

DISA FY18 Contracting Overview

Questions for Douglas Packard

Q1: Regarding DISA Agency Program Support; Does using LPTA for knowledge based, classified work, go against the 2017 NDAA?

A2: The use of LPTA in accordance with the 2017 NDAA was addressed at the Forecast to Industry Day. Because this procurement is in source selection, we're prohibited from commenting.

Q2: Can you talk about the DISA IV and V BPA contract that was awarded in Jan 2017? No task order was issued yet.

A2: Task orders are issued when mission requirements are submitted by mission partners. To date, no requirements have been submitted to the DITCOs.

Q3: DISA follows Agile Management approach a lot. It also follows Risk Management a lot. Both are extremely important for DISA. Yet why isn't DISA's DESS II PWS not mentioned or stress much in those two areas of PWS personnel acquisition? DISA only stressed much about Traditional project management. Therefore the PWS for DESS II is incomplete in my opinion.

A3: You may wish to pose this question directly to the DESS Contracting Officer, Mrs. Adelis Rodriguez adelis.m.rodriguez.civ@mail.mil. Questions and answers are posted in the form of amendments to the DESS solicitation.

Q4: Will DISA be using the OASIS SB IDIQ in the coming year?

A4: While we won't speculate on the use of any particular vehicle, DISA may use OASIS SB for any suitable requirements.

Q5: What internal tool or tools are being used to measure performance of vendors?

A5. For services, measurement is primarily a function of the contract-specific Quality Assurance Surveillance Plan (QASP) plus any applicable Service Level Agreements (SLAs).

Q6: Which contract vehicles are more commonly used for IT Infrastructure (Layer-One) Product only type procurements?

A6. DITCO often uses NASA SEWP, the U. S. Army's Computer Hardware Enterprise Software and Solutions (CHESS), and GSA Schedule 70 for its hardware procurements.

Q7: My question is regarding the support to OCAE RFI that came out over the summer. Will companies that provided responses receive follow-up communication? And will the RFQ be on the street soon?

A7. The PMO is still reviewing responses and conducting market research. No follow-up communications are anticipated. The RFP/RFQ is anticipated to be released 2QFY18.

Q8: Since GSA awarded EIS recently to replace Networx, is there a plan to begin using EIS as Networx is phased out?

A8: Yes. However, all awardees must first receive their Authority to Operate (ATO) for their Business Support Systems according to the terms and conditions of their basic contracts. At that time, all new requirements will be competed on the EIS contracts. DISA will also utilize the EIS contract to transition current Networx requirements once task orders have been awarded and transition plans developed.

Q9: Will a list of attendees be made available?

A9: No. We did not ask for permission to include attendee names in a master list.

Q10: Are the contract vehicles listed on the Procurement Services Executives slides the only contract vehicles DISA will use?

A10: No. The list is not 100% comprehensive. Not all of DISA BPAs and ID/IQs are listed.

Q11: We noticed that many of the opportunities briefed indicated "Full & Open" or "Schedule 70" under "Anticipated Acq. Strategy." We also heard Mr. Packard brief that DISA would use ENCORE III, etc., before using another IDIQ or "Full & Open." These two statements seem contradictory. Does "Full & Open" mean DISA will use ENCORE III non-small IDIQ to limit bidders, or does it mean "open" to all competitors?

A11: Fair opportunity is the means by which contractors on GSA Schedule 70 and IDIQ multiple award type contracts compete for task orders. Full and open competition relates to situations where there is no vehicle in place. Example: Encore III awardees are selected using full and open competition (no restrictions as to business size) or via a small business set-aside; task orders for both suites of contracts will be awarded following fair opportunity procedures. Encore III will figure strongly in subsequent acquisition strategies, but not exclusively.

Other Transaction Authority
Questions for Scott Stewart

Q1: The list of companies on the C5 OTA includes almost all the large traditional defense contractors. Can DISA and your office raise the bar for the big companies using this vehicle? Would you consider requiring large businesses to use both significant Non-Traditional Defense Contractor participation AND contribute 30% of the funding in order to prevent these vehicles from being dominated by large defense contractors?

A1: DISA does not control the C5 consortium and cannot select, add, or remove the contractors currently on the list. The C5 consortium is only one route to issue an OTA; if that list of vendors does not suit a requirement, alternative approaches/solicitation methods can be explored. Several of the on-going DISA OTAs are being worked through the C5 consortium which was a decision made by ACC-NJ. Now that DISA has its own OT authority, we are in a better position to either choose or not choose a consortium approach.

Q2: With new White House IT Modernization directive (EO 13800), calling for rapid embrace of commercial IT innovations like SDN, XaaS, Cloud, how will DISA retool its Innovation Research & Acquisition processes that reach outside the confines of the Defense Industrial Base which accounts for less than two percent of the Global IT Market.

A2: DISA now has authority to enter into OTs. Use of this authority will be another tool in the agency's toolkit to reach commercial IT innovative solutions.

Q3: What are you doing to educate DISA government managers on how to use OTAs?

A3: PSD hosted an Acquisition Excellence Workshop focusing on OTAs and will periodically repeat this offering, and formal classroom training is anticipated in the future. DISA has information (Including an OTA Process Guide and process highlights document) and sample OTA forms/documents.

We recognize the importance of a workforce well-informed on the use of this authority.

Q4: Can you please describe the source selection process used for the GCCS-JE acquisition through the C5 OTA?

A4: We don't have insight into the C5 approach for GCCS-JE, which is being solicited/awarded by the Army Contracting Command – New Jersey.

The standard OTA process is as follows:

1) Release the problem statement and receive "white papers" whereby the company explains their technical approach and its merit.

2) If the white paper is viable/intriguing, presentations are scheduled where the vendor presents more information, and the government asks questions.

3) Based on the presentations, the awardee is selected, and specifics on price, data rights, and the effort/performance are finalized.

As noted during F2I, our process and strategy mirrors the Commercial Solutions Offering (CSO) process pioneered by DIUx.

Development and Business Center Introduction

Questions for Alfred Rivera

Q1: How is DISA helping DOD to better, more rapid data analytics by connecting to disparate data sources to get actionable insights?

A1: DISA formed a Data Brokering Service and an Enterprise Sensing solution that manages the agency-wide ingest and dissemination of relevant data sources. These tailored enterprise data sources are ingested into our Security Information Event Manager (SIEM) and Big Data Platform (BDP) capabilities and made available to the operational community for cyber insights. Based on advice from the intelligence and DoDIN operational communities, and our ingested BDP data, DISA is creating a coordinated, community-wide DevSecOps approach that employs neural networking, machine learning, and other advanced analytics techniques to develop actionable responses to cyber intrusions and attacks. Development will occur on our pre-production environment, allowing earlier identification of anomalous behavior while refining the new capability before promoting to DISA's production SIEM/BDP capabilities. This relentless focus on cyber warfighting and an integrated approach to data sources, sensor ingest, and DevSecOps will increase our production and speed to deployment of required cyber defense capabilities.

Q2: If you had something unique to offer DISA, who do you start with, ex. OSBP, Program Managers, specialty office?

A2: We welcome innovative products and solutions. There are multiple ways to present your unique offering to DISA. Your starting point is our Industry Partners page on DISA.mil (<http://www.disa.mil/About/Industry-Partners>). The page includes links to contact the DISA Office of Small Business Programs, information about how to demonstrate your product to DISA, forms to send an inquiry or request a meeting, and other resources. The DISA Corporate Connections Office routes inquiries and meeting requests to the appropriate DISA organization.

Command & Control

Questions for Terry Carpenter

Q1: How does the recent Army award for UC factor into the DEOS program?

A1: The military services are continuing to pilot UC as the DEOS acquisition will take time to implement. Questions regarding the Army's transition plans and intent for this particular acquisition should be referred to the Army.

Q2: How is DISA participating with the Cloud Executive Steering Group on the recently released DOD Cloud RFI and anticipated 2018 procurement?

A2: DISA provided the CESG details of the DISA offerings and acquisitions in progress, to include milCloud 2.0 and Secure Cloud Computing Architecture (SCCA) services that directly support other DOD commercial off-premise cloud acquisitions.

Q3: Will it be mandatory for all DOD organizations to use DEOS?

A3: That is a policy decision to be made by the DoD CIO. Currently, it is not mandatory.

Q4: What cloud environment is DISA is moving to, commercial based cloud, such as AWS, or DISA's own cloud?

Q4. DISA awarded a contract for milCloud 2.0 to CSRA, Inc., to provide an on-premise contractor owned and operated DOD private cloud for both classified and unclassified data. DISA is also providing the SCCA (see above) to make it easy for DOD entities to acquire the security services for multiple commercial off-premise cloud service providers.

Cyber

Questions for COL Brian Lyttle

Q1: What is DISA's involvement in assessing and securing Operational Technologies that interact and support the DOD information systems technologies and networks?

A1: DISA secures the operational technology the agency operates, and DISA provides enterprise licensing for many other products used across the DOD.

Q2: Will DISA consider moving from a proprietary contractor developed and maintained big data platform to a COTS solution?

A2: Big Data Platform is a contractor-provided solution using mostly open source products similar to existing commercial solutions. We have full intellectual property rights to the solution, and, therefore, our solution is not proprietary. The current contract expires in 2021, and continued evolution will be based on (1) this platform, (2) the analytic solutions and operation missions running on that platform, and (3) the capabilities of next generation COTS solutions to possibly replace the current COTS solution. The long term DISA Big Data strategy is to continue the use of open source components while simplifying the capability to support multiple mission sets.

Q3: Will COL Lyttle be using the new DISA small business BPA, SDSS, for software development?

A3: This requirement will be assessed on a contract-by-contract basis.

Q4: Will the CNODDS contract stay on GSM-ETI?

A4: No.

Q5: How are ACAS, Secure Configuration Management (CM) and Cyber/ NetOps CM solutions related? Is the OC's CM/data Normalization and data analytics connected?

A5: The Assured Compliance Assessment Solution (ACAS) is a comprehensive network and system vulnerability scanning and reporting capability. ACAS is used to scan assets to identify cybersecurity vulnerabilities and to verify the security posture of a system. ACAS scans are used across DOD to validate the secure configuration of our Cyber/NetOps solutions.

ACAS/CM must interact and operate together, especially at the data level. The ACAS Security Center collects, manages, and presents the scan results for systems/networks and the Operations Center/DOD utilize these scan results to further secure their systems. The Cyber Directorate provides ACAS plugins (new scan checks) to the Operations Center and the DOD to ensure newly identified cyber security vulnerabilities are detectable via ACAS.

Q6: Will the cyber opportunity be solicited on a full and open basis? What contract vehicle (if any) will be used?

A6: Cyber opportunities will be solicited as a function of the required capability: software, hardware and/or service. DISA will consider all available vehicles to expedite delivery of cyber capabilities in a timely and cost effective manner.

Q7: Is the JRSS program looking into securing voice/UC traffic?

A7: If threats and effective network traffic mitigations develop in those technology areas, JRSS will assess the suitability of a defensive solution being incorporated into the architecture.

Mobility

Questions for Jacob Marcellus

Q1: Can you expand on how and why you desire to expand mobility solutions?

A1: In 2017, mobile access has become a norm. DOD personnel expect the same efficacy and efficiency they get using mobile devices in their personal lives. Our program expects to expand the usage of mobile devices for classified system access using Commercial Solutions for Classified (CSfC). Our DOD customers have specifically asked for larger form factor devices, and we will incrementally deliver expanded capabilities on tablets.

Q2: How does OMB's Mobility Categorization Management initiative, run by GSA, influence your future contracting approach on DMUC, Secret and TS?

A2: Our future contracting approach will be consistent with OMB's Category Management Initiative. DISA and DITCO are both active members of the Mobile Services Category Team and helped construct the output from that team. In addition, the approach will be driven by our mission needs while remaining cognizant of the available procurement resources, consistent with both the MSCT and M-17-22.

Computing

Questions for Anthony Purvis

Q1: Based on your feedback made to industry at the DCO Symposium earlier this year, is it still the intent of DISA to roll in the Cyber and Comms Lines of Business from the Computing Ecosystem to the GSM-O Contract in the future?

A1: The plan is to look at GSM-O II in the 2021/22 timeframe to determine if it is a good fit with ecosystem requirements.

Q2: For those vendors pushing for FEDRAMP HIGH certifications, on their products currently in use at DISA, who is the governing authority within DISA to assure a vendor's approach is aligned with DISA's requirements and is there a resource to industry that can respond to questions specific to a vendor's FEDRAMP plan and approach?

A2: DISA leverages the FedRAMP processes, supplemented by DOD requirements outlined in the DOD Cloud Computing Security Requirements Guide (SRG) for more sensitive workloads, assessing the risk and determining acceptability of a provider from a baseline of common controls. These processes would result in a provider being issued a Provisional Authorization. For any cloud system hosting DOD workload, the mission owning Authorizing Official still needs to determine the acceptability of risk related to the mission system and the data. FedRAMP processes are documented on the FedRAMP website at www.fedramp.gov, and the Cloud Computing SRG can be found on the iase.disa.mil website under the cloud computing section of the site.

Q3: Will the ecosystem scope be incorporated into GSM-O II upon award or over time?

A3: The plan is to look at GSM-O II in the 2021/22 timeframe to determine if it is a good fit with ecosystem requirements.

Joint Staff Support Center

Question for Col Douglas Shahan

Q1: How do your missions/functions differ from 844CS and JSP?

A1: The wide-ranging and diverse Information Technology (IT) requirements within JSSC, 844CS, and JSP are constantly evolving. These three organizations address various mission areas with tailored support to optimize responses to their respective users. Fundamentally, they all rely on commercially-available COTS products as well as GOTS products to meet customer needs. The JSSC Multimedia and the Global Service Desk are examples of highly tailored mission sets, but that is not to say they are completely unique. See FedBizOpps link below for a full description of JSSC's tailored mission requirements:

<https://www.fbo.gov/index?s=opportunity&mode=form&id=3e56c7f0deb3d8f6dcf5b3e17bf78c73&tab=core&tabmode=list&=>

Senior Procurement Executive

Question for Tony Montemarano

Q1: You often use terms like Agile and Risks. How many industry-certified professional are there in your organization in those areas?

A1: DISA offers Agile and Risk Management training to the workforce to augment the 200+ Defense Acquisition University (DAU) Defense Acquisition Workforce Improvement Act (DAWIA) Level III certified PM and IT professionals. In FY17, 19 acquisition professionals attended agile process training taught by industry leading vendors and have plans to train an additional 36 in FY18. Provisions in the FY18 National Defense Authorization Act also provide for future in-resident targeted training and pilot programs for agile development.

Office of Small Business Programs Update

Questions for Sharon Jones

Q1: How much of DISA's small business work utilizes NAICS code 541715, which limits small business based on company size rather than revenue? Does DISA prefer to use that NAICS code or not?

A1: The short answer is the Defense Information Systems Agency (DISA) does not have a NAICS code preference.

The longer answer derives from the U.S. Small Business Administration, Table of Small Business Size Standards. NAICS code 541715 is Research and Development in the Physical, Engineering, and Life Sciences (except Nanotechnology and Biotechnology) and is an employee based size standard. DISA will not use this NAICS code based on the associated note 11, which states the Research and Development means laboratory or physical research and development. It does not include economic, educational, engineering, operations, systems, or other not physical research; or computer programming, data processing, commercial and/or medical laboratory testing. The bottom Line: This NAICS code is NOT applicable for the services offered by the Defense Information Systems Agency.

Q2: Is there a "checklist" for small businesses just starting out to get into this world with DISA?

A2: A "checklist" is not available for small businesses just starting out to get into this world with DISA. However, there are excellent websites available to assist you in your business endeavors: The Small Business Administration website has great content at www.sba.gov or contact your local Procurement Technical Advisory Center at www.dla.mil/hq/smallbusiness/ptac or visit DISA's YouTube channel and website at www.disa.mil and www.youtube.com/user/USDISA.

Q3: Is a breakdown available showing the NAICS codes for the women owned companies that you have used and has an attempt been made to assure that WOSB's from Tech and satellite communications companies are included in your statistics.

A3: Every contract award that DISA has made to WOSBs from technology and satellite communications companies is included in DISA's overall small business statistics. Additional small business statistical information is available at www.fpds.gov.

Q4: The HUBZone target appears to have been lowered again from 2% in 2017 to 1.5% in 2018. Would you discuss some of your planned actions for 2018 to attract and engage HUBZones? In addition to DESS II, are there any planned set-asides?

A4: Yes, it is true DISA's HUBZone small business target goal was lowered from 2% to 1.5% by the OSD Office of Small Business Programs for FY18.

The Office of Small Business Programs will conduct its annual HUBZone Huddle at DITCO Scott and HUBZone Showcase at Ft. Meade.

Please review our video and slide presentations from DISA's Forecast to Industry held on Monday, Nov. 6, for upcoming small business set-aside opportunities.

Q5: Who will be replacing Ms. Sharon Jones?

A5: Ms. Sharon Jones is irreplaceable and a successor has not yet been named.

Q6: Did you overlook the DESS II IDIQ, designed for HUBZone acquisitions, on the list of DISA IDIQ vehicles, or is it too small to have significance?

A6: The DESS II IDIQ acquisition is still a solicitation and not yet a viable contract. Inclusion of DESS II IDIQ on the DISA list of available contracts will occur immediately upon contract award.

Q7: Will there be small business, WOSB and/or HUBZone set-a-sides?

A7: There will always be small business opportunities for small business and small business firms in every socioeconomic category.

Q8: Is DESS II, the HUBZone set-aside, an important part of DISA's strategy? I haven't seen it mentioned among IDIQs.

A8: Yes, the DESS II IDIQ, upon contract award, is an important part of DISA's acquisition strategy for obtaining critical mission requirements for the global warfighter.

Networking Technologies

Questions for Jessie Showers

Q1: What is the total MHz you procure now and in 2018 (Ku, Ka, X, C, L)? Will you be providing a projection of COMSATCOM demand?

A1. The DOD currently leases over 7.5 GHz of COMSATCOM bandwidth through DISA. DISA releases 12-month COMSATCOM projections each quarter through GSA eBuy.

Q2: What is the status of the MPLS gear upgrades that DISA has been making for the last few years? Could you please give us an update?

A2: MPLS currently is installed at 105 sites with a total of 364 projected. The installation is projected for completion by FY19.

Q3: How are the circuit priorities for the Tech Refresh determine? Will the \$100+M be expended in FY18 or multiple years?

A3: Circuit priorities for Tech Refresh are based on several factors including ease of transition, mission need, impact to ongoing missions and customers, network efficiencies, and cost of transition. These are weighted depending on individual circuit requirements. The \$100M will be expended across multiple years.