2018 F2I: Trusted Partnerships
Answers to Captured/ Unanswered Event Questions

DOD CIO - Mr. Deasy

Q1. How will DOD and DISA protect users of the ubiquitous Smart phones to protect unclassified and confidential conversations?

Answer: DISA is exploring solutions to allow Defense Switched Network (DSN) calling from mobile devices.

Q2. Does the DOD plan to provide overarching guidance to the military services as they pursue IT service outsourcing?

Answer: DOD policy for acquisition of services is governed by DOD Instruction 5000.74, "Defense Acquisition of Services," which includes IT service outsourcing. Section 803 of the FY17 National Defense Authorization Act (NDAA) mandates a review and, if necessary, revision of this instruction with a particular focus on modernization of services acquisitions. DOD CIO is collaborating with A&S, Comptroller and other DOD organizations to review and update the instruction, along with DOD Instruction 5000.75, "Business Systems Requirements and Acquisition," to align overarching guidance for acquisition of IT services with the DOD cloud strategy and commercial IT service business models.

The Department currently provides extensive guidance on securely developing and operating IT systems. Current law governing federal information security, the Federal Information Security Management Act of 2002 or FISMA, requires that the Department hold outsourced IT services to the same cyber requirements as internally developed system and services. Thus, the full set of DOD cybersecurity requirements are applicable to outsource IT including: DOD Instruction 8500.01, "CyberSecurity;" DOD Instruction 8510.01, "Risk Management Framework (RMF) for DOD Information Technology (IT);" and DOD Instruction 8530.01, "Cybersecurity Activities Support to DOD Information Network Operations."

Q3. Recent activity on the Hill seeks to eliminate DISA, suggesting the agency is inefficient or that its mission can be performed better by the DOD services. Can Mr. Deasy address this perspective and the Department's position regarding DISA's value?

Answer: DISA is an integral piece of the Department of Defense. DISA performs a multitude of functions across the DOD, ranging from providing secure critical infrastructures for our service members around the globe to also providing rapid and interoperable communications during humanitarian crisis situations. Without a doubt, the scope of DISA is wide and the military and civilians at DISA bring a wealth of knowledge to the DOD.

Q4. I didn't hear anything about developing secure applications/software so that systems operate as intended under malicious attack. Where does secure software development fit into your Cyber priorities?

Answer: Secure software development is a very high priority for the Department. We recognize that in today's IT-based mission environment, the ability to rapidly adapt software to emerging and persistent threats and mission needs is an increasingly essential component of mission success. Therefore, adopting secure, agile software development practices, processes and technologies that fully integrate IT development, security, and operations (Agile DevSecOps) is critical to achieving IT superiority. The DOD has several programs that have already embraced the principles driving Agile DevSecOps and we are looking to build upon those successes. To that end, the

Department intends to leverage commercial best practices and work with our industry partners to establish an enduring enterprise environment. Similarly, military services can obtain an integrated and automated suite of development and test tools and security software that enable Agile DevSecOps within our Defense Enterprise Cloud Environment and are fully aligned and integrated with the Department's cybersecurity architectures, policies, and capabilities.

Q5. Can you elaborate on the role GSA will play in DEOS and how they will bring value in terms of mitigating cost and schedule risk.

Answer: GSA will provide the contracting and acquisition support for DOD Enterprise Office Suite (DEOS) capability. We will leverage the existing GSA IT Schedule 70 contract vehicle as it provides flexibility for the Department to accomplish our goals, maintain our commitment to a full and open competition and at the same time align ourselves with the President Management Agenda.

The IT Schedule 70 vehicle is a proven contract vehicle and includes industry leaders in this space. GSA, through its FAStLane process, will expedite vendors not currently on Schedule 70 to be added promptly in order to compete for the DEOS requirements.

From a cost perspective, we can negotiate with GSA to garner a better fee structure for the Department in its entity. Secondly, using GSA supports category management, and with centralized management, will provide greater visibility into the cost of these services. The whole-of-DOD approach will foster economies of scale and provide a better Government position for negotiating price.

From a schedule perspective, GSA IT Schedule 70 includes a large pool of industry leaders in this space. Since the contracts (schedules) are already awarded, we plan to award a blanket purchase agreement under FAR Part 8 for the DEOS capability. This will streamline the procurement process and get us to contract award/implementation in a shorter time period.

Q6. What can the Department do differently to borrow from private industries successful move to the Cloud and use of AI?

Answer: With the recent cloud acquisitions and AI efforts, the Department is making significant strides away from custom developed IT solutions and toward commercially available technologies and services. The Department is leveraging the best technologies, skills, and capabilities from both private industry and academia to improve IT operational effectiveness and ensure IT superiority.

Q7. Does DOD plan to use DISA as key analytic cloud provider for USCC and CCMDs, or will they source their own solutions?

Answer: The DOD, through both the JEDI and DEOS clouds, will leverage analytic cloud capabilities when appropriate for both USCC and the CCMDs in order to achieve the required visibility to make informed decisions.

<u>MONTEMARANO – SPE</u>

Q8. Does DISA intend to leverage 5G technologies, and if they do how do you see them being leveraged?

ANSWER: Like all emerging technologies, DISA is actively following the development of 5G capabilities. Major carriers are just now announcing plans to deploy 5G infrastructure and phone vendors in general are not shipping 5G handsets yet, so while DISA is interested in the speed 5G brings and will look at use cases in the Defense Information Systems Network, there are no firm plans to leverage the capability at this time. Specific locations and uses will be better determined as the commercial capability is fielded and costs are stabilized

Q9. What is the status of the DOD budget flowing down to DISA and MILDEPS? Is funding available at the PM level? If not, when?
ANSWER: The budget is approved and the appropriate allocations have been made.

STEWART – OTA

Q10. Please clarify which OTAs DISA may use.
Answer: DISA intends to award "point-to-point" Agreements. We do not plan to use any existing OTAs that may have been established for decentralized ordering.

Q11. What consortiums are you utilizing for your OTA management, execution, and distribution? C5, SOSSEC, Cornerstone, etc.?
Answer: We are not currently using a consortium.

Q12. Are you issuing topics from the government to industry? If so, how? Through the consortiums or through DISA?
Answer: We may issue Requests for Information to gather information on industry capabilities. We plan to post Requests for White Papers through Federal Business Opportunities (FEDBIZOPPS), and at https://dreamport.tech through our partnership with the Maryland Innovation and Security Institute.

Q13. Does DISA view an OTA submission led by a non-traditional defense contractor more favorably than a submission led by a traditional contractor with significant participation by a non-traditional?
Answer: We do not view the relationship more or less favorably. The relationship is merely different since there will need to be an assessment of the extent of the relationship.

Q14. Can you elaborate on what Mr. Montemarano mentioned regarding the challenges around incorporating agile and OTAs?
Answer: OTAs provide a great deal of agility as they are not bound by all the policies and procedures in the Federal Acquisition Regulation (FAR) or Defense FAR Supplement.

Q15. How does a company become a member of the DISA OTAs?
Answer: We are building a data base of interested parties. Companies may send capability statements to the DISA Agreements Officers disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil and they will be added to the database.

Q16. What organizations is manage (sic) the consortiums?
Answer: We are not currently using a Consortium Management Firm (CMF). If we choose to use a CMF it will be competed.

TIMERMAN – DEVELOPMENT & BUSINESS CENTER

Q17. How does DISA evaluate new innovations from Industry?
ANSWER: DISA uses a variety of methods to evaluate new technology. We have our Technical Exchange Meeting (TEM), which provides a forum for industry and government to come together and learn about new innovations within industry. DISA TEM's support the exchange of technical and innovative ideas between industry partners and the government. To request a meeting, a firm can go to the following site https://disa.mil/About/Industry-Partners and then select the link "Demonstrate Your

Product to DISA". Also, we work with various Worx environments within the DOD to evaluate new technologies. Finally, we have ad-hoc evaluations of various solutions where we bring them into both government owned as well as integrator facilities for evaluation.

Q18. Could you please repeat your best estimate of when the NBIS responsibilities will transfer to DSS?
ANSWER: The transition will be incremental starting with Operational Control (OPCON) in FY19 and Administrative Control (ADCON) in FY20, pending DEPSEC directive to transition NBIS to DSS. A transition plan will outline the actions and time line to be accomplished before the transition is complete. These steps will include transitioning the program management and the Milestone Decision Authority as part of the OPCON; funding and personnel transition as part of the ADCON.

Q19. You mentioned the NBIS project is turning over to the sponsor - DSS. What is the milestone that triggers that transition?
ANSWER: The trigger for the transition will be the pending DEPSEC directive to transition NBIS to DSS.

HERMANN – SD
Q20. Is your directorate planning to leverage the Encore 3 IDIQ for procurements (once protests are cleared)? If so, please elaborate on how you will determine the Task Order requirements that will be sent to the vehicle.
ANSWER: It is our goal to maximally leverage appropriate pre-competed contract vehicles especially DISA IDIQs including ENCORE 3, Systems Engineering, Technology and Innovation (SETI), and the Agency Program Support (APS) Blanket Purchase Agreement. After market research, program managers submit task order performance work statements (PWS) and statements of work (SOW) to the contracting officer for advertisement among the appropriate vendor pools on the selected contract vehicle.

Q21. Will the DEOS opportunity be a Small Business set-aside or Unrestricted on GSA Schedule 70?
ANSWER: We are currently evaluating the final market research from the GSA-released DEOS request for information, which was discussed at the Dec. 3, 2018 GSA-hosted DEOS Industry Day.

BELT – CYBER
Q22. How is DISA evolving its Cybersecurity requirements as the services you are securing become more hybrid (multi-vendor)?
ANSWER: Cybersecurity requirements are not evolving in response to the diversity of our vendor base. Cybersecurity requirements are evolving to adapt to changing capabilities of our adversaries. DISA views a diverse vendor base as an enhancement to our overall security. Steps DISA is taking because of the increase in diversity in our vendor base include more scrutiny on vendor interoperability when we evaluate products, formulation of data strategies to address diverse data, and multi-vendor automation and orchestration platforms to reduce the human interaction with diverse platforms.

Q23. What are the major activities DISA is taking on and their related opportunity timelines regarding NDAA Section 1653 and Comply to Connect?
ANSWER: DISA, along with DOD/CIO, NSA, and USCC are in the process of formulating a comprehensive end point security strategy. The comply to connect function will be a component of that strategy. Early capabilities recommended by the strategy will begin deployment in early FY19. The entire capability, including comply to connect would therefore be available before 2022.

Q24. With AI and machine learning becoming a bigger part of the cyber security conversation, does DISA plan to include these in its plans/production?
ANSWER: We do have a number of plans as well as projects in execution that will leverage ML and AI. We do not see ML or AI as standalone products but as capabilities that can be added to larger solutions. We are working with vendors in the analytics as well as identity spaces to integrate ML and AI where appropriate.

DISA is leveraging ML and AI in a couple of key areas, including signatureless end point protection for tactical environments and analysis of big data. DISA plans to continue to evaluate ML/AI systems for utility and effectiveness as well as identifying other mission areas that will benefit from the technology.

Q25. How do SCADA and OT networks fit into the DISA strategy? Often these critical networks are over looked but critical to mission.
ANSWER: DISA generally does not monitor, control, or operate these networks. It is the responsibility of the mission owner to ensure that the networks are protected.

Q26. The recent Acropolis RFI asked questions regarding innovation and machine learning, but the draft PWS did not reflect those questions.
ANSWER: Acropolis 3 scope is focused primarily around maintaining the Acropolis environment and providing Tier II sustainment services for the hosted Defensive Cyber Ops (DCO) applications. At present, Acropolis doesn't host machine learning capabilities. However, as existing DCO applications continue to evolve and improve, machine-learning experience may be needed. The final PWS includes ML capabilities consistent with the missions assigned to the Acropolis capability.

Q27. Why are you not putting ACAS on ENCORE 3 as it is currently ENCORE 2?
ANSWER: We are continuing to review contract vehicles for the ACAS acquisition. ENCORE 3 small business is under protest and therefore not the automatic contract vehicle for consideration. There are potent small businesses that can perform the ACAS requirements. Contract vehicles will be determined based on market research to identify the optimal vehicle.

Q28. What is the status of the "cloud-based internet isolation solution"? – DISA did an RFI for this several months ago.
ANSWER: A Request for White Papers was issued Nov. 28, 2018 and Papers were submitted by the Dec. 14, 2018 due date.

Q29. What is being done to de-conflict all of the capabilities at the Perimeter in order to close the vulnerability gaps that still exist?
ANSWER: DISA rejects the thesis that there are vulnerabilities at the perimeter caused by conflicting capabilities. DISA is looking at End Point protection, perimeter, and JRSS in a more holistic manner to avoid duplicative functions and enhance the overall cyber posture of the DODIN. DISA is also looking at a number of technologies, such as

internet isolation, and GCDS which promise to lower the volume of data that must be inspected by perimeter security systems, which will allow them to be more effective. DISA is also working with JFHQ/DODIN to help ensure a consistent perimeter security posture across the entire DOD.

Q30. Several small businesses have been key partners on Acropolis. A sources sought notice asked for our capabilities under Acropolis 3.0. Is DISA giving serious consideration to allowing a proven small lead this great mission?
ANSWER: We appreciate the capability of the businesses interested in providing Acropolis 3.0 services. We are carefully comparing the responses to our sources sought with the full scope of the Acropolis 3.0 PWS and will make a decision about acquisition approaches based on this assessment consistent with FAR guidelines.

Q31. The requirements outlined in the recent Acropolis 3.0 sources sought notice did not sound like commodity services (e.g. innovative services and cloud transformation). As such, is DISA considering splitting the PWS into two acquisitions (one for O&M and one for transformation) and/or moving acquisition to a schedule or vehicle other than ENCORE III?
ANSWER: At present, it is not our intent to split the acquisition into multiple pieces. Given the importance of the Acropolis program and the potential impact to all of the hosted DCO applications, the Acropolis PMO seeks to reduce integration risk where possible. DISA's need for this capability includes assigning full end-to-end responsibility for delivery of Acropolis 3.0 capabilities to a single vendor. The PMO determined that dividing responsibilities into two acquisitions is not in the best interest of the government.

MARCELLUS – MOBILITY

Q32. Knowing that Bring Your Own Device (BYOD) will make immediate cost/time efficiencies impacts for the National Guard and Reserves. Can you please share DISA's BYOD Strategy?
ANSWER: The DOD Mobility PMO continues to work with the DOD CIO office and our mission partners to develop a potential future service offering for BYOD access. This on-going analysis includes considerations for technical and non-technical challenges with providing DOD data on personally owned devices.

Q33. What is the DISA mobility program doing to support tactical edge use cases and enabling our warfighters with mobile solutions?
ANSWER: The DOD Mobility PMO provides managed platforms that can be used for both administrative and tactical use cases. Mission partners with tactical use cases have submitted Apps that are approved for DMUC. We continue to personally engage with mission partners to understand their operational needs and how DMUC can be an enabler. Recent use case is deployment of the Precision Fires StartGuides app for the Army.

Q34. What is the DMUC program doing to streamline the approval of mobile applications for use on DISA managed mobile devices?
ANSWER: The DOD Mobility PMO vets apps using the Risk Management Framework and NIAP protection profiles. We have created a self-service workflow system that mission partners can submit and view status of App vetting. Apps that are built within RMF and NIAP standards have taken as little as 7 days to obtain approvals. The Mobility PMO's automated risk scoring algorithm against NIAP Protection Profiles

further reduces vetting times, streamlining to flash-to-bang from submission to deployment.

MARTIN – COMPUTING

Q35. What are the timeframes and milestones for decommissioning the milcloud 1.0 infrastructure?
ANSWER: DISA Leadership has not identified a date for decommissioning the milCloud 1.0 Infrastructure.

Q36. You mentioned capacity contracts, with the re-compete being in source selection for well over a year, what is the anticipated award timeframe for the x86 processor capacity contract?
ANSWER: The contract was award Dec. 18, 18, to HPE.

Q37. How will milcloud 2.0 interface functionally with JEDI, if at all?
ANSWER: milCloud 2.0 will not interface functionally with JEDI.

Q38. Who is SE's milCloud 2 lead?
ANSWER: The milCloud 2.0 PM is Ms. Caroline Bean.

Q39. How are you helping the 4th estate CIOs move to milCloud 2.0? What guidance or Cloud Adoption Frameworks are you providing or recommending to these CIOs?
ANSWER: DISA is providing 4th Estate Migration leads and engineers to assist the Agencies in migrating to milCloud 2.0. DISA hosted multiple Cloud workshops and summits and continues to publish lessons learned and best practices to the mission partners.

CAPENOS – SMALL BUSINESS

Q40. Does DISA utilize a Tiered approach for acquisitions under FAR 215.203-70 to increase socioeconomic participation?
Answer: There is nothing prohibiting DISA's use of DFARS 215.203-70, Request for proposals – tiered evaluation of offerors. However, this has not been utilized.

Q41. In what I have seen, many of DISA's requirements require the contractor to be cleared at time of award. Is DISA willing to sponsor uncleared small businesses?
Answer: Generally, no. In order for DSS to process a clearance, there needs to be a contract that has a security access requirement. Since the clearance process takes a long time most Programs don't have the flexibility to postpone the commencement of work under a contract while a contractor obtains the necessary clearances.

Q42. Modernization, Consolidation, Data Sharing, Data Availability, Global are all today's needs. Can you please advise on how the process of bringing innovation and proof of concepts can be streamlined for small businesses?
Answer: DISA is working on an answer to your question but we don't have one right now. With the standup of the Innovation Directorate, the pending award of the Systems Engineering, Technology and Innovation (SETI) small business pool awards and DISA's new authority to enter into Other Transaction Authority (OTA) Agreement, DISA has not identified the process to connect innovation, small businesses and our Mission Partner's requirements yet, but acknowledges that it needs to be explored.