: By my signature below, I certify that the supporting data under my review which is included in this Justification for an Exception to Fair Opportunity is accurate and complete.

Program Manager

Name:	[redacted]
Position Title:	
Email address:	
Phone:	

Program Manager Supervisor (or one level above Program Manager)

Name:	[redacted]
Position Title:	
Email address:	
Signature:	
Date:	

10. Contracting Officer's Approval (Required for proposed contract not to exceed $700,000 (value calculated including all options)): I hereby certify that this justification is accurate and complete to the best of my knowledge. I approve this sole source justification subject to availability of funds, and provided that the services and supplies herein described have otherwise been authorized for acquisition.

Name:	[redacted]
Signature:	

11. Legal Review:

N/A

12. OPDIV Competition Advocate Approval (Required for proposed contract over $700,000 but not exceeding $13.5 million value calculated including all options)):

I have reviewed this justification and find that it adequately supports an exception to fair opportunity.

Name:	[redacted]
Signature:	

13. Office of Small and Disadvantaged Business Utilization:

I have reviewed this justification and find that it adequately supports an exception to fair opportunity.

Name:	N/A	Phone:	
Signature:		Date:	

14. OPDIV HCA Approval (Required for proposed contract over $13.5 million but not exceeding $68 million value calculated including all options)):

Name:	N/A	Phone:	
Signature:		Date:	

15. Department Competition Advocate:

Concur:	☐	Non-Concur:	☐
Name:	N/A	Phone:	
Signature:		Date:	

(The below approval paragraph is required if the cumulative contract value, including all options, exceeds $68 million.)

16. HHS Senior Procurement Executive (SPE) Approval:

Based on the foregoing justification, I hereby approve the procurement of stated supplies/services being procured on the exception to the fair opportunity basis pursuant to the authority of paragraph 5, 41 U.S.C. 4101, as implemented by FAR 16.501-2.

State supplies/services being procured:

The estimated value of the proposed action, including all options, i[redacted]This total consists of [redacted] for base tasks and [redacted] or all optional tasks, plus the applicable NITAAC/NIH contract access fee of 0.65% ([redacted] for optional tasks).

This requirement is for continued Access Management Services (AMS) and HSPD-12 System Integration Services, with primary emphasis on the operation, maintenance, and enhancement of the Okta Federated Identity Hub for the Department of Health and Human Services (HHS) and the Health Resources and Services Administration (HRSA). The contractor shall provide comprehensive operations and maintenance (O&M) support for the Okta platform (Software-as-a-Service), including administration of the Okta tenant; configuration and sustainment of single sign-on (SSO); management of identity federation services (e.g., SAML and OpenID Connect integrations); and support for authentication and authorization services across HRSA and HHS applications. Services also include user provisioning and deprovisioning, identity lifecycle management, system monitoring, incident response, troubleshooting, and implementation of security patches, upgrades, and enhancements.

In support of the broader Identity, Credential, and Access Management (ICAM) environment, the contractor shall maintain integration between the Okta Federated Identity Hub and the HHS Card Management System (CMS) to enable Personal Identity Verification (PIV)-based authentication in accordance with HSPD-12 and FIPS 201 requirements. The contractor shall also support implementation of Federal cybersecurity requirements, including multi-factor authentication (MFA) and Zero Trust architecture initiatives.

While Okta is a commercial platform, the services to be procured are peculiar to the existing HRSA implementation, including its configurations, integrations, and dependencies with the HSPD-12 infrastructure and enterprise applications. These elements constitute a highly specialized environment that is not readily transferable without significant cost, time, and operational risk.

The anticipated period of performance is a 12-month base period (July 25, 2026 through July 24, 2027). If necessary, services may be extended under FAR 52.217-8 to ensure continuity of operations. The scope of work remains consistent with the base requirement, focusing on sustaining and enhancing the existing Okta and HSPD-12 environment. Any optional tasks included in this action will support incremental enhancements, such as integration of additional SaaS and custom applications, expansion of enterprise authentication capabilities, and alignment with evolving Federal ICAM and cybersecurity requirements.

State the full statutory authority and FAR cite and title, consistent with paragraph 4, e.g. 41 U.S.C. 3304:

Name:		Phone:	
Signature:		Date:	