RFQ 35438
INFORMATION ASSURANCE AND COMPLIANCE AUDIT OF THE DEFENSE
INFORMATION SYSTEMS AGENCY (DISA)

Questions with Government Responses.
10 June 2004

Question 1. Who will sign the consolidated SAS-70/88 opinion? IG DOD or the contractor?

> *Answer: IG DoD as the statutory auditor for the DoD financial statements will opine on the SAS 70 Type II review. The contractor performing the SOW will prepare the SAS 70 Type II report and the IG DoD will sign and issue the report.*

2, Does DOD intend for the contractor to evaluate compliance with DISA Security Technical implementation Guides (STIGs) for all environments supported by 0 ISA? Can you provide a list by location for which the STIG compliance requirements are to be addressed?

> *Answer: We do not envision that every platform at every site will be tested. The number of reviews for STIG compliance will be determined by the contractor, in coordination with DoDIG, to ensure that adequate coverage of the general controls are tested, that the results of system security reviews can be relied upon, and an opinion can be expressed.*

3. Will the IG DoD provide deliverable dates as they have in past solicitations?

> *Answer: We have attached a revised schedule of delivery dates.*

4. In Section 6.2 of the SOW, ADP-1 clearance is required ‘for access to systems’. The DD-254 specifies SFCRET facility and safeguarding clearance under this contract. Does the IG DoD expect that contractor to provide ADP-1 (SSBi or TS-cleared) individuals to perform the hands-on systems work? If so, is a TOP SECRET DD-254 required?

Answer: This section 6.2 of the SOW should read, A SECRET clearance is required for unescorted access to facilities housing the audited systems. For those personnel accessing government computer systems to extract audit information, those position are designated as ADP-I and require a favorable adjudicated Single Scope Background Investigation (SSBI).

5. It is our understanding that UNISYS systems are also maintained at DECCs and will therefore be subject to the review. If this is correct, please clarify how many UNISYS systems will the contractor be required to test.

> *Answer: Exact number of UNISYS systems can not be provided at this time. We do not envision that every platform at every site will be tested. The number of platforms, database, storage devices, security software databases, etc will be determined by the contractor, in coordination with DoDIG, to ensure that adequate coverage of the general controls are tested and an opinion can be expressed. This determination should be based on prior results at the specific site and risks assigned by the contractor.*
>
> *However, DISA transformation is consolidating the majority of the financial systems running in a Unisys environment to a single location, but backed up to another location. Also, DIFMS, one of the major Unisys financial systems is in the final stages of migrating out of the Unisys environment.*

6. For the DISA DECCs using IBM mainframes, please provide us with the following:

The number of LPARs (DISA wide) that share security software databases (RACF, ACF2 and TopSecret)
The number of LPARs executing OS/390 or z/OS that share a common set of parmlibs for MVS.
The number of LPARs executing OS/390 or z/OS that share DASD (Direct Access Storage Devices)

Answer: Exact number of systems can not be provided at this time. We do not envision that every platform at every site will be tested. The number of platforms, database, storage devices, security software databases, etc will be determined by the contractor, in coordination with DoDIG, to ensure that adequate coverage of the general controls are tested and an opinion can be expressed. This determination should be based on prior results at the specific site and risks assigned by the contractor. See answer to number 10 for additional information.

7. The SOW did not list DISA CENTCOM, DISA Europe, DISA Pacific data center locations. Please clarify if these data center locations should be considered as being in scope for this review?

> *Answer: These centers will not be included in this SOW. The review will consist of DISA DECCs and detachments that process financial data.*

8. . The SOW requires a SAS 70/88 Type II report as part of the final report deliverables. Will DoD require a CPA firm to provide an opinion on the Type II report? Also, will DoD provide the contractor with a description of the internal control environment as well as the control objectives that will be the starting point for a SAS 70/88 report?

> *Answer: IG DoD as the statutory auditor for the DoD financial statements will opine on the SAS 70 Type II review. The contractor performing the SOW will prepare the SAS 70 Type II report and the IG DoD will sign and issue the report.*
>
> *To the extent that management has described their internal control environment and control objectives, we will provide them to the contractor receiving the contract award.*

9. We are assuming a period of review to be covered by the SAS 70 as 6 months -- -the minimum under the AICPA standard. Is this correct? What 6 month period do you want covered?

> *Answer: The period of testing of the DISA Computer Services will span 6 months. It is not necessary to test a span of 6 month at each location. Testing should be complete by 31 Mar 05.*

10. Please provide the following information to enable the contractor to determine the scope of the work:

Mainframe environment:

- Number of computers to be tested for each DECC
- Number of logical partitions (by each DECC location or DISA wide)
- Types of Operating system(s) and release number(s)
- Access Control Software (ACF2, RACF, Top Secret, etc.)
- Job Scheduling Software
- Database software
- Transaction Manager software
- Tape Management Software
- Type of network connections (SNA, TCP/IP, or other)

Midrange Computing environment:

- Type of Midrange computers (such as AS/400)
- Types of Operating system(s)
- Types of database software
- Types of Networks
- Type of network connections (SNA, TCP/IP or other)

Server Environment

- How many of the 1,350 servers (DISA wide) will need to be tested?
- Describe operating environment for each server to be tested

Answer: Exact numbers can not be provided at this time. We do not envision that every platform at every site will be tested. The number of platforms, database, storage devices, security software databases, etc will be determined by the contractor, in coordination with DoDIG, to ensure that adequate coverage of the general controls are tested and an opinion can be expressed. This determination should be based on prior results at the specific site and risks assigned by the contractor.

IBM Mainframe Environment:

The majority of our LPARS (approximately 78%) are currently running under release 2.10 of OS/390, with approximately 20% running under release 1.4+ of zOS and the rest under release 1.4e of zOS.

DISA has a fairly even distribution among the three Access Control Software systems (RACF, ACF2, and Top Secret). DISA is on ACF2 maintenance level 6.4 and have about an even distribution between maintenance levels 5.2 and 5.3 of Top Secret.

The majority of their Job Scheduling is done under Control-M, but some under MSS.
Database Software includes DB2, IDMS, Oracle, Supra, IMS, and M204.
The major Transaction Manager software is CICS, but we also support Roscoe and IDMS DC.
The major Tape Management Software is CA-1.
For network connections, we support both SNA and TCP/IP.

Midrange Computing Environment:

Types of computers: Sun: 6800, 4800, V880, V480, E5500, E3500, E 450, E350, E250
HP Superdome, HP 9000: rp8400, rp7400, rp7410, L3000, L2000, N4000, V2600, V2500, K570, K460, T520

Types of Operating Systems: Sun Solaris 8 & 9; HPux 11.0
Types of Database Software: Primarily Oracle
Types of networks: fiber channel and ethernet
Type of network connection: TCP/IP

11. Section 3.1 of the SOW lists the locations for the DISA DECCs but does not mention the following locations/functions that would need to be reviewed to support FISCAM/FFMIA compliance

· Change Control functions performed by CDA (for example FMSO) to support the DECCs
· Entity-wide Security Program management functions at DISA HQ (Fort Myers, VA).
· COOP site at Slidell, LA.
· NOC site under the Columbus DECC
· Patch management function performed by GNOSC.

Please clarify if these locations/functions are within the scope of the general controls testing.

> Answer: *Yes and any other sites identified during the audit that is deemed necessary. Computing Services-wide Security Program Management functions are performed at the DISA facility in Chambersburg, Pennsylvania..*

12. The objectives listed in the SOW require the contractor to determine whether application controls are adequately designed and effective? Since the DISA DECCs provides computing services to the DoD community, it is our understanding that only general controls need to be tested? Is our assumption correct? If application controls testing is required, please provide the list of applications that will be subject to testing.

> *Answer: The only application controls to be reviewed will be those applications that DISA uses to manage the centers, i.e, trouble tickets, patch management, configuration control, etc to determine the reliability of the data. DISA uses TMS as its standard trouble ticket system. Other products used include: Tivoli, MICS, HP Openview, Managed Objects – Formula, CA-Unicenter, ACC, Mainview.*

13. Page 2 of the Cover Letter states that "?.resumes and letters of commitment are required of all key staff." Also, section 6.3.1 ("Key Personnel" of the SOW requires the contractor to provide the Procuring Contracting Officer (PCO) with a list of key personnel at the senior level and above assigned to the contract. Our assumption is that "key staff" and "senior level" personnel mean individuals who are responsible for managing and directing the project and are not categorized as a "labor category" under the GSA Schedule. Is our assumption correct?

Answer: The IG DoD is only requiring resumes and letters of commitments for key staff. The IG DoD is defining key staff as those individuals responsible for directing and managing the project.

14. The SOW requires an information assurance and compliance audit of the DISA Computer Services. However, it also requires the contractor to perform an audit to comply with FFMIA. Since FFMIA applies more to financial management systems, a full scope FFMIA compliance would be out of scope under this SOW. There are aspects that a contractor could assess compliance regarding FFMIA, however, this would only include the internal controls associated with the general control environment at the DECCs and DISA Computer Services and this type of review would not be considered a full scope review under FFMIA since the financial management portions (i.e. compliance with federal accounting standards) would not be included. Please clarify regarding the extent of FFMIA compliance that will be required as part of the testing to be performed.

Answer: Only those FFMIA requirements that are applicable to DISA Computer Services need be tested.

15. Statement of work, page 1, section 2.0. "Specifically, the contractor will determine whether DISA: (1) general and application controls are adequately designed and effective; (2) complies with the FFMIA and all other applicable laws and regulations; and (3) is properly certified and accredited in accordance with DITSCAP."

Please elaborate on the requirement to evaluate application controls. Ensuring that application controls are appropriately designed and operating effectively is typically the responsibility of the application owners who are responsible for the design and functionality of the application and the application users who process transactions in the systems. What aspects of application controls does the OIG envision that the contractor will perform in the audit of DISA?

Please elaborate on the requirement to perform an evaluation of compliance with FFMIA requirements. Is the expectation that contractors will evaluate FFMIA compliance for the more than 1,400 applications described as being hosted by DISA? Given that these applications are owned by DISA client organizations, what is the expectation regarding the scope of the FFMIA assessments?

Answer: See answers to 12 and 14

16. Statement of Work, page 1, section 3.0. "The DISA computing environment has approximately 800,000 users and process 1400 applications at 18 data centers."
Statement of Work, page 2, section 3.1. "Locations…"

The first section states that there are 18 data centers and the second section lists 17 DECCs and Detachments. Please elaborate on why these numbers are not identical.

Answer: DECC detachment Jacksonville (DECC Mechanicsburg) was accidentally omitted in the SOW and should be include. Number of DECCs and detachments is 18.

17. Statement of Work, page 1, section 3.0. "General controls are the polices and procedures that apply to all or a large segment of the entity's information systems and help ensure proper operation."

Please specify the appropriate GSS area that the IG DoD expects to be reviewed. For example, does the IG DoD expect contractors to review GSS that support DISA financial statements, GSS that support DISA operations / other agency support, or all DISA GSS?

Please elaborate on the expectations regarding the contractor's inspection of physical security controls. If these are included, it will affect the level of effort having someone visit each of the sites.

Answer: See answer to 12 and we expect that all sites that process data for financial systems will need to be tested. Testing of physical security controls should be based on the FISCAM requirements and other applicable policy. The extent of testing needed at each detachment will be determined by the contractor, in coordination with DoDIG, to ensure that adequate coverage of the general controls are tested and an opinion can be expressed.

18. Statement of Work, page 2, section 3.0. "Application controls are directly related to individual computerized applications owned and operated by DISA to manage, operate, and secure the computing environment."

Is the requested testing limited to DISA owned applications that support the development of DISA financial statements?

Answer: No, see the answer to question 12.

19. Statement of Work, page 2, section 3.1. "Locations…"

Will the IG DoD please provide an overview of the size and number of general support/ application systems at each DECC? This information will significantly affect the overall level of effort.

Answer: The location of applications systems and the systems administration of those systems is currently changing on a weekly basis as a result of our workload transformation. Location information will only be meaningful as specific systems to be tested and related timelines are identified. However, one aspect of the transformation, that should reduce the travel requirements, is that Defense Finance and Accounting Service (DFAS) workload is being consolidated to a smaller number of sites.

20. Statement of Work, page 11, section 6.2. "The contractor is responsible for obtaining employee security clearances, where required, and for providing proof of such clearances to each site visited."

Please clarify the security clearance requirement for performing test work at DISA. This will help ensure the most appropriate resources are committed to this project. Specifically, what level of clearance will be required of contractor staff to obtain physical access to DISA data centers and to perform controls testing activities such as reviewing security software settings and performing vulnerability assessments? In addition, will interim security clearances be acceptable?

Answer: See answer to question 6 and the security requirement for unescorted access to DISA data centers is a SECRET clearance. Yes, interim clearances will be recognized.

21. Statement of Work, page 13, section 6.14.1. "The COR will measure the contractor's performance against the standards and other guidance associated with performing this audit."

Please specify and elaborate on what is meant by "other guidance."

Answer:Guidance as identified in section 4 of the SOW

<u>General Comment</u>

Insight into DISA information assurance program should begin with a visit to their Field Security Office in Chambersburg, Pennsylvania. They have overall corporate level responsibility for the information assurance program within Computing Services and can prepare the winning vendor an overview of what to expect at field locations.

We will arrange for the winning vendor to receive an overview of the Computing Services workload transformation to aid in developing the audit plan. This transformation involves relocation of hardware and workload, as well as remote management of systems. This type of change is going on almost every weekend, so site-specific information is almost meaningless without very specific dates. In addition, the transformation events impacting specific sites should be taken into account in the scheduling of any audit visits to ensure key people are available to work with the audit team.