Enclosure 29 – IS Security Review Questions

System No.	Overall Review Finding:	Reviewed By:	Date:

Administrative

	YES	NO	N/A
8-202. Has the contractor obtained written accreditation for the SSP?			
8-202a. If no, was interim approval granted? Up to 180 Days☐ 181 to 360 Days☐			
8-202. Did the contractor begin processing classified information before interim approval or written accreditation?			
8-202a. If interim approval was granted, has the specified time period expired?			
8-202g. Has the Information System Security Manager (ISSM) been authorized self-approval authority?			
8-202g. If yes, does the ISSM certifying all IS under the Master SSP?			
ISL 01L-1. If yes, does the ISSM provide notification to DSS?			
8-202d. Does the IS require reaccreditation based on 3 year limit?			
8-202e. Has accreditation been withdrawn?			
8-202f. Has accreditation been invalidated?			
8-202e. If withdrawn or invalidated, has memory and media been sanitized?			
Responsibilities			
8-101b. Has contractor management published and promulgated an IS Security Policy?			
8-101b. Has an ISSM been appointed?			
8-103. If yes, are the ISSM's duties and responsibilities being carried out?			
8-104. Has the ISSM designated one or more Information System Security Officer(s) (ISSOs)?			
8-104. If yes, are the ISSO(s) duties and responsibilities being carried out?			
8-307. Are the privileged users duties and responsibilities understood?			
8-307. Are the general users responsibilities identified and understood?			
System Security Plan (SSP)			
8-402. What protection level (PL) is authorized? PL 1☐ PL 2☐ PL 3☐ PL 4☐			
8-401. Highest level of data processed? Confidential☐ Secret☐ Top Secret☐			
User Requirements			
Table 4. Clearance level of privileged users: Confidential ☐ Secret ☐ Top Secret ☐			
Table 4. Clearance level of general users: Confidential☐ Secret☐ Top Secret☐			

	YES	NO	N/A
Table 4. Do the users understand the need-to-know requirements of the authorized PL?			
8-303a. How is the user granted access to the IS? User-IDs☐ Personal identification☐ Biometrics☐			
ISL 01L-1. If passwords are used, does the user understand his/her responsibility for password creation deletion, changing, and length?			
8-311. Is the "user" involved in configuration management (i.e., adding/changing hardware, software, etc)?			
8-311. If yes, does the user understand and following the configuration management plan?			
IS Hardware			
8-311a. Does the SSP reflect the current hardware configuration?			
8-311d. If not, does the maintenance logs reflect changes in the hardware configuration?			
8-306a. Does the IS equipment bear appropriate classification markings?			
Physical Security			
8-308. How is the IS physically protected? (Check all that apply) Closed Area☐ Restricted Area☐ IS Protected Areas☐ Approved Containers☐ PDS [1]☐ Approved Locks☐ Access Control Devices☐ Alarms☐ Guards☐ Patrols☐ Seals☐ Other (Specify)☐ [1] Protected Distribution System Intrusion Detection System☐			
5-800. If closed area, are all construction requirements met?			
5-306. Is access controlled by cleared employee, guard or supplanting access control device?			
5-306. If access is controlled by cleared employee, what criteria is used before granting access?			
5-312. If access is controlled by a supplanting access control device, are all requirements met?			
5-307. If required, is supplemental protection provided by guards or an approved IDS?			
5-307b. If supplemental protection is provided by guards, are all requirements met?			
5-900. If supplemental protection is provided by an IDS, are all requirements met?			
5-306a. Is open shelf or bin storage of classified information, media or equipment approved?			
NSTISSI 7003. If classified wirelines leave the closed area, are all PDS construction requirements met?			
NSTISSI 7003. If PDS is used, are all inspection requirements followed?			
NSTISSI 7003. If PDS is used, do they contain unclassified wirelines?			
NSTISSI 7003. If closed area has false ceilings or floors, are transmission lines not in a PDS inspected at least: Monthly (Security In-Depth)☐ Weekly (No Security In-Depth)☐			
8-502b. If restricted or IS protected area, is the IS downgraded before/after use?			
ISL 01L-1. If seals are used to detect unauthorized modification, are the DS2 website guidelines followed?			

	YES	NO	N/A
ISL 01L-1. If seals are used, does the audit log reflect why the seal was replaced?			
8-308c. Is visual access to the IS or classified information obtainable by unauthorized individuals?			
Software			
ISL 01L-1. Are contractor personnel that handle system or security related software appropriately cleared?			
8-302a. Does the contractor follow the installation procedures identified in the SSP?			
8-306c. Is the media on which software resides write-protected and marked as unclassified?			
8-306c. Is non-changeable media (e.g. CD read-only) appropriately handled and marked?			
8-202c. Is security related software evaluated before use?			
8-305. Is software from an unknown or suspect origin used?			
8-305. If used, how is the software validated before use?			
8-305. Is software tested for malicious code and viruses before use?			
8-305. Are incidents involving malicious software handled in accordance with SSP procedures?			
8-502d. Is a dedicated copy of the operating system software maintained?			
Media			
8-306. Is media labeled to the classification level of the data?			
5-300. Is media appropriately safeguarded when not in use?			
ISL 01L-1. Are approved procedures followed when unclassified media is introduced into the system?			
Security Audits			
ISL 01L-1. Are all appropriate Audit entries recorded?			
8-602a. Are processing times reasonable (i.e., hours between breaks)?			
8-602. Are the protection requirements for each audit requirement recorded?			
8-602a. Are the Audit Logs/Records reviewed weekly?			
8-602a. Is the reviewer authorized and briefed on what and how to review the audit records?			
8-602. Does the reviewer understand his/her responsibility for handling audit discrepancies?			
8-602/ISL 01L-1. Are audit Logs/Records retained for 12 months?			
Security Awareness			
8-103a. Has the contractor implemented an IS training program?			
8-103a. Are users briefed before access is granted?			
IS Operations			
8-502. If possible, have the user step through the security level upgrading procedures.			
8-502. Is the user responsible for clearing memory and buffer storage?			

	YES	NO	N/A
8-502. If yes, does the user know how to clear memory and buffer storage?			
8-502. Is magnetic media cleared/sanitized before and after classified processing?			
8-310. Does the user understand his/her responsibility for handling/reviewing data and output (in-use controls)?			
8-310/ISL 01L-1. Does the user follow approved procedures when doing a trusted download?			
8-310/ISL 01L-1. If possible, have the user step through the security level downgrading procedures.			
Maintenance and Repair			
8-304a. Is maintenance done at the contractor's facility with cleared personnel?			
8-304a. If yes, is need-to-know enforced?			
8-304b. Is maintenance done at the contractor's facility with uncleared personnel?			
8-304b. If yes: are the maintenance personnel U.S. citizens?			
8-304b. does the escort understand his/her responsibilities?			
ISL 01L-1. does the audit log reflect the escorts name?			
ISL 01L-1. Is diagnostic or maintenance done from a remote location using secured/nonsecured comm. lines?			
ISL 01L-1. Is maintenance physically done away from the contractor's facility?			
8-304b(4) If uncleared maintenance personnel, is a dedicated copy of the operating system software maintained?			
8-304b. Is the system and diagnostic software protected?			
8-304b. Is the entire IS or individual components sanitized before/after maintenance?			
8-103. Has the ISSM approved the use of maintenance tools and diagnostic equipment?			
Media Cleaning, Sanitization and Destruction			
8-502. Is the user responsible for clearing memory (volatile/nonvolatile)?			
8-502. Is the user responsible for sanitizing memory (volatile/nonvolatile)?			
ISL 01L-1. If yes, does the user annotate the audit records?			
8-502. Ask the user to describe or step through the procedure.			
8-502. Is the user responsible for clearing magnetic storage media?			
8-502. Is the user responsible for sanitizing magnetic storage media?			
ISL 01L-1. If yes, does the user annotate the audit records?			
8-502. Ask the user to describe or step through the procedure?			
ISL 01L-1. Is an approved overwrite utility used to clear or sanitize magnetic media?			
ISL 01L-1. If yes, does the user annotate the audit records?			
IA Web site. Does the contractor have approved procedures for the destruction of non-magnetic media (e.g. Optical Disks)?			
ISL 01L-1. What level magnetic tape is used? Type I☐ Type II☐ Type III☐ Unknown☐			
ISL 01L-1. Does the contractor use an approved tape degausser to sanitize magnetic			

	YES	NO	N/A
tapes?			
If yes, what level tape degausser? Type I☐ Type II☐ Type III☐ Unknown☐			
If yes, does the user annotate the audit records?			
If yes, does the contractor verify the tape degausser is within NSA specifications?			
ISL 01L-1. Does the contractor follow approved procedures for clearing/sanitizing Printers?			
STU-III			
Does the contractor use a STU-III for classified data transmission?			
If yes, are users briefed on proper use and security practices?			
Are installed terminals supported by a COMSEC account or hand carry receipt?			
Are installed terminals in controlled areas?			
Does the SSP reflect the outside STU-III connections?			