APPENDIX F
SECURITY INSPECTION CHECKLIST

This Security Inspection Checklist should be used as discussed in Chapter 1, paragraph 1-206, when conducting self reviews. Each checklist should be marked with the appropriate security classification markings and declassification instructions. **Core Compliance Items (CCI) are identified in *blue italic font*.** (Note: In addition to the references provided, local Activity or individual Agency/Component Service policy, procedures, and regulations may also apply).

Code / No.	Question	References	Yes	No	N/A
A. SECURITY MANAGEMENT					
A-1	Has the contractor implemented the provisions of the JAFAN 6-0 on initial contract award or modification or subsequent modification? (Note: Implementation must be within 6 months of publication of the JAFAN 6-0 via a Contract Security Classification Specification (DD Form 254))	6/0: 1-102c & Foreword			
A-2	Are requests for waivers to established SAP policies and procedures only submitted when they are in the best interest of the Government?	6/0: 1-106a			
A-3	In those cases where waivers are required, has the waiver request been submitted to the service component SAPCO or designee via the PSO's chain of command?	6/0: 1-106b			
A-4	Within 90 days of electing to implement commensurate protective measures, has the PSO notified the service component SAPCO of the commensurate level of protection and requested validation/final approval?	6/0: 1-107			
A-5	Are PSOs appointed, in writing, by the SAPCO or designee?	6/0: 1-200a(1)			
A-6	Are GSSOs appointed, in writing, and assigned to specific facilities/projects/ subcompartments? Are copies of appointment letters provided to the PSO?	6/0: 1-200a(2)			
A-7	Are CPSOs appointed, in writing, and assigned to specific facilities/projects/ subcompartments? Are copies of appointment letters provided to the PSO?	6/0: 1-200a(2)			
A-8	*Does the SAP Security Officer have the position, responsibility, and authority commensurate with the degree of SAP security support required?*	*6/0: 1-200b*			
A-9	Has the GSSO/CPSO prepared comprehensive SOPs to implement the security policies & requirements unique to their facilities?	6/0: 1-201			
A-10	Are proposed SOPs and SOP changes forwarded to the PSO for approval?	6/0: 1-201			

Code / No.	Question	References	Yes	No	N/A
A-11	*Has an annual self-inspection been conducted by GSSO/CPSO (as appropriate) and did it address issues reflected in the "Security Inspections Checklist" found in JAFAN 6-0, Appendix F?*	*6/0: 1-206d*			
A-12	Are self-inspection reports submitted to the PSO within 30 days following completion of the inspection?	6/0: 1-206d			
A-13	Is the PSO notified immediately if the inspection discloses the loss, compromise or suspected compromise of classified material?	6/0: 1-206d			
A-14	Are self-inspection reports retained for two years following the formal government CSA inspection?	6/0: 1-206d			
A-15	Are all outstanding items *(i.e., those with on-going corrective actions)* completed prior to the destruction of the self-inspection?	6/0: 1-206d			
A-16	Are instances of Government and Industry fraud, waste, abuse and corruption reported through channels designated by the service component SAPCO?	6/0: 1-207			
A-17	Is the name and telephone number for the current FWAC manager or monitor prominently displayed throughout each SAPF?	6/0: 1-207b			
A-18	If multiple SAPs are located within a SAPF, has a CUA been executed between PSOs prior to occupancy?	6/0: 1-210			
A-19	Where there is co-utilization of SCI within a SAPF, or SAP within a SCIF, has authorization from the PSO & the servicing SSO been obtained?	6/0: 1-210b			
A-20	Are the GPM and PSO notified in advance of any Arms Control Treaty Visits?	6/0: 1-300f			
A-21	Is the PSO made aware of any litigation actions that may pertain to the SAP, to include the physical environments, facilities or personnel or as otherwise directed by the GPM?	6/0: 1-300g			
A-22	*Are all security violations reported within 24 hours of discovery to the CPSO/GSSO/PSO, as appropriate?*	*6/0: 1-301*			
A-23	Are violations involving contractor personnel reported by the PSO using the appropriate Defense Security Service (DSS) SAP channels?	6/0: 1-301			
A-24	Has the PSO promptly advised the service component SAPCO in all instances where national security concerns would impact on collateral security programs or clearances of program-accessed individuals?	6/0: 1-301			

Code / No.	Question	References	Yes	No	N/A
A-25	Has the security official of the affected facility determined the scope of the corrective action taken in response to a security infraction/violation and reported it to the PSO?	6/0: 1-301			
A-26	Are security infractions documented and made available for review by the PSO during visits?	6/0: 1-301a(2)			
B. SECURITY PLANNING					
B-1	When a badge system is considered necessary has it been documented in the facility SOP & address topics such as badge accountability, storage, inventory, disposition, destruction, format & use?	6/0: 1-202			
B-2	Is a badge system in place to permit total personal identification & access level determinations (unless the program area is small enough (normally less than 25 people))?	6/0: 1-202			
B-3	When all individuals within a SAPF cannot be personally identified, has a badging system been implemented by the PSO?	6/0: 1-202			
B-4	Are TEMPEST Requirement Questionnaires (TRQ) submitted when processing data on an information system?	6/0: 10-100b			
B-5	Has the PSO, with guidance from a CTTA, determined if countermeasures are required based upon the completed TRQ?	6/0: 10-100b			
B-6	Are OPSEC plans/surveys accomplished to identify, define, and develop countermeasures to vulnerabilities?	6/0: 10-400			
C. PERSONNEL SECURITY					
C-1	Does the GSSO/CPSO possess a personnel security clearance at least equal to the highest level of classified information for which they require access? Possess access to all SAPs assigned to the facility(s) for which he/she is responsible?	6/0: 1-200c(1) & (2)			
C-2	*Do personnel possess access to all SAPs assigned to the facility(s) for which he/she is responsible?*	*6/0: 1-200c(4)*			
C-3	*Are all briefed personnel reporting to the PSO any information which may adversely reflect on the Program-briefed employee's ability to properly safeguard classified Program information?*	*6/0: 1-300a*			
C-4	Is all travel outside the continental United States, Hawaii, Alaska and the U.S. possessions (i.e., Puerto Rico) reported to the GSSO/CPSO thirty days in advance?	6/0: 1-300e & 1-303			
C-5	Has the CPSO/GSSO notified the PSO before program accessed personnel travel to any country, with special emphasis on travel to countries identified on the National Security Threat List?	6/0: 1-300c			

Code / No.	Question	References	Yes	No	N/A
C-6	Is a written report of all changes in the personal status of SAP indoctrinated personnel provided to the PSO?	6/0: 1-300c			
C-7	Have personnel determined to have had unauthorized or inadvertent access to classified SAP information: (1) been interviewed to determine the extent of the exposure, and; (2) been requested to complete an Inadvertent Disclosure Form (see SAP Format 5)?	6/0: 1-301b			
C-8	Has the PSO been made aware of any reports which affect the baseline facility clearance or any incident of a personnel security clearance nature?	6/0: 1-300 & 2-100			
C-9	Has the PSO forwarded all reportable information to the appropriate officials (i.e. Special Access Program Central Adjudication Facility (SAPCAF), CI commands/agencies, etc)?	6/0: 1-300			
C-10	*Do SAP-accessed personnel have a valid need-to-know and certification that he/she will materially and directly contribute to the Program?*	*6/4: 1.2c*			
C-11	Is SAP Format 2 "Special Access Information Agreements" signed prior to briefing an individual approved for access?	6/0: 1-300b			
C-12	Does the access data base or listing will contain the name of the individual, position, billet number (if applicable), level of access, social security number, and security clearance information?	6/0: 2-205			
C-13	*Has every individual accessed to a SAP been given an initial indoctrination? Are these indoctrinations conducted by the PSO/GSSO/CPSO or designee?*	*6/0: 3-101*			
C-14	Has a formal debriefing program been developed?	6/0: 3-102a			
C-15	Do formal debriefings include: (1) how to obtain a release before publishing, (2) what can & cannot be discussed or placed in resumes & applications for security clearances, (3) turning in all holdings, (4) applicability of & penalties for engaging in espionage, (5) where to report suspected Foreign Intelligence Service (FIS) contacts or any attempt by unauthorized persons to solicit program data and, (6) appropriate espionage laws and codes.	6/0: 3-102a(1) through (6)			
C-16	Has a SAPIA been executed at the time of the debriefing and forwarded to PSO within two business days?	6/0: 3-102			

Code / No.	Question	References	Yes	No	N/A
C-17	If attempts to locate an individual either by telephone or mail are not successful, and the whereabouts of the individual cannot be determined in 30 days; is the individual administratively debriefed (i.e,, completion of a debriefing form, annotating the form with "INDIVIDUAL NOT AVAILABLE- ADMINISTRATIVELY DEBRIEFED")? Is the appropriate database updated to reflect this?	6/0: 3-103			
C-18	Are Foreign Travel briefings and debriefings conducted for all accessed personnel prior to and following return of travel using SAP Format 6, Notification of Foreign Travel, or its SCI community equivalent form (either are acceptable)?	6/0: 3-104			
C-19	Do individuals processed for program access meet the prerequisite personnel clearance and/or investigative requirements?	6/4: 1.2c & 3.2			
C-20	Does the candidate nomination package contain a completed PAR, a copy of the nominee's PSQ (SF 86/86c or eQIP printout - current within one year) and results of the Local Records Check (if legally available)?	6/4: 3.3b			
C-21	When the candidate's nomination package is ready to be forwarded to the Government PSO, has the CPSO completed the PAR, to include their signature, date of signature, concurrence and a check to ensure all pertinent attachments are identified and included, as appropriate?	6/4: 3.3d			
C-22	Do Letters of Compelling Need (LOCN) accompany those access approval requests which require a waiver? Do LOCNs describe the candidate's unique skills or knowledge and the benefit to the program?	6/4: 4.3.d(4)			
C-23	*Are those candidate nomination packages that cannot be mitigated at the 2nd Tier level forwarded to the SAPCAF for action?*	*6/4: 7.1*			
C-24	When an access eligibility determination is unfavorable, has the SAPCAF issued a Letter of Intent (LOI)?	6/4: 7.4			
C-25	Has the CPSO or GSSO provided the LOI to the candidate?	6/4: 7.4			
C-26	When a candidate is unsuccessful in his/her appeal, has the SAPCAF forwarded the candidate a Letter of Denial (LOD) or Letter of Revocation (LOR)?	6/4: 7.5			

Code / No.	Question	References	Yes	No	N/A
D. ACCOUNTABILITY					
D-1	Are TOP SECRET engineering notebooks permanently bound documents and each page numbered consecutively, front and back?	6/0: 4-201a & d			
D-2	Are the outer covers and each page of TOP SECRET engineering notebooks marked with the highest classification and program identification(s) contained in the notebook?	6/0: 4-201b			
D-3	Has a Top Secret Control Official (TSCO) been designated in writing?	6/0: 5-201e			
D-4	*Has an annual 100 percent inventory of accountable SAP classified been conducted by the TSCO or alternate and a disinterested party?*	*6/0: 5-202*			
D-5	Are these inventories conducted by sighting all copies of accountable material held within the facility?	6/0: 5-202			
D- 6	*Has all TOP SECRET SAP information been entered into a PSO approved document control accountability system whenever it is received, generated or dispatched either internally or externally to other SAPFs?*	*6/0: 5-201a*			
D- 7	Is each item of TOP SECRET SAP material numbered in series and identified with an individual copy number and total copy count?	6/0: 5-201f			
D- 8	Do all TOP SECRET working papers have a cover sheet marked with the date of origin, originator's name and the annotation "WORKING PAPER"?	6/0: 5-203			
D- 9	Are all TOP SECRET SAP working papers EITHER entered into the accountability system OR destroyed after 30 calendar days from the date of origin?	6/0: 5-203b			
E. CLASSIFICATION AND MARKING					
E-1	*Does each SAP have a Security Classification Guide to identify Critical Program Information (CPI)?*	*6/0: 4-101*			
E-2	Are challenges to SAP classified information and/or material classifications forwarded through the PSO to the appropriate Original Classification Authority (OCA)?	6/0: 4-101			
E-3	Has a DD Form 254, Contract Security Classification Specification Requirements, been prepared for each contractor performing work on SAPs?	6/0: 4-103			
E-4	Is all SAP material marked and controlled in accordance with JAFAN 6-0, NISPOM (baseline marking requirements), the program SCG, and other program guidance?	6/0: 4-200			

Code / No.	Question	References	Yes	No	N/A
E-5	*Do cover sheets when used as a Record of Disclosure will remain affixed to TOP SECRET documents at all times? Does the Record of Disclosure include the identity of all persons given access to the information and the date of the disclosure?*	*6/0: 4-202 & 5-201a*			
E-6	Is Unclassified HVSACO information safeguarded IAW Appendix "A"?	6/0: Appendix "A"			
F. REPRODUCTION					
F-1	Is program material only reproduced on equipment approved by the PSO?	6/0: 5-600			
F-2	Have the GSSOs/CPSOs prepared written reproduction procedures?	6/0: 5-600			
F-4	Is reproduction equipment positioned to assure immediate and positive monitoring?	6/0: 5-600			
F-5	Has a notice indicating if equipment can or cannot be used for reproduction of classified material been posted?	6/0: 5-600			
F-6	Are procedures approved in writing by the PSO (including clearing of equipment, accessing of operators, clearing of media, handling malfunctions, etc.) when reproduction equipment is used outside a SAPF (i.e. TSWA)?	6/0: 5-600			
G. DESTRUCTION					
G-1	Upon contract close-out, are requests for retention of classified information submitted to the Contracting Officer through the PSO for review and approval?	6/0: 5-700			
G-2	Has the contractor submitted a request to the Contracting Officer through the PSO for authority to retain classified material beyond the end of the contract performance period?	6/0: 5-701			
G-3	Is all classified waste destroyed as soon as possible (not allowing materials to accumulate beyond 30 days unless approved by the PSO)?	6/0: 5-704			
G-4	Is classified waste residue inspected during each destruction to ensure that classified information cannot be reconstructed?	6/0: 5-705			
G-5	Has the PSO reviewed and approved all destruction procedures?	6/0: 5-703			
G-6	Are destruction certificates completed and signed by both of the individuals completing the destruction immediately after destruction is completed?	6/0: 5-706			

H. PHYSICAL SECURITY					
H-1	Has the SAPF been formally accredited in writing by a government PSO or designee prior to conducting any SAP activities?	6/9: 1.1.4			
H-2	Has an accreditation checklist (e.g., JAFAN 6/9, Annex A, SAPF Fixed Facility Checklist) been completed and approved by the PSO?	6/9: 2.2.1			
H-3	Are PEDs, with the exception of the following, prohibited within a SAPF: (1) Electronic calculators, spell checkers, language translators, etc. (2) Receive-only pagers. (3) Audio and video playback devices. (4) Receive only Radios. (5) Infrared (IR) devices that convey no intelligence data (text, audio, video, etc.), such as an IR mouse and/or remote controls. (6) Medical, life and safety portable devices.	6/0: 5-900			
H-4	Are entry/exit inspections conducted to deter the unauthorized removal of classified material, and deter the introduction of prohibited items or contraband?	6/9: 2.7			
H-5	Has the PSO instituted procedures for control of electronic devices and other items introduced into or removed from the SAPF?	6/9: 2.8.1			
H-6	When conditions warrant, has a TSCM evaluation been requested (at the discretion of the PSO)?	6/9: 2.3.3			
H-7	Are combinations changed immediately whenever: • a combination lock is first installed or used? • a combination has been subjected, or believed to have been subjected to compromise? • whenever a individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock? • at other times when considered necessary by the PSO?	6/9: 2.6.1			
H-8	Has co-location/co-utilization of Sensitive Compartmented Information within a SAPF been authorized via PSO?	6/9: 2.4.2			

Code / No.	Question	References	Yes	No	N/A
I. ACCESS CONTROL					
I-1	Is a written/electronic visit notification coordinated in advance & acknowledged/ approved prior to visiting a SAPF (via hardcopy/electronic transfer/database)?	6/0: 6-100			
I-2	Has the GPM or his/her designated representative approved all visits between program activities? Has the PSO or designee certified the accesses to the facility?	6/0: 6-101a(1)			
I-3	Are twelve-month visit certifications not authorized unless approved in writing by the PSO?	6/0: 6-101b			
I-4	Are all visit requests transmitted via PSO-approved channels (via hardcopy/electronic transfer/database)?	6/0: 6-100			
I-5	Has the PSO/GSSO/CPSO or his/her designated representative immediately notified all recipients of the cancellation or termination of visit requests?	6/0: 6-101g			
I-6	Is positive identification of each visitor made using an official State or Federal-issued identification card/credential with a photograph?	6/0: 6-101d			
I-7	Are non-program accessed visitors continuously escorted and their movements closely controlled while in a SAPF?	6/0: 6-101f			
I-8	Are advance arrangements coordinated between the visitor, the visitor's cognizant security officer and the destination facility's security officer regarding the hand carrying of program material?	6/0: 6-101(3)			
I-9	Has use of internal warning systems been considered or employed along with other additional methods (e.g., verbal announcements) to warn or remind personnel of the presence of uncleared personnel?	6/0: 6-101f			
I-10	Are all non-program briefed personnel (e.g., maintenance workers, repair technicians, etc) required to complete the visitor's record and be escorted by a resident program-briefed individual?	6/0: 6-102			
I-11	Has a separate program visitor's record been established for program briefed visitors? Does it show the visitor's name, last four digits of the individual's SSN, organization or firm, date, time in and out, and sponsor on the log?	6/0: 6-103			
I-12	Are program meetings and conferences conducted only in approved SAPFs? *(Note: PSOs may authorize additional locations, i.e. Temporary Secure Working Area (TSWA))*	6/0: 6-200			

Code / No.	Question	References	Yes	No	N/A
J. COMPUTER SECURITY					
J-1	Does a formal IA Program exist with all required Documentation available, current and complete? a. Certification and Accreditation b. Delegations of Authority c. MOUs & CUAs d. SSP/SSAA and other procedural documents e. Guest systems documentation f. Audit documents	J-1: 6/3: 2.B.6.c(1) J-1: 6/3: 9.F.2 a: 6/3: 2.B.4.c; 9.D.4 b: 6/3:2.B.2.b(3) b: 6/3:9.D.3.b(1) c: 6/3: 9.D.2.b(2) d: 6/3:2.B.7.c(3) d: 6/3:9.C.3 e: 6/3: 8.B.6 f: 6/3: 4.B.1.b(2) f: 6/3: 4.B.2.a(4)(c)			
J-2	Does a Configuration Management program appropriate for the PL exist? a. Is it a formally documented process? b. Does it address all aspects of hardware & software management. c. Does it address maintenance and disposition of equipment	J-2: 6/3: 5.B.1.a(2) a: 6/3: 2.B.7.c(7) b: 6/3: 5.B.1.a(2)(b) c: 6/3: 8.B.5.e c: 6/3: 8.B.8.c(7)			
J-3	Does a formal IA Training Program exist that addresses all users: a. IAM/ISSM/ISSR duties b. SysAdmin and privileged users c. Regular Users d. Special Requirements (DTO etc)	J-3: 6/3: 8.B.1.a a: 6/3: 2.B.5.c(9) a: 6/3: 8.B.1.b b: 6/3: 8.B.1.c(1) c: 6/3: 8.B.1.c(2) d: 6/3: 8.B.1.b(4)			
J-4	Does a media management plan exist that addresses the following: a. Does it address ALL media in the facility b. Are formal procedures for data extraction/data transfer approved and in use c. Does the plan address media movement & day to day management d. Are sanitization/disposition procedures in place for ALL media types in use e. Are appropriate markings and labeling procedures in use	J-4: 6/0: 8-101 a: 6/0: 8-102 b: 6/3: 8.B.3 c: 6/0: 8-102 d: 6/3: 8.B.5 e: 6/3: 8.B.2.a			

Code / No.	Question	References	Yes	No	N/A
K. TRANSMISSION					
K-1	If transmission by a commercial courier is anticipated, has the PSO approved its use?	6/0: 5-400b			
K-2	Is all classified SAP material prepared, reproduced, and packaged by program-briefed personnel in SAPFs?	6/0: 5-401			
K-3	Are receipts for the transmission of all classified (SECRET/TOP SECRET) material used/ maintained?	6/0: 5-401a			
K-4	Is tracer action initiated when a receipt or acknowledgment of a shipment of material is not returned within 30 days?	6/0: 5-401b(1)			
K-5	Are Two-Person courier teams used for all handcarry of TOP SECRET/SAP data unless a single-person courier is approved in advance by the cognizant PSO?	6/0: 5-402a			
K-6	Are problems encountered by couriers while enroute will be immediately reported to the PSO?	6/0: 5-402e			
K-7	Are Courier Authorization letters (i.e., SAP Format 28) or card *(see below)* issued by the PSO/GSSO/CPSO from the departure location outlining the courier procedures? (1) Does the Courier Authorization and pre-departure instructions address the: a) method of transportation, b) travel itinerary (intermittent/ unscheduled stops, remain-overnight scenarios, etc), c) specific courier responsibilities (primary/alternate roles-as necessary), and d) completion of receipts (as necessary) and full identification of the classified data being transferred and e) a discussion of emergency/contingency plans (include after-hours POCs, primary/alternate contact data, telephone numbers, etc) (2) Has each courier will acknowledge receipt/understanding of this briefing in writing. (3) In the case of experienced program-briefed individuals who frequently or routinely perform duties as classified couriers, are they issued Courier Authorization cards by the PSO/GSSO/CPSO in lieu of individual letters for each trip? (4) Are courier cards revalidated/reissued annually?	6/0: 5-402c(1) & (2)			

Code / No.	Question	References	Yes	No	N/A
K-8	*Is Top Secret material transmitted only by authorized means (e.g., 2-person courier, secure electronic means)?*	*6/0: 5-402a & 5-403*			
K-9	Is SAP information double-wrapped using opaque material which precludes observation of contents?	6/0: 5-401c			
K-10	When secure facsimile and/or electronic transmission is permitted, has the PSO approved the system in writing?	6/0: 5-403			
K-11	When a U.S. Postal mailing channel is approved by the PSO, is mail received only by appropriately cleared and accessed personnel?	6/0: 5-404			
K-12	Are problems, misdeliveries, losses, or other security incidents encountered with transmission of SAP information immediately reported to the the PSO?	6/0: 5-404e			
K-13	Before any movement of classified SAP assets are transportation plans developed and approved by the PSO at least 30 days in advance of the proposed movement?	6/0: 5-404f			
K-14	Are two program briefed personnel destroying accountable classified program material?	6/0: 5-702			
K-15	Are receipts maintained IAW Appendix "C" (five year period)?	6/0: Appendix "C"			
L. SECURITY EDUCATION					
L-1	*Have all individuals received initial and refresher training per Table 1, JAFAN 6-0, and topics covered as listed on SAP Format 17?*	*6/0: 3-100 & Appendix "G"-SAP Format 17*			
L-2	Have GSSOs/CPSOs ensured that the Security Education & Training program meets specific and unique requirements of individual SAPs?	6/0: 3-100			
L-3	Has each individual reviewed their eQIP/SF86 printout on an annual basis and updated it as necessary? *(Note: annual refresher training sessions are a good opportunity to accomplish this)*	6/0: 3-101			
M. CONTRACTING					
M-1	When a subcontractor does not have the requisite facility clearance, has the prime CPSO initiated the necessary FCL paperwork and submitted it to the PSO? Has the PSO coordinated with DSS to initiate action to provide the subcontractor a facility clearance?	6/0: 7-101			

Code / No.	Question	References	Yes	No	N/A
M-2	In the pre-contract phase, has the prime contractor advised the prospective subcontractor (prior to any release of SAP information) of the procurement's enhanced special security requirements? Have arrangements for subcontractor program access been pre-coordinated with the PSO?	6/0: 7-102			
M-4	Has the CPSO completed a SAP Format 13, Subcontractor/Supplier Data Sheet, and submitted it to the PSO?	6/0: 7-102			
M-5	Has the CPSO included the reason for considering a subcontractor and attached a proposed DD Form 254 to the SAP Format 13? *(Note: The DD Form 254 shall be tailored to be consistent with the proposed support being sought.)*	6/0: 7-102			
M-6	Are DD Form 254s prepared by prime contractor CPSOs and forwarded to the PSO for approval (before signature by the prime contractor and release to subcontractors)? Have PSOs coordinated these DD Form 254s with the GPM and Government Contracting Officer (GCO)?	6/0: 7-103			
N. GUARD FORCE					
N-1	Within the U.S. at at CLOSED storage SAPF, is a response force capable of responding to an alarm within 15 minutes after annunciation and a reserve response force available to assist the responding force?	6/9: 3.1.1.1			
N-2	Within the U.S. at at OPEN storage SAPF, is a response force capable of responding to an alarm within 5 minutes after annunciation and a reserve response force available to assist the responding force?	6/9: 3.1.2.1			
N-3	Are response force personnel appropriately trained and equipped according to SOPs to accomplish initial or follow-up response to situations that may threaten the SAPF's security?	6/9: Annex B, para 5.2.2			
N-4	Is the IDE maintained by US citizens? *(Note: Non-US citizens shall not provide these services without prior written approval by the PSO)*	6/9: Annex B, para 5.3.1			
N-5	Is the alarm monitoring station continuously supervised and operated by US citizens who are trained alarm monitors, cleared to the SECRET level?	6/9: Annex B, para 5.1.1			

O. SPECIAL EMPHASIS ITEMS