Workforce 3.0
Attachment 1: Scope and Ordering Guide

Solicitation Number: HT003821R0001 Amen. 0002
Program Executive Office, Healthcare Management Systems (PEO DHMS)

SECTION I

1.0 DESCRIPTION OF RELATIONSHIP

1.1 Purpose.

The purpose of this IDIQ solicitation is to form contractual relationships necessary to deliver workforce components of the "world-class technology firm" that is a core tenet of the PEO 3.0 Strategy. As such, the resulting IDIQ contracts are referred to as "Workforce 3.0" and will be supported by the other PEO 3.0 efforts.

Workforce 3.0 is a managed solution that leverages innovative new processes, methods, and/or best-in-class methodologies from the private sector to enable the entire PEO DHMS workforce to deliver world-class technology.

Contractor employees shall not perform inherently governmental functions as discussed in FAR Subpart 7.5, "Inherently Governmental Functions" nor personal services as defined in as discussed in FAR 37.104.

1.2 Background

As a nation, our health is one of our most critical and important resources. Whether in the context of maintaining economic output, the readiness of our military to defend our national security, or paying the debt we owe to those who made sacrifices to do so, a healthy society is the engine for these activities. The Office of the National Coordinator (ONC) recently published its 2020-2025 Federal Health IT Strategic Plan (the "Plan"), laying out the Federal Government's role in healthcare and how it uses Health Information Technology (Health IT) to fulfill that role. In short, the Government regulates, purchases, and uses healthcare while also regulating, purchasing, developing, and using Health IT. The Plan further lays out some of the biggest challenges facing the healthcare industry and how the Government plans to use technology to address these and improve health outcomes. Among these are cost growth, capacity in the system, and poor health outcomes especially in areas such as obesity, substance abuse, and mental health.

PEO DHMS is a key Federal Health IT partner, and is chartered to deliver the single Electronic Health Record (EHR) and other Health IT for the Departments of Defense (DoD), the Department of Veterans Affairs (VA), and the United States Coast Guard (USCG). Sitting at the nexus of healthcare and defense, which together account for approximately 40% of that national budget, PEO DHMS is in a unique position to substantially impact strategic challenges facing the nation. National defense, like healthcare, faces challenges in resources, capacity, and capability that can be addressed through innovative technology strategies.

In its official Purpose, Goals, and Strategies (PGS) document, PEO DHMS lays out its vision for maximizing its impact on healthcare and defense. While many tend to equate PEO DHMS with EHR, PEO DHMS and its subordinate/partner offices have a considerably broader and continually expanding mission. According to data collected by ONC, EHR adoption across the country is approaching 100% (Office of the National Coordinator for Health Information Technology, OCT 2020). The Federal Health IT Strategic Plan looks well beyond core EHR capabilities while PEO DHMS missions are pivoting to provide comprehensive health management, advanced data applications, improved usability, reduced provider/patient burden, and other priorities. PEO DHMS recognizes technology will enable these missions to achieve success.

PEO DHMS delivers on these missions with a strong workforce comprised of federal civilians from multiple Agencies, military personnel from each Service, support contractors, and Prime mission product contractors. This workforce is organized into major program offices, project teams, coordinating offices, and a back office/corporate team.

PEO DHMS' workforce strives to deliver world-class technologies in the health information field. In order to succeed at one of the Department of Defense's most important missions, PEO DHMS must, to the greatest extent possible, ensure its technologies and conduct are indistinguishable from those of leading private-sector technology firms. This includes:

- Frictionless and seamless solutions and products that create the best possible user experience
- Quality products to drive demand from Government and non-Government users
- Increased competition and ignited innovation from other Health IT developers in the private sector

- Attracting the best people in these fields to join and stay in the PEO DHMS workforce

To achieve these lofty and worthy goals, PEO DHMS must undergo a fundamental shift in how it does business. In its continual evolution to achieve these objectives, PEO DHMS has transitioned across three distinct operational paradigms:

- (2013 - 2014) The first and previous phase, **PEO 1.0**, was launched via the 2013 Secretary of Defense (SECDEF) charter to establish an Electronic Health Record (EHR) for use by the Department of Defense (DoD) DoD and the Department of Veterans Affairs (VA). This phase represents the "crawl" of the PEO DHMS organization as operational processes were identified and initially established.
- (2014 - Present) The second and current phase, **PEO 2.0**, is anchored by the successful procurement and ongoing deployment of the MHS GENESIS EHR. This phase represents the "walk" of the PEO DHMS organization as operational processes entered sustainment and flagship products were launched into the market to achieve initial customer value.
- (Present - 2026) This third and next phase, **PEO 3.0**, is characterized by achieving a digitally transformed organization with ambitious year-over-year growth in product portfolio value and customer outcomes. This phase represents the "run" of the PEO DHMS organization as focus shifts from internal organizational deployment to fostering external product development across the portfolio.
- PEO DHMS seeks to launch the PEO 3.0 phase in FY21 with a four-pronged strategic effort that mirrors the operational strategies of leading commercial counterparts: *Workforce 3.0* ("WF3") to perform business support services, *Workplace 3.0* ("WP3") to provide business infrastructure, *DevMAC* to provide software development support services, and *Federal XaaS* ("XaaS") to provide software development infrastructure. For communications purposes, this strategy has been distributed through a graphical metaphor outlining parallels to the construction industry.

Inherently, the more time passes, the more a given set of circumstances change. Since PEO 2.0 began, there has already been substantial change throughout the PEO portfolio of programs, and more change is certain in the coming years, most likely at an accelerated pace.

Notably, on 01 JUL 2017, the Secretary of Veterans Affairs (VA) issued a Determination and Findings (D&F) pursuant to 41 U.S.C. § 3304(a)(7) that it was in the public interest for VA to issue a solicitation directly to Cerner for the acquisition of the EHR system being deployed by the DoD, in order to enable seamless healthcare to Veterans and qualified beneficiaries. Moreover, on 22 MAR 2018, the Deputy Commandant for Mission Support, United States Coast Guard (USCG), formally requested to partner with PEO DHMS to implement MHS GENESIS for the USCG to ensure that every military beneficiary and retiree has access to a single, unified Electronic Health Record. These decisions set off a chain of events that created a need to rethink how health IT products behave across all PEO DHMS programs and at partner agencies. These events ultimately resulted in Congress' creation of the Federal Electronic Health Record Modernization Program Office (FERHM), chartered in DEC 2019. The FEHRM tightly partners with and works side-by-side with PEO DHMS to implement health IT across the Federal ecosystem. This focal point for Federal health IT has already significantly increased the complexity of the PEO DHMS mission and is likely to

drive further growth as additional health IT partners are brought into the fold, and additional technology needs are identified.

PEO DHMS recognizes that these changes will drive considerable growth in requirements and complexity. Moreover, PEO DHMS is cognizant that the organization is not currently constructed to handle even its current product line efficiently let alone a significantly expanded one. In order to maintain its ability to meet this rapidly growing mission, without requiring substantial additional resources which may not be available, substantial transformation of its operations are required. As a result, PEO DHMS developed a comprehensive strategy to transform into a world-class technology organization.

To begin, PEO DHMS engaged in identifying specific and measurable characteristics of a "world class technology organization." The resultant assessments supported the conclusion that PEO 2.0 was some way off the standard of a mature, let alone a world-class, organization.

Perhaps more telling than the roll-up scores are some of the statements from current PEO and Program leadership in the figure below (comments are non-attributional, sources are omitted for privacy reasons):

- "[There is] no coherent strategy; everyone has a different answer. We need to know what we want to be, [need to] know where we want to go, and need to have someone who has a voice for the customer."
- "One of key things is we're all here for the mission - some of us hang on because we believe and are passionate about the mission. But it needs to trickle down to how we do that on a day-to-day basis. You can love the mission but not understand how to satisfy the mission."
- "Some [people] are lazy, some want to be spoon fed, and sometimes people don't have an understanding of what's going on. They have blinders on purpose [but] there are times that there's clarity needed."
- "We want to be more like [industry]. We want good people around; you know it when you see it."
- "We're not taking advantage of [our] vehicles to get the best and brightest out of Silicon Valley. There are people out there; why can't they support us?"
- "DHMS should have a culture of being inspired. Innovation is the result of being inspired; but right now, we aren't inspired."

Overwhelmingly, the assessments drive a conclusion that the level of organizational transformation required is substantial and that the PEO DHMS working environment is not currently able to recruit, retain, or leverage the talent required to deliver high quality technology products. World-class technology organizations are incredibly competitive in the talent market. Many best practices and techniques that make organizations attractive to the best talent are traditionally unavailable in Government, especially in the DoD. In many cases, existing policies and standards are significant barriers to performing as a world-class technology organization. This will substantially complicate any effort to transform.

Moreover, persistent blockers across the enterprise result in downstream degradation of personnel morale. A recent Defense Health Agency (DHA) staff survey indicated a Net Promoter Score (NPS) of (-20) in employee fulfillment (Defense Health Agency, JAN 2021). This is substantially lower than industry-wide figures ranging from 27 on the lowest end for Healthcare and 71 on the highest end for Education & Training (Retently, 2020).

1.3 Outcomes

When the transformation efforts are complete, the PEO will:

1. Manage a portfolio of product teams and products that prioritize the experience of those using the products
2. Have a culture that prioritizes continuous improvement, rapid decision-making, and streamlining business priorities by maximally leveraging policy and regulatory flexibilities to adopt the very best practices in each area of its business.
3. Be a center of excellence for dynamic, multifaceted technologies, platforms, applications, and cyber security compliance.
4. Adopt effective communications with internal and external stakeholders.
5. Employ technology operations that reduce redundancies across the organization to achieve cost savings and improve agility.
6. Drive collaboration between the federal government, industry, and academia to improve the nation's health.
7. Expertly manage the portfolio to rapidly deliver capabilities across the organization.

8. Recruit high-performing, innovative personnel who are accountable to the organization's mission by making PEO DHMS an employer and business partner of choice.
9. Follow efficient and accountable processes that support corporate operations and audit readiness.

SECTION II

2.0 IDIQ CONTRACT SCOPE

2.1 Scope

PEO DHMS defines Workforce 3.0 as a self-driven, high-agency talent pool focused on actively enabling PEO DHMS to achieve its strategic vision and the strategic vision of its subordinate organizations. These ambitions must be achieved while continuously and incrementally transforming PEO DHMS into a high-achieving technology organization that can deliver world-class technology. Workforce 3.0 will be a seamless, badge-less team working in concert to achieve the goals necessary to deliver the PEO DHMS vision. The Workforce will include Government employees and military personnel fulfilling inherently governmental functions, providing strategic direction, performance management, and stakeholder engagement. However, Government personnel cannot deliver all capabilities necessary to operate and transform a high-achieving technology company. This contract will form the relationships with industry necessary to deliver those capabilities; subject matter expertise; and related studies, assessments, plans, and models.

The Government considers a managed solution to cover the full breadth of digital workforce capabilities from technical, administrative, and organizational, across its subordinate and full partner organizations (e.g., the Federal Electronic Health Record Modernization (FERHM) office, the United States Coast Guard, DHA Health Informatics, etc.). In this manner, a managed solution will enable one seamless workforce where an individual's Agency or employment status does not affect the individual's experience at work and where this condition can easily scale and accommodate fluctuations in demand rapidly. It is an actively managed "stack" of capabilities, where the burden does not fall on the Government to execute tactical actions, perform all critical thinking, or specify labor requirements. Additionally, the managed solution must be capable of rapid evolution as the needs of the workforce or cutting-edge technology and capabilities evolve. The overarching outcome desired by PEO DHMS of this effort is that the Workforce will have the same capabilities and talent of a leading-edge technology firm. PEO DHMS will measure the results of contract performance against the extent to which this outcome is satisfied, considering the strategic goals being pursued by its organizations. It is critically important to emphasize that for PEO DHMS to attract/retain the caliber of workforce it requires; solutions should include the full "stack" of capabilities and innovative teaming arrangements. Workforce solutions should ensure the "stack" contains the most cutting-edge private-sector ideas and methodologies throughout.

Contract Types: Task Orders shall be Firm Fixed Price (FFP)

2.2 Lot Definitions

WF3 consists of two (2) Task Order lots covering differing aspects of the transformation. The SF-1449 specifies to which Lot each awardee is assigned, and each prime awardee is assigned to only one of the two Lots.

Awardees **cannot** propose on Task Order Fair Opportunity competitions in a lot to which they are not assigned. A prime contractor from Lot 1 may not perform as a subcontractor on Lot 2.

2.2.1 Lot 1

Lot 1 consists of Task Orders necessary to establish one, seamless team accountable for achieving the specified transformation and growth metrics over a specified length of time to be continuously evaluated against the overarching outcomes specified in Paragraph 1.3. This Lot includes the work necessary to ensure that all functions necessary for operation of the "world class technology" organization are performed in accordance with the agreed upon designs. Lot 1 awardees are accountable to the overall delivery of the new workforce paradigm.

2.2.2 Lot 2

Lot 2 awardees will perform the work necessary to solve finite, specific projects that cover the full spectrum of complexity and difficulty, and may result in the delivery of events, reports, studies, processes, or operations. Rather than focusing on the full breadth of transformation and operation over a specified duration, and on an annual basis like Lot 1, Lot 2 orders will identify one or more specific problems to be solved over flexible durations, when they are identified. Lot 2 orders may independently supplement the functions and transformation activities occurring in Lot 1 from time-to-time. It is expected that more than one Lot 2 order will be active, solving their respective problems, at any given time.

2.3 Responsibilities

2.3.1 Contracting Officer (CO)

The CO is responsible for the award, administration, and management of the IDIQ contract and any solicitations, source selections, Task Orders and Task Order modifications utilizing the Workforce 3.0 IDIQ contract.

- Proactively partners with, maintains, and manages relationship with contractors, especially on higher-vis/prime mission efforts
- Provides advice and guidance to appointed Contracting Officer Representative (CORs), senior leaders, and WF3 primary contract holders regarding all WF3 related matters
- Understands execution of WF3 operational and transformational activities and maintain readiness to satisfy business needs
- Provides direction, oversees changes, and referees all WF3 related issues
- Product manager for contracting products (e.g., RFPs, Source Selections), including reporting status/risk/schedule for contracting events
- Provides final decisions on contract matters in coordination with leadership
- Coordinates/approves public communications about contracting matters
- Appoints and terminates all CORs utilizing WF3 and provides contract specific training to all appointed CORs
- Determines if/when Ad-Hoc Task Orders are necessary

2.3.2 Government Board of Directors

The Government BoD consists of executive leaders to include but not limited to the PEO Director and Director of Contracting.

- The BoD will meet at the Government discretion no less than quarterly
- Ensures WF3 transformational activities remain in alignment with overall PEO 3.0 Strategy
- Approves proposed transformation designs
- Provides advice, guidance, and assistance to the Contracting Officer
- Helps with WF3 issue resolution when elevated, especially when an issue involves more than one product team
- Oversees “Gamechanger” award plan and Incentive evaluation operations

2.3.3 Task Order Contracting Officer Representatives (CORs)

- Monitor and evaluate contractor performance using Quality Assurance Surveillance Plan (QASP) and provide data supporting logical follow-on/Fair Opportunity determinations
- Monitor contractor adherence to PWS and manage deliverables submitted by contractor (i.e., CDRLs)
- Gather and provide periodic reporting of performance to Contracting Officer (as requested)
- Manage and ensure all aspects of compliance (e.g., Government Furnished Property, assets, training, key personnel, etc.)
- Ensure COR reports are uploaded in JAM monthly
- Assist Contracting Officer with CPARs as needed
- Elevate issues to the Contracting Officer when issues cannot be resolved at lowest level
- Onboard and Off-board WF3 contractors (CACs, badges, etc.); if applicable
- Assist with Task Order closeout

2.3.4 Contractors (IDIQ level)

Shall provide point of contact information for the following:

- Contract Specific Issues/Awards/Modifications
- Task Order Proposal Request Inquiries
- Executive Leadership Engagement/Inquiries
- Ask Me Anything Sessions
- Adhere to the proposal procedures for WF3
- Update POC information with the Government
- Report any issues to COR and Contracting Officer (as required)

SECTION III

3.0 IDIQ-Wide Requirements

3.1 Place of performance

Virtual work is strongly encouraged; fixed Government facilities will not be available for day-to-day or collaboration work, and fixed or dedicated contractor facilities for day-to-day work are not required, but the contractor may provide physical collaboration space from time-to-time for shared contractor/Government use.

3.1.1 Travel

The Government strongly encourages virtual work, but when and if the Government and industry partners agree travel will provide value, the Government may, at its discretion, authorize travel consistent with the substantive provisions of the Joint Travel Regulation and the limitation of funds specified in this contract. All travel requires Government approval/authorization and notification to the Contracting Officer Representative (COR).

3.2 Recognized Federal holidays

WF3 industry partners are not required to perform services on the following holidays:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

3.3 Hours of operation

Fixed work hours are not required. The contractor is responsible for assuring that workers are available to support planned activities, respond to emergent urgent requirements, achieve agreed levels of service, and to reach agreed outcomes and deadlines.

3.4 Contract Operations Staff

Lot 1 and Lot 2 contractors shall provide a list of two points of contact that delineates responsibility by function and assure that this staff is available during the Government's normal working hours and within 1-hour after hours or on holidays.

3.5 Personal Conduct

Industry partners shall adhere to the same or better standards of conduct required of government employees per direction of the DHA Commander.

3.6 Culture

Traditional workplace culture is often rooted in hierarchy and relies on authoritative communication styles and strict policies (e.g., set working hours, formal dress code, inflexible work arrangements). The Government believes it is of benefit to replace this model with a new, modern workplace culture. Modern workplace cultures engage employees in open dialogue, inspire them to think creatively, trust them to manage their work schedules with autonomy and empower them to collaborate to reach business decisions. Most importantly, as stated in Section II, "the overarching outcome desired by PEO DHMS of this effort is that the Workforce will have the same capabilities and talent of a leading-edge technology firm." In order to compete for this talent and effectively manage such capability, a modern working culture is required.

Industry partners are expected to spearhead organizational and cultural change management efforts across the PEO DHMS enterprise. To this end, the industry partner must not only execute strategic initiatives to achieve this outcome but must also instill and practice the core tenets of modern workplace conduct within its own staff members. Tactically, the Government anticipates the following attributes at a minimum:

- Managing employee well-being and actively mitigating burn-out potential and retention risk amongst staff members,
- Embracing technology that enables flexible work arrangements to allow employees to get work done from

almost anywhere,

- Fostering a culture of professional development and personal growth,
- Encouraging open two-way communication without negative repercussions for honest feedback,
- Discouraging inconsistent treatment of employees based on being physically present versus being digitally present,
- Upholding diversity, equity, and inclusiveness as a key strategic priority,
- Promoting a badge-less, seamless structure that does not discriminate staff based on their corporate alignment,
- Fostering curiosity and the pursuit of innovation in both functional and technical endeavors,

The Government believes these attributes are necessary and justified for achieving a successful, enduring digital transformation. Industry partners cannot merely enact such changes amongst Government personnel; these changes must be reflected in the Industry partner's own organization. When organizations have cultures grounded in holistic wellness, employees perform better and are more resilient in challenging times. When employees can adequately care for their needs, they can handle conflict at work with more clarity, resolve and positivity.

3.7 Standards of Practice

In lieu of traditional Quality Control (QC) and Quality Assurance, the Government and industry partners will agree to: 1) a set of targeted strategic outcomes and associated objective measures of effectiveness, and; 2) method for verifying and documenting level of achievement, specific to that Task Order. Achievement of minimum agreed targets shall define satisfactory performance. Exceeding minimum targets shall serve as the basis for awarding incentive and/or "gamechanger" compensation in accordance with the Addendum to FAR Clause 52.212-4. These metrics will also be utilized to evaluate past performance and whether the efficiency and effectiveness logical follow-on Fair Opportunity exemption may apply.

3.8 Common Access Card (CAC)

The CAC is standard identification for eligible DoD industry partners. As required, each WF3 worker shall provide to the Government all information required per the DHA CAC request process, current version 2.1, January 2018, or more recent when updated. See attached instructions.

3.9 Training

Industry partners shall complete all requirements, training, and forms per the DHA's Onboarding Checklist for Contractor Employees, current edition February 2018 or more recent when updated. See the form at https://info.health.mil/sites/DOP/OnboardingCtr/Contractor_OnBoarding_Checklist.pdf.

3.10 Physical Security

Industry partners shall safeguard all Government equipment, information and property provided by Government for their use.

3.11 Manpower Reporting

WF3 industry partners who receive Task Orders of $3M or more shall report "contractor manpower" (including subcontractor manpower) via the Office of the Secretary of Defense (OSD) Personnel and Readiness (P&R) secure data collection site at http://www.ecmra.mil/. As part of its submission, WF3 industry partners shall provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period shall be the period of performance not to exceed 12 months ending September 30 of each government fiscal year and must be reported by 31 October of each calendar year. Report via either Extensible Markup Language (XML) data transfer to the database server, or fill in the fields on the website. Direct questions to the help desk at: http://www.ecmra.mil/.

3.12 Non-Disclosure Agreement (NDA)

WF3 industry partners who will obtain access to proprietary, classified, or confidential information or any information release of which is protected or governed by law or regulation associated with DHA acquisitions shall complete and sign an NDA prior to beginning work. WF3 partners shall execute an NDA on behalf of their companies, and shall ensure that all staff assigned to, including all subcontractors and consultants execute an NDA protecting the procurement sensitive information of the Government and the proprietary information of other contractors. WF3 industry partners shall execute NDAs not later than first day of employment and renew them upon

exercising a contract option period. Assignment of staff who have not executed this statement, or failure to adhere to this statement, shall constitute default on the part of the industry partner. Industry partners shall maintain originally signed NDAs of individual employees and provide copies to the COR.

3.13 Post award conference/periodic progress meetings

When directed by the Government, WF3 industry partners shall attend a post-award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. These meetings shall be at no additional cost to the Government.

3.14 Government furnished, property, equipment and services

The Government will not furnish property, equipment or services.

3.15 Contractor furnished supplies and services

The Contractor shall furnish all supplies, equipment, facilities and services required to execute any awarded Task Order.

3.16 General Requirements Overview

Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws. This Section addresses the Contractor's requirements under The Privacy Act of 1974 (Privacy Act), The Freedom of Information Act (FOIA), and The Health Insurance Portability and Accountability Act (HIPAA) as set forth in applicable statutes, implementing regulations and Department of Defense (DoD) issuances. In general, the Contractor shall comply with the specific requirements set forth in this Section and elsewhere in this Contract. The Contractor shall also comply with requirements relating to records management as described herein.

3.16.1. DTIC

This Contract incorporates by reference the federal regulations and DoD issuances referred to in this Section. If any authority is amended or replaced, the changed requirement is effective when it is incorporated under contract change procedures. Where a federal regulation and any DoD issuance govern the same subject matter, the Contractor shall first follow the more specific DoD implementation unless the DoD issuance does not address or is unclear on that matter. DoD issuances are available at http://www.dtic.mil/whs/directives. For purposes of this Section, the following definitions apply.

3.16.1.1

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDI 5400.11, DoD Privacy and Civil Liberties Programs, January 29, 2019 and DoDI 5400.11- R, Department of Defense Privacy Program, May 14, 2007.

3.16.1.2

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 Code of Federal Regulations (CFR) Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-E (Enforcement), as amended. Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this Section and are not included in the term HIPAA Rules.

3.16.1.3

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances are DoDM 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, DoDI 6025.18, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs, March 13, 2019, and DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs, August. 12, 2015.

3.16.1.4

Defense Health Agency (DHA) Privacy Office is the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA.

3.17 Records Management.

When creating and maintaining official government records, the Contractor shall comply with all federal requirements established by 44 United States Code (U.S.C.) Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management. The Contractor shall also comply with DoD Administrative Instruction No. 15 (DoD AI-15), "OSD Records and Information Management Program" (May 3, 2013) and Records Management requirements outlined in the current TRICARE Operations Manual (TOM).

3.18 Freedom of Information Act (FOIA)

The Contractor shall comply with the following procedures if it receives a FOIA request and immediately contact the DHA FOIA Officer for evaluation/action.

3.18.1 DHA FOIA

The Contractor shall inform beneficiaries that DHA FOIA procedures require a written request preferably sent via the National FOIA Portal at: www.FOIA.gov. However, requesters may also submit requests via email at DHA.FOIA@mail.mil; or via postal delivery addressed to the DHA Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042-5101. All FOIA requests shall describe the desired record as completely as possible to facilitate its retrieval from files and to reduce search fees which may be borne by the requestor. Contract and/or Modification numbers must be included in all FOIA requests seeking DHA procurement records. Although the administrative time limit to grant or deny a request (ten working days after receipt) does not begin until the request is received by DHA, the Contractor shall act as quickly as possible and respond to DHA within ten working days.

3.18.2 Requests

In response to requests received by the Contractor for the release of information, unclassified information, documents and forms which were previously provided to the public as part of routine services shall continue to be made available in accordance with previously established criteria. All other requests from the public for release of DHA records and, specifically, all requests that reference FOIA shall be immediately forwarded to DHA, ATTENTION: Freedom of Information Officer, for appropriate action. Direct contact, including interim replies, between TRICARE contractors and such requestors is not authorized. The Contractor shall process requests by individuals for access to records about themselves in accordance with directions from the DHA Freedom of Information Service Center. If such a requestor specifically makes the request under the Privacy Act or does not make clear whether the request is made under FOIA or the Privacy Act, the Contractor shall process the request in accordance with directions from the DHA Privacy Office. If requestor specifically seeks PHI under HIPAA, the Contractor shall follow paragraph 3.23, relating to individual rights of access to PHI.

3.19 Systems of Records

In order to meet the requirements of the Privacy Act and the DoD Privacy Act Issuances, the Contractor shall identify to the DHA Contracting Officer (CO) systems of records that are or will be maintained or operated for DHA where records of PII collected from individuals are maintained and specifically retrieved using a personal identifier. Upon identification of such systems to the CO, and prior to the lawful operation of such systems, the Contractor shall coordinate with the DHA Privacy Office to complete systems of records notices (SORNs) for submission and publication in the Federal Register as coordinated by the Defense Privacy, Civil Liberties, and Transparency Division, and as required by the DoD Privacy Act Issuances.

3.19.1 SORN

Following proper SORN publication and Government confirmation of Contractor authority to operate the applicable system(s), the Contractor shall also comply with the additional systems of records and SORN guidance, in coordination with the DHA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by the DoD Privacy Act Issuances, Office of Management and Budget (OMB) Memorandum 99-05, Attachment B, OMB Circular A-130, and Privacy Act of 1974 requirements applicable to contractors operating systems of records on behalf of federal agencies. The Contractor shall promptly advise the DHA Privacy Office of changes in systems of records or their use that may require a change in the SORN.

3.20 Privacy Impact Assessment (PIA)

If DHA data is stored on a Contractor owned system, a PIA is required from the Contractor.

3.21 Data Sharing Agreement (DSA)

Applies if contract requirements involve the use of DHA data (including PII/PHI, a limited data set, or de-identified data. The Contractor shall consult with the DHA Privacy Office to determine if the Contractor must obtain a DSA or Data Use Agreement (DUA), when DHA data will be accessed, used, disclosed or stored, to perform the requirements of this Contract.

3.22 DSA/DUA

The Contractor shall comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and DoD HIPAA Issuances. Likewise, the Contractor shall comply with the DoD Privacy Act Issuances.

3.23 PHI

Prior to using any data involving PHI for research purposes, as defined by HIPAA, the Contractor must gain approval from the DHA Privacy Board. Thus, the Contractor shall comply with DHA Privacy Board requests for additional documentation.

3.24 DSA Requests

To begin the DSA request process, the Contractor shall submit a DSA Application (DSAA) to the DHA Privacy Office. Upon approval, the requestor shall enter into one of the following agreements, depending on the data involved:

- DSA for De-Identified Data • DSA for PHI
- DSA for PII Without PHI
- DUA for Limited Data Set

3.25 DSA Expiration

DSAs executed for contract support will expire after 1 year or at the end of the contract option year, whichever comes first. If the contractual use of DHA data will continue after the DSA expiration date, the Contractor shall submit a DSA Renewal Request template to the Privacy Office; however, if the DSA will not be renewed, the Contractor shall close the DSA by providing a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

3.26 Privacy Act and HIPAA Training

The Contractor shall ensure that its entire staff, including subcontractors and consultants that perform work on this Contract receive training on the Privacy Act, HIPAA, and the federal regulations on confidentiality of substance use disorder patient records, 42 CFR Part 2. Refer to FAR 52.224-3 regarding specific requirements for Privacy Training appropriate to the Contractor's scope of involvement with DHA's PHI and its regulatory responsibilities as either a Covered Entity, or Business Associate. The Contractor shall ensure all employees and subcontractors supply a certificate of all training completion to the Contracting Officer's Representative (COR) within 30 days of being assigned and on an annual basis based on the trainee's birth month thereafter.

3.27 HIPAA Business Associate Provisions

3.27.1 Business Associate – General Provisions

The Contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business Associate Agreement (BAA) between the Contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. The contractor shall use the DoD BAA, which shall be used by all organizational entities within the DoD, referred to collectively as the "DoD Components", located at, https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language/HIPAA-Compliant-Business-Associate-Agreement-for-the-MHS.

3.28 Breach Response

Definitions Related to Breach response.

3.28.1 Breach

Breach means a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII; or (2) an

authorized user accesses or potentially accesses PII for an other than authorized purpose. The foregoing definition is based on the definition of breach in DoDM 6025.18. Breaches are classified as either possible or confirmed (see the following two definitions) and as either cyber or non-cyber (i.e., involving either electronic PII/PHI or paper/oral PII/PHI).

3.28.2 Possible Breach

A possible breach is an incident where the possibility of unauthorized access is suspected (or should be suspected) and has not been ruled out. For example, if a laptop containing PII/PHI is lost, and the contractor does not initially know whether or not the PII/PHI was encrypted, then the incident must initially be classified as a possible breach, because it is impossible to rule out the possibility of unauthorized access to the PII/PHI. In contrast, that possibility can be ruled out immediately, and a possible breach has not occurred, when misdirected postal mail is returned unopened in its original packaging. However, if the intended recipient informs the contractor that an expected package has not been received, then a possible breach exists until and unless the unopened package is returned to the contractor. In determining whether unauthorized access should be suspected, the contractor shall consider at least the following factors:

- How the event was discovered;
- Did the information stay within the covered entity's control;
- Was the information accessed/viewed; and
- Ability to ensure containment (e.g., recovered, destroyed, or deleted).

3.28.3 Confirmed Breach

A confirmed breach is an incident in which it is known that unauthorized access could occur. For example, if a laptop containing PII/PHI is lost and the contractor knows that the PII/PHI is unencrypted, then the contractor should classify and report the incident as a confirmed breach, because unauthorized access could occur due to the lack of encryption (the contractor knows this even without knowing whether or not unauthorized access to the PII/PHI has actually occurred). If the laptop is subsequently recovered and forensic investigation reveals that files containing PII/PHI were never accessed, then the possibility of unauthorized access can be ruled out, and the contractor should re-classify the incident as a non-breach incident.

3.28.4 HHS Breach

A HHS breach is an incident that satisfies the definition of breach in Section 164.402 of the HIPAA Breach Rule. The text of the HHS definition states:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part [i.e. the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.

3.28.5 HHS Breach Exclusions

HHS breach excludes:

3.28.5.1

Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a DoD covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

3.28.5.2

Any inadvertent disclosure by a person who is authorized to access PHI at a DoD covered entity or business associate to another person authorized to access PHI at the same DoD covered entity or business associate, or organized health care arrangement in which the DoD covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted the HIPAA Privacy Rule.

3.28.5.3

A disclosure of PHI where a DoD covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. Except as provided in this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under this

issuance is presumed to be a breach unless the DoD covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

3.28.6 Cybersecurity Breach

A cybersecurity incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, with respect to electronic PII/PHI. A cybersecurity incident may or may not involve a breach of PII/PHI. For example, a malware infection would be a possible breach if it could cause unauthorized access to PII/PHI. However, if the malware only affects data integrity or availability (not confidentiality), then a non-breach cybersecurity incident has occurred.

3.28.7 General

3.28.7.1

The breach response requirements shall be followed for all unauthorized use or disclosure of information regardless of whether the information is PHI or solely PII.

3.28.7.2

Because DoD defines "breach" to include possible (suspected), as well as actual (confirmed) breaches, the Contractor shall implement these breach response requirements immediately upon the Contractor's discovery of a possible breach. These procedures focus on the first two steps (breach identification and reporting) of a comprehensive breach response program, but also require addressing the remaining steps: containment, mitigation (which includes individual notification), eradication, recovery, and follow-up.

3.28.7.3

The contractor shall establish internal processes for carrying out the procedures set forth below. These processes shall assign responsibility for investigating, classifying, reporting and otherwise responding to breaches and cybersecurity incidents. The contractor should consult with the DHA Privacy Office where guidance is needed, such as when the contractor is uncertain whether a discovered breach is the contractor's responsibility (e.g., if the contractor discovers a breach not caused by the contractor), or how the contractor is to classify an incident (breach vs. non-breach, confirmed vs. possible, cyber vs. non-cyber). Under no circumstances will a contractor delay reporting a confirmed or possible breach to the DHA Privacy Office beyond the 24-hour deadline. In conjunction with its initial investigation, the contractor shall immediately take steps to minimize any impact from the occurrence, proceed with further investigation of any relevant details (such as root causes, vulnerabilities exploited), and initiate further breach response steps.

3.28.7.4

In the event of a cybersecurity incident not involving a PII/PHI breach, the contractor shall follow applicable DoD cybersecurity and NIST requirements, which include United States Computer Emergency Readiness Team (US-CERT) reporting (see paragraph 3.17.12.3) If at any point a contractor finds that a cybersecurity incident involves a PII/PHI breach (possible or confirmed), the contractor shall immediately initiate the reporting procedures set forth below. The contractor shall also continue to follow any required cybersecurity incident response procedures and other applicable DoD cybersecurity requirements.

3.28.7.5

Contractors shall require subcontractors who discover a possible breach or cybersecurity incident to initiate the incident response requirements herein by reporting the incident to the contractor immediately after discovery. The time of that report to the contractor shall trigger the contractor's DHA Privacy Office reporting deadline (24 hours) under paragraph 3.31.2.4. If a cybersecurity incident is involved, the contractor's deadline for US-CERT reporting (1 hour) runs from the time the incident is confirmed. The contractor shall require the subcontractor to cooperate as necessary to meet these deadlines, maintain records, and otherwise enable the contractor to complete the breach

response requirements herein. Alternatively, the contractor and subcontractor may agree that the subcontractor shall report directly to US-CERT and the DHA Privacy Office, and that the subcontractor shall be responsible for completing the response process, provided that such agreement requires the subcontractor to inform the contractor of the incident and the subsequent response actions.

3.28.7.6

Contractors shall maintain records of all breach and cybersecurity incident investigations, regardless of the outcome. Investigations identifying unauthorized disclosures must be logged for HIPAA and Privacy Act disclosure accounting purposes, whether or not individual notification is required under the HIPAA Breach Rule.
W

3.28.7.7

Contractors, when acting as HIPAA-covered entities, and not as business associates, are not subject to the breach response requirements herein. However, such contractors are subject to both the HIPAA Breach Rule (applicable to them in their capacity as covered entities) and DoD cybersecurity requirements (applicable to them in their capacity as DoD contractors).

3.28.8 Reporting Provisions

3.28.8.1

Immediately upon discovery of a possible or confirmed breach or cybersecurity incident, the contractor shall initiate an investigation. If the incident involves electronic PII/PHI, and if the investigation finds a confirmed breach or cybersecurity incident, the contractor shall report it, within 1 hour of confirmation, to the US-CERT Incident Reporting System at https://forms.uscert.gov/report/, as required by the Department of Homeland Security (DHS).

Note: DHS no longer requires US-CERT reporting of non-cyber breaches or unconfirmed electronic breaches. However, DHS permits US-CERT reporting of unconfirmed cyber-related incidents on a voluntary basis. Thus, if a contractor is uncertain whether a possible cyber-related incident should be treated as confirmed and thus reportable, the contractor may voluntarily report the incident.

3.28.8.2

Before submission to US-CERT, the contractor shall save a copy of the on-line report. After submitting the report, the contractor shall record the US-CERT incident reporting number, which shall be included in the initial report to the DHA Privacy Office as described in paragraph 3.31.2.4.

Note: Regardless of whether or not an incident is confirmed as a breach, the contractor must also investigate whether or not the incident impacts data integrity or availability of PII/PHI. If such impact is confirmed, then the incident is reportable to US-CERT as a cybersecurity incident. For guidance on investigating the impact on data integrity and availability, refer to DoD cybersecurity and NIST guidance.

3.28.8.3

The contractor shall provide any updates to the initial US-CERT report by email to soc@uscert.gov, with the Reporting Number in the subject line. The contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office if requested. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

3.28.8.4

In addition to US-CERT reporting, the contractor shall report to the DHA Privacy Office by submitting the form specified below within 24 hours of discovery of a breach (possible or confirmed), unless the breach falls within a category that the Privacy Office has determined to be not reportable. This 24-hour period runs from the time of discovery, unlike the 1 hour USCERT reporting period, which runs from the time a cybersecurity incident is confirmed. Thus, depending on the time period needed to confirm, the report to the DHA Privacy Office may be due either before or after the US-CERT report.

3.28.8.5

The breach report form required within the 24-hour deadline shall be sent by e-mail to: DHA.PrivacyOfficer@mail.mil. The contractor shall also e-mail the report to the CO, the COR and its usual point of contact at the applicable Program Office. Encryption is not required, because reports and notices shall not contain

PII/PHI. If electronic mail is not available, telephone notification is also acceptable (at 703-275-6363), but all notifications and reports delivered telephonically must be confirmed in writing as soon as technically feasible.

3.28.8.6

Contractors shall prepare the breach reports required within the 24-hour deadline by completing the Breach Reporting Department of Defense Form DD 2959 (Breach of PII Report), available at https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2959.pdf. For non-cyber incidents without a US-CERT number, the contractor shall assign an internal tracking number and include that number in Box 1.e of the DD Form 2959. The contractor shall coordinate with the DHA Privacy Office for subsequent action, such as beneficiary notification, and mitigation. The contractor must promptly update the DD Form 2959 as new information becomes available.

3.28.8.7

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Contractor shall submit a revised form or forms promptly after the new information becomes available, stating the updated status and previous report date(s) and showing any revisions or additions in red text. The Contractor shall provide updates to the same parties as required for the initial Breach Report Form.

3.28.9 Individual Notification Provisions

3.28.9.1

If the DHA Privacy Office determines that individual notification is required, the Contractor shall provide written notification to beneficiaries affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities and addresses of the beneficiaries are ascertained. The 10-day period begins when the Contractor is able to determine the identities (including addresses) of the beneficiaries whose records were impacted. If notification cannot be accomplished within 10 working days, the contractor shall notify the DHA Privacy Office.

3.28.9.2

The Contractor's proposed notification to be issued to the affected beneficiaries shall be submitted to the DHA Privacy Office for approval. The notification to beneficiaries shall include, at a minimum, the following:

- Specific data elements,
- Basic facts and circumstances,
- Recommended precautions the beneficiary can take,
- Federal Trade Commission (FTC) identity theft hotline information, and
- Any mitigation support services offered, such as credit monitoring.

3.28.9.3

Contractors shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the Contractor and/or subcontractor organization that suffered the breach.

3.28.9.4

If media notice is required, the contractor will submit a proposed notice and suggested media outlets for the DHA Privacy Office review and approval (which will include coordination with the DHA Communications Division).

3.28.9.5

In the event the Contractor is uncertain on how to apply the above requirements, the Contractor shall consult with the CO, who will consult with the Privacy Office as appropriate when determinations on applying the above requirements are needed.

3.28.9.6

The Contractor shall, at no cost to the Government, bear any costs associated with a breach of PII/PHI that the Contractor has caused or is otherwise responsible for addressing

3.28.10 Training and certification

Contractor employees performing cybersecurity / cyberspace functions shall comply with the following requirements:

3.28.10.1

All contractor and associated subcontractor employees working Cybersecurity (Information Assurance (IA))/Cyberspace functions must comply with DoD training requirements in Department of Defense Directive (DoDD) 8140.01, and DoD 8570.01-M.

3.28.10.2

Per DoDD 8140.01, Defense Federal Acquisition Regulation Supplement (DFARS) 252.239-7001, contractor employees supporting Cybersecurity (Information Assurance)/Cyberspace functions shall be appropriately certified upon contract/Task Order award. The baseline certification as stipulated in DoD 8570.01-M must be completed prior to the beginning of their contract support services. In addition, the contractor shall comply with Computing Environment (CE) certification requirements as specified in the contract. CE certifications shall be obtained within the timelines specified in DoD 8570.01-M.

3.28.10.3

All contractor employees with privileged user status must comply with the requirements of DHA-Administrative Instruction (AI) 081, Employee use of Information Technology.

SECTION IV

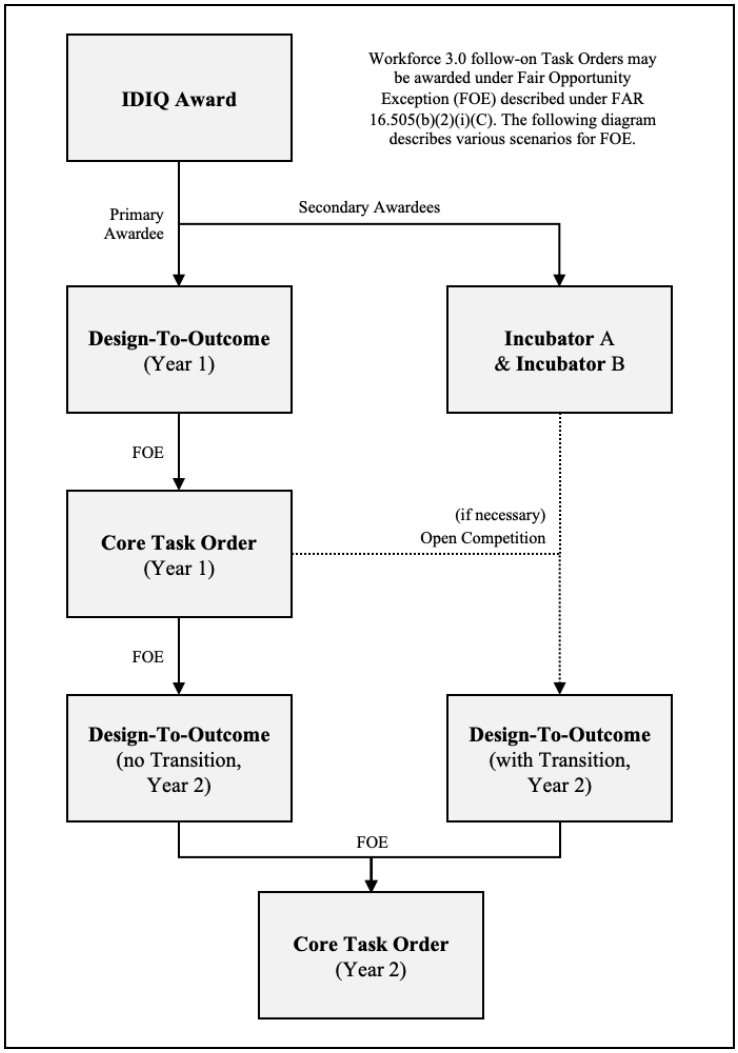
TASK ORDER RULES OF ENGAGEMENT

This section governs the issuance of orders on the WF3 contract. It explains the process that will be used when awarding each Task Order.

This is a centralized multi-award IDIQ, with two Lots. Orders under Lot 1may be set-aside if sufficient small business primes are available within the pool. Orders under Lot 2 will be exclusively set-aside for small business, and may be further set-aside for sub-socioeconomic categories if applicable. Awardees may only submit against Fair Opportunity solicitations for the Lot they are assigned.

Competition and Exception to Fair Opportunity

In accordance with FAR 16.505(b)(2)(i)(C), if a Task Order is a follow-on or continuation of a previously competed Task Order, then award may be given to the previously awarded contractor on the basis of a justification prepared pursuant to FAR 16.505(b)(2)(ii)(B). After award of the first Task Order, at the Government's sole discretion Task Orders may be awarded based on an exception to Fair Opportunity. The diagram below describes potential scenarios for Task Orders.



4.1 Lot 1

4.1.1 Restrictions and minimums associated with Task Orders

The first Design-to-Outcome Task Order is awarded during the initial IDIQ source selection. IDIQ awardees not selected as part of that Fair Opportunity were awarded "Incubator" Task Orders to satisfy the minimum guarantee. The contract contemplates common and frequent usage of two primary circumstances when an exception to Fair Opportunity may be used.

4.1.2 Lot 1 Linked Design-to-Outcome Task Orders

There will be up to a total of six Lot 1 Task Order cycles. Each cycle will consist of an initial Design-to-Outcome Task Order with the potential for a logical follow-on for a Core Task Order to execute the design delivered in the Design-to-Outcome Task Order, if the conditions of the Fair Opportunity exemptions are satisfied. The purpose of the Design-to-Outcome Task Order is to allow the awardee to observe, plan and propose a set of activities that measurably contribute to targeted transformational outcomes for DHMS mid- and back-office functions. It is during the Design-to-Outcome order that the objectives, outcomes, and measures for the Core Task Order are negotiated and agreed upon with the Government. A logical follow-on Core Task Order may then be awarded to that same Offeror to execute against the proposal. This Core Task Order will ensure coverage of core capabilities, continuation of services, and setting a foundation to steadily execute the organizational digital transformation.

If the Government cannot reach an agreement with the Offeror on the initial Design-to-Outcome Task Order, a Fair Opportunity competition may be conducted with the other Lot 1 awardees at the Government's discretion.

4.1.3 Performance Assessment

PEO DHMS will conduct ongoing performance monitoring for Offeror Core Task Orders. After the fifth month of performance of each Lot 1 Core Task Order, PEO DHMS will assess the overall performance of the contractor against the performance metrics that were agreed upon for that particular Task Order at the completion of the linked Design to Outcome task order. If, based on this assessment, PEO DHMS determines that the contractor's performance meets or exceeds all performance metrics, then PEO DHMS will have a strong basis to develop a justification for using the logical follow-on exception to the Fair Opportunity process, in the interests of "economy and efficiency," for the next cycle of Task Orders (linked Design to Outcome and Core); however, regardless of the contractor's level of performance, PEO DHMS will conduct the necessary analysis under FAR 16.505(b)(2)(ii)(B) before using the logical follow-on exception and will always retain the option to compete the next cycle of Task Orders amongst the pool of Workforce 3.0 awardees. The Government will seek to complete its determination regarding how to proceed with next cycle Task orders within one month of performance assessment in order to maintain continuity of the WF3 task order cycles. Offerors will be notified as soon as the determination is finalized. This cycle of linked Task Orders and mid-point performance assessment will repeat itself throughout each ordering period of Workforce 3.0. The intent is to be iterative and to constantly assess and evolve PEO DHMS.

4.1.4 Continuation of Lot 1 work when successful

As part of DTO Task Order performance, the awardee and the Government shall negotiate and agree to a set of performance metrics tied to successfully achieving value at PEO DHMS. These metrics provide a long-term benchmark on the progress of the PEO 3.0 digital transformation. The Government shall assess the awardee's progress against these metrics using methods including but not limited to awardee self-reporting, Government direct measurements, sampled measurements, and systematic measurements. If the awardee meets performance to a sufficient level determined by the Government BoD, PEO DHMS may use a logical follow-on (exception to the Fair Opportunity process) for the next cycle of Lot 1 Task Orders if it can establish (consistent with the requirements of FAR 16.505(b)(2)(ii)(B)) that the value achieved against the agreed metrics, taken into account with other necessary factors, satisfies the "in the interests of economy and efficiency" standard under FAR 16.505(b)(2)(i)(C). In such cases, the awardee will then be granted another Design-to-Outcome Task Order to design, plan, and negotiate the objectives, outcomes, and measures for the next Core Task Order.

4.1.5 Fair Opportunity when Lot 1 work is not successful

If the awardee's performance of the Lot 1 work is "not successful," then there likely will be little basis for the Government to determine that any subsequent orders under the contract constitute logical follow-ons to the unsuccessful work. In such circumstances, PEO DHMS will initiate the Fair Opportunity process amongst Workforce 3.0 IDIQ Lot 1 participants for the next DTO Task Order. The Government shall provide Fair

Opportunity details in an RFP once a decision to utilize the Fair Opportunity process is made. The active Offeror shall be tasked with maintaining continuity of services for the current Core Task Order and ensure proper handoff as part of its remaining performant responsibilities.

4.1.6 On Ramping

Additional awardee(s) may be on-ramped onto the Lot 1 IDIQ in the event such actions are in the best interest of the Government, to be determined unilaterally at the discretion of the Contracting Officer in consultation with the Board of Directors.

4.2 Lot 2

4.2.1 Restrictions and minimums associated with Task Orders

Lot 2 awardees will receive one Accelerator Task Order each to cover contract kick off and other administrative functions. These orders will satisfy the "minimum guarantee".

4.2.2 Lot 2 linked Task Orders

The Government will issue these Task Orders on an as-needed basis to address special projects, and the period of performance of such projects will be determined during the associated Accelerator Task Order. Each Lot 2 project will consist of an initial Accelerator Task Order with a linked logical follow-on ad-hoc Task Order, which may be issued if performance under the linked Accelerator Task Order satisfies the exception to Fair Opportunity. During the Accelerator Task Order, the contractor will assess the provided problem statement and prepare a detailed Design-to-Outcome approach and proposal for the award of the follow-on ad-hoc Task Order to successfully address the stated problem. A logical follow-on ad-hoc Task Order will then be awarded to that same Offeror to execute against the proposal. Depending on the nature of the problem statement, the Government may award more than one Accelerator during the Fair Opportunity phase and more than one logical follow-on Task Order if multiple Accelerator solutions have sufficient merit and value.

4.2.3 Off Ramping

If an awardee fails to respond to over 75% of eligible opportunities issued across the four (4) most recent Task Order solicitations issued under the Lot 2 IDIQ and does not provide sufficient "no bid" rationale, the awardee will be off ramped (removed) from the IDIQ, will no longer be able to propose on future Task Order solicitations.

4.2.4 On Ramping

Additional awardee(s) will be on-ramped onto the IDIQ if there are fewer than two (2) average bidders across the four (4) most recent Task Order solicitations issued under the Lot 2 IDIQ. Details on how Offerors will be qualified for on-ramping will be determined upon identification of the need for additional awardee(s).

4.3 Task Order Types/definitions

4.3.1 Lot 1 Task Orders

There are three types of Task Orders within Lot 1.

4.3.1.1 Design-to-Outcome Task Orders

These Task Orders serve as observation, design, planning, and negotiation periods. They allow for preliminary work and cashflow to commence immediately, while providing the Offeror time to assess operations and prepare a detailed outcome-oriented approach for commencing and executing performance on the follow-on Core Task Order. The approach shall include agreed-upon performance metrics to measure performance on the Core Task Order and inform contract profit calculations. **The initial Design-to-Outcome Task Order allows for transition of PEO DHMS mid- and back-office functions to the contractor**, and allows for a longer time period to accommodate the shift of functions and ensure no gap in coverage of operational activities. The remaining Design-to-Outcome Task Orders will be shorter as transition will have already occurred, unless the government deems the contractor has failed to meet metrics and decides to compete the next cycle of Task Orders. In such an event, Design-to-Outcome Task Orders may encompass subsequent transitions events.

4.3.1.2 Core Task Order

These Task Orders may be issued as logical follow-ons, based on the terms agreed upon during the Design-to-Outcome Task Orders. **The intent is to transition coverage of Workforce 3.0 core capabilities and operational activities to provide continuation of services for mid and back office functions.** The Offeror will be expected to execute the organizational digital transformation in accordance with the performance metrics and outcomes agreed upon during Design-to-Outcome Task Order 1. In addition, Offerors will be expected to seek innovation opportunities while maintaining baseline capabilities.

4.3.1.3 Incubator Task Orders

These Task Orders are issued to advise on PEO DHMS innovation posture and capability gaps. They will be awarded to Lot 1 Awardees that are not currently awarded and executing on a Core Task Order. The intent is to perform independent surveys of the health technology domain and report on PEO DHMS strengths, opportunities, and blockers as it compares to best-in-class methodologies of health technology.

The table below summarizes the characteristics of Lot 1Task Orders.

Lot 1 Task Orders	Contract Type	Priced At	Ordering*	Award Basis	Duration
Design-to-Outcome (DTO) Task Orders					
DTO1 CLIN 0001	FFP	IDIQ	Unilateral	Fair Opportunity	90 Days
DTO w/o Transition CLINs 0101, 0201, 0301, 0401, 0501	FFP	IDIQ	Unilateral	Potential Exception to Fair Opportunity	60 Days
DTO w/ Transition CLINs 0107, 0207, 0307, 0407, 0507	FFP	IDIQ	Unilateral	Fair Opportunity	90 Days
Core Task Orders (CTO)					
CTO 1-6 CLINs 0002, 0102, 0202, 0302, 0402, 0502	FFP	TO	Bilateral	Exception to Fair Opportunity	11 Months
Incubator Task Orders					
Incubator TO A1-A6 CLINs 0003, 0103, 0203, 0303, 0403, 0503	FFP	IDIQ	Unilateral	Fair Opportunity	60 Days
Incubator TO B1-B6 CLINs 0004, 0104, 0204, 0304, 0404, 0504	FFP	IDIQ	Unilateral	Fair Opportunity	60 Days

*Task orders identified as unilateral may be awarded at the Government's discretion utilizing the pricing incorporated from the original proposal at any time and without notice.

4.3.2 Lot 2 Task Orders

There are two types of Task Orders within Lot 2.

4.3.2.1 Accelerator Task Orders

These Task Orders are issued prior to Ad-Hoc Task Orders. The intent is to provide time to accurately scope and negotiate the terms for the Ad-Hoc Task Order when the need for an Ad-Hoc Task Order is identified. Accelerator Task Orders are linked to Ad-Hoc Task Orders, in that they allow work to begin immediately and will result in an agreed upon expectation for completion of the Ad-Hoc Task Order.

4.3.2.2 Ad-Hoc Task Orders

Task Orders issued to address specific needs, such as short-term projects, limited time access to unusually high subject matter experts, or for targeted studies and reports. These Task Orders will be issued on an as-needed basis and the period of performance will be determined and agreed upon during the Accelerator Task Order.

The table below summarizes the characteristics of Lot 2Task Orders.

Lot 2 Task Orders	Contract Type	Priced At	Ordering*	Award Basis	Duration
Accelerator Task Orders					
CLIN 1001	FFP	IDIQ	Unilateral	Fair Opportunity	30 Days
Ad-Hoc Task Orders					

CLINs 1002	FFP	IDIQ	Bilateral	Potential Exception to Fair Opportunity	TBD

*Task orders identified as unilateral may be awarded at the Government's discretion utilizing the pricing incorporated from the original proposal at any time and without notice.

4.3.3 Task Order Inputs and Outputs

The inputs for the linked design Task Orders for both Lot 1 and Lot 2 are depicted in Table below.

Inputs for Design-to-Outcome and Accelerator Task Orders
PEO DHMS Purpose, Goals, Strategy
2020-2025 Federal Health IT Strategic Plan
PEO 3.0 Strategic Plan
PEO DHMS Desired Outcomes
Maturity Assessments
Attributes/Ideals
User Vignettes/Pain Points
Bounding/Scoping Assumptions

The outputs for Design-To-Outcome and Accelerator Task Orders for both Lot 1 and Lot 2 (respectively) are depicted in the Table below.

Outputs for Core & Ad-hoc Task Orders	Description
PWS	A clearly defined PWS that describes the performance objectives and standards expected of the contractor during the Core Task Order.
Quality Assurance Surveillance Plan (QASP)	Specifies how the contractors will verify and document the metrics and objectives that were agreed upon during the Design-to-Outcome Task Order. The QASP will incorporate the metrics for Core Task Orders.
Contract Data Requirements List (CDRL)	Formally document the deliverables that will be produced during execution of the Task Order
Gamechanger Award Pool Plan Specifications	Agreed upon total pool for Gamechanger award and timing of interim evaluations.
Assertions of restrictions on data rights	See 52.212-4 Addendum X
Pricing	The agreed upon price.
Approved Design/Approach	Design artifacts including outcomes, plans, milestones, and schedules.

The data elements expected as part of the Contractor QASP for both Lot 1 and Lot 2 are depicted in the Table below.

Type	QASP Data Elements	Description of data element
Metric Description	Required Service(s)	Over arching
	PWS Section	List out the PWS sections this service is linked to
	Acceptable Quality Level	Detailed description of the metric to achieve and REMEDY if the metric is not met satisfactorily
	Method of Surveillance	Describe how the Government will be able to analyze the acceptable quality level to ensure the contractor is meeting expectations
Performance Ratings	Unsatisfactory	Measurable performance requirement that will result in an unsatisfactory rating for this specific metric
	Marginal	Measurable performance requirement that will result in a marginal rating for this specific metric
	Satisfactory	Measurable performance requirement that will result in a satisfactory rating for this specific metric

	Very Good	Measurable performance requirement that will result in a very good rating for this specific metric
	Exceptional	Measurable performance requirement that will result in an exceptional rating for this specific metric

The data elements expected as part of the Contractor CDRL for both Lot 1 and Lot 2 are depicted in the Table below.

CDRL Title/Element	Title of the deliverable
Authority (DID)	Identify any data acquisition document number(s) will be used as the basis for the expectation of the data to be delivered as part of this CDRL. If one is not known, annotate "N/A see special instructions"
PWS Reference	Annotate PWS sections this CDRL applies to
Distribution Statement	Distro statement will be Distro D unless otherwise annotated differently by the contract. (see below for Distribution statements)
Deliver frequency	Identify when the first deliverable will be sent to the Government and when subsequent updated deliveries will be sent
Review timeline	(Fill in the blanks). The Government shall have _____ days after receiving the completed CDRL for review and comment. Revised and resubmit the updated CDRL to the Government for approval _____ days after receiving comments. Subsequent submissions are as required until the CDRL is approved.
Special instructions	Special instruction: • If one or more authority data acquisition document is identified as a foundation for this CDRL, describe any tailoring that will be completed (i.e., additional data will be added, or data will not be part of the deliverable). • If there is no authority data acquisition document, provide a description of the data elements that will be part of this deliverable. • Add any additional information in this section that is applicable to this specific CDRL.