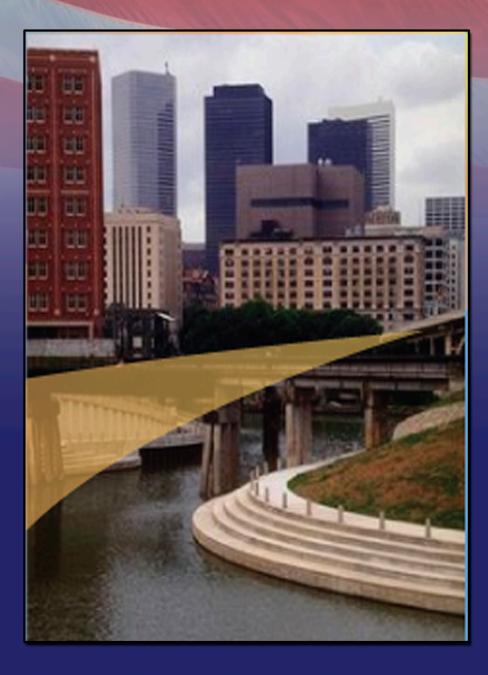
Self Inspection Handbook for NISP Contractors





October 2006

Self-Inspection Handbook for NISP Contractors TABLE OF CONTENTS

The Contractor Security Review Requirement	. 1
The Contractor Self-Inspection Handbook	
The Elements of Inspection	
Inspection Techniques	
Interview Techniques	

ELEMENTS OF INSPECTION

Α.	FACILITY CLEARANCE
В.	ACCESS AUTHORIZATIONS
C.	SECURITY EDUCATION 4
D.	CONSULTANTS
E.	STANDARD PRACTICE PROCEDURES (SPP)5
F.	SUBCONTRACTING
G.	VISIT CONTROL
Н.	CLASSIFIED MEETINGS 6
I.	CLASSIFICATION 6
J.	EMPLOYEE IDENTIFICATION7
K.	FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE
L.	PUBLIC RELEASE
Μ.	CLASSIFIED STORAGE
N.	CONTROLLED ACCESS AREAS 9
О.	MARKINGS 10
Ρ.	TRANSMISSION 10-11
Q.	CLASSIFIED MATERIAL CONTROLS 11
R.	REPRODUCTION 12
S.	DISPOSITION
Т.	INFORMATION SYSTEMS 13-17
U.	COMSEC/ CRYPTO 18
V.	INTERNATIONAL OPERATIONS 18-20
W.	OPSEC
Х.	SPECIAL ACCESS PROGRAMS

INSPECTION ADDENDUM

Suggested Questions When Interviewing Uncleared Employees	22
Suggested Questions When Interviewing Cleared Employees	22-24
The Program Specific Self-Inspection Process	24-25
A Program Specific Self-Inspection Scenario	25
The Program Manager Interview	25-26
Employee Interviews	

SELF-INSPECTION HANDBOOK FOR NISP CONTRACTORS

The Contractor Security Review Requirement

"Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles." [1-206b, NISPOM]

The Contractor Self-Inspection Handbook

The National Industrial Security Program Operating Manual (NISPOM) requires all participants in the National Industrial Security Program (NISP) to conduct their own security reviews (self-inspections). The Self-Inspection Handbook is designed as a job aid to assist you in complying with this requirement. It also suggests various techniques to help you enhance the quality of your self-inspections.

The Elements of Inspection

The Self-Inspection Check List contained within this handbook addresses basic NISPOM requirements through a series of questions arranged according to "Elements of Inspection." Before beginning your self-inspection, review the "Elements of Inspection" to determine which ones are applicable to your facility's involvement in the NISP. Use those elements which you have identified as pertaining to your security program to create your self-inspection check list.

The first three Elements of Inspection: (A) Facility Security Clearance (FCL), (B) Access Authorizations, and (C) Security Education must be covered during the self-inspection of all cleared facilities. Any remaining elements need only be covered if they relate to your security program. If you have questions about the relevancy of any element of inspection for your facility, please contact your IS Representative for guidance. A look at your Standard Practice Procedure (SPP), if you have one, may also provide clues. Of course, as your program becomes more involved with classified information (e.g., changing from a non-possessing to a possessing facility), you will have to expand your self-inspection checklist to include those additional elements of inspection. Also remember that not all of the questions (requirements) within each element may relate to your program. Since each question includes a NISPOM paragraph citation, review each requirement against the context of your industrial security program. If your involvement with classified information invokes the requirement, your procedures should comply with it and your self-inspection should assess your compliance. Reading all questions in the relevant elements of inspection will help you become more knowledgeable of the NISPOM requirements. In all cases, the regulatory guidance takes priority over company established procedures.

Inspection Techniques

To get a clear picture of your facility's security posture, you must (1) know the requirements by which you are inspected (this is where the check list will help), (2) know your facility's physical layout (i.e., where the classified material is stored, worked on, etc.), and (3) have knowledge of the processes involved in the classified programs at your facility. Remember, your primary sources of information are *documents* and *people*.

Your job as the FSO is to *verify* and *validate* that your facility security program is properly protecting classified material and information. To do this, simply review the self-inspection questions against the appropriate documentation (including the classified information) and the people (including their actions) involved in the facility's industrial security program. This is where the self-inspection check list comes in handy. It not only provides you with the NISPOM requirements, but organizes them into elements of common security concern. These elements should not be viewed independently during your self-inspection, but interdependently, as it will become obvious to you that they frequently interrelate.

Interview Techniques

A quality self-inspection depends on your ability to ask questions which may identify security problems. Seek information about *current* procedures and *change*s which could affect future actions. Get out of your office and into the facility working environment. Talk to the people!

- All questions should be considered in the present and future sense.
- Let people tell their story. Ask open ended questions (using who, what, where, when, why and how).
- Let people show you how they perform their job while handling classified information.
- Follow-up the check list questions with your own questions.
- □ Keep good notes for future reference and corrective action.

	The Self-Inspection Check List			
A. FACIL	ITY CLEARANCE			
NISPOM REF:	Question:	YES	NO	N/A
1-302g(3)	Have all changes (e.g. changes in ownership; operating name or address; KMP information; previously reported FOCI information or action to terminate business) affecting the condition of the FCL been reported to your DSS IS Rep?			
1-100c	Has the fact that the company has an FCL been used for advertising or promotional purposes?			
2-104	Are the senior management official, the FSO, and other Key Management Personnel cleared as required in connection with the FCL?			
2-106a-b	Have the proper exclusion procedures been conducted for uncleared company officials?			
2-108	Does the home office have an FCL at the same or higher level than any cleared facility within the Multiple Facility Organization?			
2-111	Are the DD Forms 441 and/or 441-1, SF 328, and DD Form 381-R, available, properly executed and maintained in current status?			

B. ACCE	SS AUTHORIZATIONS			
NISPOM REF:	Question:	YES	NO	N/A
	Have you validated all the information in JPAS / JCAVS pertaining to your cleared employees ?			
	Does each employee's JCAVS record indicate an appropriate "eligibility" and "access?"			
	Have all JCAVS users and account managers been officially appointed, issued unique user names and passwords and given the appropriate level in the JPAS / JCAVS?			
	Have all JCAVS users received training appropriate for their duties and responsibilities?			
2-200d	Are the number of clearances held to a minimum consistent with contractual requirements?			
2-202a	Are employees in process for security clearances notified in writing that review of the SF 86 is for adequacy and completeness only and that the information will be used for no other purpose within the company?			
2-202b	Are procedures in place to ensure that the applicant's SF 86 and fingerprint cards are authentic, legible and complete to avoid clearance processing delays?			
2-202b	Are original, signed copies of the SF 86 and Releases retained until the applicant's eligibility for access to classified has been granted or denied, and then destroyed?			
2-205	Are all pre-employment offers based on acceptance to begin employment within 30 days of granting eligibility for a PCL?			
2-207	Has citizenship been verified for each PCL applicant?			
1-302	Have reports on all cleared employees been submitted to the DISCO or the DSS IS Rep as required? NOTE: JCAVS may be used for submission of some of these reports.			

C. SECUR	C. SECURITY EDUCATION					
NISPOM REF:	Question:	YES	NO	N/A		
3-102	Have you, as the FSO, completed security training considered appropriate by the CSA ?					
3-103, 9- 202	Are Government special security briefings and debriefings provided by DSS or GCA when required?					
3-104	Do cleared persons at other locations receive the required security training?					
3-105	Are SF 312's properly executed by cleared employees prior to accessing classified and forwarded to DISCO for retention?					
3-105	Are refusals to execute the SF 312 reported to DISCO?					
3-106	Do initial security briefings contain the minimum required information?					
3-107	Does the security education program include refresher security briefings?					
1-205, 3- 100 - 3-108	Are all cleared employees provided with security training and briefings commensurate with their involvement with classified information?					

Conduct personnel interviews in the work place during inspection tours of the facility and determine the effectiveness of your security education program. What do the employees remember from the last security briefing? Have them demonstrate the application of security procedures in their job function.

3-108	Are cleared employees debriefed at the time of a PCL termination, suspension, revocation, or FCL termination?		
1-300	Are there established internal procedures that ensure cleared employees' awareness of their responsibilities for reporting pertinent information to the FSO, the FBI, and other Federal authorities as required?		
1-301,302	Is there an effective procedure for submission of required reports to the FBI, the DSS, and DISCO?		
1-304	Is there a graduated scale of administrative disciplinary action in the event of violations or negligence?		
1-204	Does management support the industrial security program? This NISPOM section is titled "Cooperation with Federal Agencies and Credentialed Reps of Those Agencies" The wording is not a clear link with the actual NISPOM requirement, which relates to cooperating in investigations		
1-207	Are employees aware of the Defense Hotline?		

D. CONS	D. CONSULTANTS						
	Question:	YES	NO	N/A			
REF:							
2-212	Have you and your consultants jointly executed a "consultant certificate"						
	setting forth your respective security responsibilities?						
2-212	Does the consultant possess classified material at his/her place of						
	business?						

For security administrative purposes, the consultant shall be considered an employee of the using contractor.

E. STANDARD PRACTICE PROCEDURES (SPP)					
NISPOM	Question:	YES	NO	N/A	
REF:					
1-202	Is the SPP current and does it adequately implement the requirements of				
	the NISPOM?				

Remember that a written SPP must be prepared when the FSO or the CSA believes it is necessary for the proper safeguarding of classified. 1-202

F. SUBCONTRACTING				
NISPOM REF:	Question:	YES	NO	N/A
7-101	Are all required actions completed prior to release or disclosure of classified information to sub-contractors?			
7-101b(1)	Are the clearance status and safeguarding capability of all subcontractors determined as required?			
7-101b(2)	Do requests for facility clearance or safeguarding include the required information?			
7-101c	Is sufficient lead-time allowed between the award of a classified subcontract and the facility clearance process time for an uncleared bidder?			
7-102	If your company is the prime on a contract, have you incorporated adequate security classification guidance into each classified subcontract?			
7-102	Are contractor-prepared <i>Contract Security Classification Specifications</i> (DD 254) signed by a designated contractor official?			
7-102a	Are original <i>Contract Security Classification Specifications</i> (DD 254) included with classified solicitations?			
7-102b	Are revised Contract Security Classification Specifications (DD 254) issued as necessary?			
7-103	If your company is the prime on a contract, have you obtained approval from the Government Contracting Activity for subcontractor retention of classified information associated with a completed contract?			

G. VISIT	CONTROL			
NISPOM	Question:	YES	NO	N/A
REF:				
6-101	Are classified visits held to the minimum?			
6-101	Are procedures established to ensure positive identification of visitors prior to disclosure of classified?			
6-101	Are procedures established to ensure that visitors are only afforded access to classified information consistent with their visit. (i.e., need-to-know)?			
6-102	Is disclosure of classified information based on need to know (a contractual relationship) or an assessment that the receiving contractor has a bona fide need to access classified information?			
6-104	Are visit authorization requests sent and received through JCAVS whenever possible?			
6-104	Do visit authorization requests include the required information, and are they updated to reflect changes in the status of that information?			
6-105	Are long-term visitors governed by the security procedures of the host contractor?			

H. CLAS	H. CLASSIFIED MEETINGS (sponsored by the Government)					
NISPOM REF:	Question:	YES	NO	N/A		
6-201	Has the government agency sponsoring the meeting approved all security arrangements, announcements, attendees, and the meeting location?					
6-201a	Did your request for authorization include all required information?					
6-201c	Have all security arrangements been approved by the authorizing agency?					
6-201c (2)	Is attendance limited to persons appropriately cleared who have the need-to-know?					
6-201c (3) and 6-202	Is prior written authorization obtained, from the relevant Government Contracting Activity, before disclosure of classified information?					

Remember that classified presentations can be delivered orally and/or visually. Copies of classified presentations, slides, etc. shall not be distributed at the meeting, but rather safeguarded and transmitted as require d by the NISPOM. 6-201 (3)

6-202b	Has a copy of the disclosure authorization been furnished to the		
	Government agency sponsoring the meeting?		

Authority to disclose classified information at meetings, whether by industry or government, must be granted by the Government Contracting Activity having classification jurisdiction. [6-202]

6-203	Are your employees properly screened for clearance and need-to-know		
	prior to attending classified meetings?		

I. CLASS	IFICATION			
NISPOM REF:	Question:	YES	NO	N/A
4-102	Are employees designated to perform derivative classification actions sufficiently trained and do they have access to appropriate classification guidance?			
4-102b	Is all derivatively classified material appropriately marked?			
4-103	Is all classification guidance adequate and is the <i>Contract Security</i> <i>Classification Specification</i> provided as required?			
4-103	Do you possess a <i>Contract Security Classification Specification</i> for every classified contract issued to your company?			
4-103c	Upon completion of a classified contract, did proper disposal of the relevant classified information take place or is the classified material being retained for two years?			
4-104	Is improper or inadequate classification guidance being challenged?			
4-105	Is contractor-developed information appropriately classified, marked, and protected?			
4-107	Are downgrading and declassification actions accomplished as required, and is action taken to update records when changing the classification markings?			

J. EMPLO	J. EMPLOYEE IDENTIFICATION				
NISPOM	Question:	YES	NO	N/A	
REF:					
5-410b	Do personnel possess the required identification card or badge when				
	employed as Couriers, Handcarriers or Escorts?				

Security procedures should maximize the use of personal recognition verification for access to classified material. Note that the NISPOM makes only passing reference to IDs and badges for use in specific instances. When such programs are employed as part of your security-in-depth procedures, the specifics should be reviewed with your IS representative.

	IGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI) to Completion of the SF 328 should be used to ensure your SF 328 contain	e curro	nt and	
accurate in		13 Curre	in and	
NISPOM REF:	Question:	YES	NO	N/A
	The following questions apply to all contractors:			
2-302	Have there been changes in any of the information previously reported on your SF 328?			
2-302a	Has the presence of any/all FOCI factors been reported to your DSS IS Rep in the manner prescribed?			
2-302b	Does the SF 328 "Certificate Pertaining to Foreign Interests" contain current and accurate information? Has the most current information pertaining to the SF 328 been provided to your DSS IS Rep?			
2-302b	Has your DSS IS Rep been notified of negotiations for merger, acquisition, or takeover by a foreign interest?			
	The following questions apply to facilities involved with FOCI:			
2-302b	Has a FOCI Negation Plan been submitted to your DSS IS Rep?			
2-303c	If cleared under a Special Security Agreement, has your company received the special authorization needed to access "proscribed information?" Proscribed information is TOP SECRET/Restricted Data/Communications Security/Special Access Programs and Sensitive Compartmented Information. The special authorization must be manifested by a favorable national interest determination that must be program/project/contract specific from the appropriate Government Contracting Activity.			
2-306	Has a Government Security Committee been appointed from the Board of Directors under a Voting Trust, Proxy Agreement, Special Security Agreement (SSA), or Security Control Agreement (SCA)?			
2-307	Have you developed a Technology Control Plan (TCP), approved by the DSS, when cleared under a Voting Trust, Proxy Agreement, SSA, or SCA?			
2-308a	If operating under a Voting Trust, Proxy Agreement or Security Control Agreement, does your senior management officials meet annually with the DSS to review the effectiveness of the arrangement?			
2-308b	Is an annual Implementation and Compliance Report submitted to your DSS IS Rep?			

Visit the FOCI webpage found on the DSS website – <u>www.dss.mil</u> – for sample FOCI Negation Plans, Technology Control Plan, electronic copy of SF 328 and instructions.

L. PUBL	L. PUBLIC RELEASE					
NISPOM	Question:	YES	NO	N/A		
REF:						
5-511	Was approval of the Government Contracting Activity obtained prior to					
	public disclosure of information pertaining to a classified contract?					
5-511a	Is a copy of each approved "request for release" retained for one					
	inspection cycle for review by your DSS IS Rep?					

M. CLAS	SIFIED STORAGE			
NISPOM	Question:	YES	NO	N/A
REF:				
5-101	Do your cleared employees know where they can and can't hold			
	classified discussions?			
5-102a	Is there a system of security checks at the close of each working day to			
	ensure that classified material is secured?			
5-103	Is a system of perimeter controls maintained to deter or detect			
	unauthorized introduction or removal of classified from the facility?			
5-103	Are signs posted at all entries and exits warning that anyone entering or			
E 404	departing is subject to an inspection of their personnel effects?			
5-104	Are procedures developed for the safeguarding of classified material			
5 000	during an emergency?			
5-302	Is TOP SECRET classified stored only in approved GSA security			
	containers, approved vaults, or Closed Areas with supplemental			
5-303	protection? If SECRET material is stored in containers as described in 5-503, is		ł – –	
5-303	supplemental protection being used during non-working hours?			
5-	Is supplemental protection provided for all SECRET material NOT stored			
3- 303,307	in GSA-approved containers or vaults?			
5-306	Are Closed Areas constructed in accordance with the requirements of		ł – –	
0 000	the NISPOM?			
5-306b	Has DSS approval been granted for the open storage of documents in			
	Closed Areas?			
5-308	Is the number of people possessing knowledge of the combinations to			
	security containers minimized?			
5-308a	Is a record of the names of people having knowledge of the			
	combinations to security containers maintained?			
5-308b	Are security containers, vaults, cabinets, and other authorized storage			
	containers kept locked when not under direct supervision of an			
	authorized person?			
5-308c-d	When combinations to classified containers are placed in written form,			
_	are they marked and stored as required?			
5-309	Are combinations to security containers changed by authorized persons			
	when required?			
5-311	Are General Services Administration-approved containers repaired as			
	required by the NISPOM?			
5-313a	Do ID cards or badges, used in conjunction with Automated Access			
	Control Systems, meet NISPOM standards?			

N. CON	N. CONTROLLED ACCESS AREAS						
NISPOM REF:	Question:	YES	NO	N/A			
5-303	Are supplemental controls in place for storage of SECRET material in Closed Areas?						
5-305	Do Restricted Areas have clearly defined perimeters and is all classified material properly secured when the area is unattended?						
5-306	Are persons without the proper clearance and need-to-know escorted at all times when in a Closed Area?						

The CSA may grant self-approval authority for closed area approvals. [5-306]

5-306	Are Closed Areas afforded supplemental protection during non-working		
	hours?		

Supplemental Controls are not required for SECRET classified storage during non-working hours if Security-In-Depth has been approved. See definition of Working Hours, Apx. C, NISPOM.

5-312	If Supplanting Access Control Systems are used, do they meet NISPOM criteria,		
	5-313 & 5-314, and were they approved by the FSO prior to installation?		

Watch entrances to Closed Areas to determine the procedure employed when supplanting access control devices are utilized. Are authorized users allowing unauthorized persons to piggy-back into the area?

5-900	Is IDS approved by DSS prior to installation as supplemental protection		
5-901	and does it meet NISPOM or UL 2050 standards as required?		
5-307	Do intrusion detection systems (IDS), utilized as supplemental		
5-900	protection, meet NISPOM requirements?		

When guards are authorized as supplemental protection [5-307b], required patrol is two hours for TOP SECRET and four hours for SECRET.

Remember that GSA-approved security containers and approved vaults secured with locking mechanisms meeting Fed. Spec. FF-L-2740 and located in areas determined by the CSA to have security-in-depth do not require supplemental protection. [5-307c].

5-902b	Are trained alarm monitors cleared to the SECRET level in continuous		
	attendance when the IDS are in operation?		
5-902d	Are alarms activated at the end of business?		
5-902d-e	Are alarm records maintained as required?		
5-903a	Does the Central Alarm Station report failure to respond to alarm		
(3)	incidents to the CSA as required?		

Commercial Central Station Alarm Company guards do not require a personnel clearance unless their duties afford them the opportunity to access classified material when responding to those alarms. [5-903a(2)]

5-904	Are all IDS at the contractor facility installed by UL-listed installers and		
5-905	so certified?		
5-904,	Has a UL 2050 CRZH certificate been issued?		
905			

O. MAR	KINGS			
NISPOM	Question:	YES	NO	N/A
REF:				
4-200	Is all classified material, regardless of its physical form, marked properly?			
4-201				
4-202	Is all classified material marked to show the name and address of the			
	facility responsible for its preparation and the date of preparation?			
4-203	Are overall markings marked conspicuously as required?			
4-206	Are portions of classified documents properly marked?			
4-207	Do markings for subject lines and titles immediately following the item?			
4-202,	Are all additional markings applied to classified as required?			
4-208				
4-210	Are special types of classified material marked as required?			

Special types of classified material includes: 1) files, folders or groups of documents; 2) E-mail and other electronic messages; 3) messages; 4) microforms; and 5) translations

4-213	Are appropriate classification markings applied when the compilation of unclassified information requires protection?		
4-216	Are downgrading/declassification notations properly completed?		

Contractors must seek guidance from the GCA prior to taking any declassification action on material marked for automatic declassification. If approved by the GCA, all old classification markings shall be cancelled and new markings substituted whenever practical. [4-216a]

5-203	When classified working papers are generated are they dated when created, marked with the overall classification and annotated "Working		
	Papers," and destroyed when no longer needed?		

P. TRAN	ISMISSION			
NISPOM	Question:	YES	NO	N/A
REF:				
5-202	Are procedures established for proper receipt and inspection of classified			
5-401	transmittals?			
5-401	Is classified information properly prepared for transmission outside the			
	facility?			
5-401	Are receipts included when classified transmission requires?			
5-401b	Is a suspense system established to track transmitted documents until			
	the signed receipt is returned?			
5-402	Are authorized methods used to transmit classified outside the facility?			
5-403				
5-404				

Remember that transmission of TOP SECRET, outside the facility requires written authorization from the Government Contracting Authority. 5-402

Additionally, TOP SECRET material may never be transmitted through the U.S. Postal Service.

2-100	Is the facility clearance and safeguarding capability of the receiving facility determined prior to transmission of classified?		
5-408	Does the contractor use a qualified carrier, authorized by the Government, when shipping classified material?		

5-408	Are classified shipments made only in accordance with the NISPOM or		
5-409	instructions from the contracting authority?		
5-410	Are Couriers, Handcarriers, and Escorts properly briefed?		
Requiren	nent to maintain receipt and dispatch records is eliminated.		

 5-410
 Is handcarrying of classified material outside the facility properly authorized, inventoried, and safeguarded during transmission?

 5-411
 Is handcarrying aboard commercial aircraft accomplished in accordance with required procedures?

 5-412
 Are sufficient numbers of escorts assigned to classified shipments and are they briefed on their responsibilities?

Change: The requirement for escorts apply only when an escort is necessary to ensure the protection of classified information during transport. 5-412

For information concerning international transfer of classified, see International Operations. 10, Sec. 4

Q. CLAS	Q. CLASSIFIED MATERIAL CONTROLS				
NISPOM	Question:	YES	NO	N/A	
REF:					
5-100	Do your cleared employees understand their safeguarding responsibilities?				

Facility walk-throughs are a good way to determine employee knowledge of safeguarding classified when inuse. Interview and observe how classified is handled in the work place.

5-200	Is your information management system capable of facilitating the		
	retrieval and disposition of classified material as required?		

Test your system for document retrieval by conducting <u>forward</u> and <u>reverse</u> checks of your classified holdings. Take a sample of classified material from your information management register and attempt to locate it within your facility. Conversely, conduct spot checks at sample locations throughout the facility where classified is stored. Identify items and determine if they are reconciled in the information management system.

5-201a	Are TOP SECRET control officials designated at facilities possessing		
	TOP SECRET classified?		
5-201a	Are TOP SECRET accountability records maintained as required and is an annual inventory conducted?		
5-202	Is all classified material received at the contractor facility and delivered directly to designated personnel?		
5-102	Are security checks to ensure proper storage of classified materials conducted at the end of each working day?		
5-103	Does the contractor maintain a system of controls to deter or detect unauthorized introduction or removal of classified from the facility?		
1-300 1-303	Are your cleared employees aware of their responsibility to promptly report the loss, compromise, or suspected compromise of classified?		
5-104	Are procedures adequate to protect classified during emergencies?		

Conduct a walk-through inspection during lunch breaks, after hours, and on late work shifts, if classified is being accessed, to determine the actual state of security at your facility.

R. REPF	RODUCTION			
NISPOM REF:	Question:	YES	NO	N/A
	Does the equipment used for classified reproduction have any sort of memory capability? If yes, the equipment may require accreditation as an information system.			
5-600	Is reproduction of classified material kept to a minimum?			
5-600	Is the reproduction of classified accomplished only by properly cleared, authorized, and knowledgeable employees?			
5-601	Is reproduction authorization obtained as required?			
5-602	Are reproductions of classified material reviewed to ensure that the markings are proper and legible?			

Any review of classified reproduction should include concern for waste, copy overruns, etc., any materials used in production which may retain classified information or images requiring destruction or safeguarding and for the type of copier machine used (any copier that retains any type of memory may have to be accredited as an information system rather than a copier.

5-603	Is a record of reproduction maintained for accountable material and is it		
	retained as required?		

Remember, the NISPOM requires a formal accountability system for Top Secret material, and an Information Management System for Secret and Confidential material. [5-201; 5-203]

S. DISPO	DSITION			
NISPOM	Question:	YES	NO	N/A
REF:				
5-700b	Is a program established to review classified holdings on a recurring			
	basis for the purpose of reduction?			
5-701	Is the disposition of classified material accomplished in accordance with			
	the required schedule?			
5-702	Is retention authority requested as required?			
5-704	Is classified material destroyed as soon as possible after it has served its purpose?			
5-705	Is an effective method of destruction employed that meet NISPOM standards?			
5-706	Is classified material destroyed by authorized personnel (may include appropriately cleared subcontractor personnel) who fully understand their responsibilities?			

The NISPOM requires two persons for the destruction of TOP SECRET and one person for the destruction of SECRET and CONFIDENTIAL.

5-707	Are proper records maintained for the destruction of TOP SECRET classified and do those who sign have actual knowledge of the material's destruction?		
5-708	Is classified waste properly safeguarded until its timely destruction?		

System No.	Overall Review Finding: Rev	riewed By:	Date:		
	Administrati				
NISPOM REF:	Question:	ve	YES	NO	N/A
8-202.	Has written accreditation for the SSP been obtained from	DSS?			
8-202a.	If no, was interim approval granted? Up to 180 Days				
8-202.	Did the user begin processing classified information before accreditation?	re interim approval or written			
8-202a.	If interim approval was granted, has the specified time pe	eriod expired?			
8-202g.	Has the Information System Security Manager (ISSM) be	een authorized self-certification authority?			
8-202g.	If yes, does the ISSM certify all IS under the Master SSF	?			
	If yes, does the ISSM provide notification to DSS?				
8-202d.	Does the IS require reaccreditation based on 3 year limit	?	1		
8-202e.	Has accreditation been withdrawn?				
8-202f.	Has accreditation been invalidated?				
8-202e.	If withdrawn or invalidated, has memory and media been	sanitized?			
	Responsibili	ties		1	
8-101b.	Has management published and promulgated an IS Sec	urity Policy?			
8-101b.	Has an ISSM been appointed?				
8-103.	If yes, are the ISSM's duties and responsibilities identifie	d and being carried out?			
8-104.	Has the ISSM designated one or more Information Syste	m Security Officer(s) (ISSOs)?			
8-104.	If yes, are the ISSO(s) duties and responsibilities identified	ed and being carried out?			
8-307.	Are the privileged users' duties and responsibilities ident	ified and understood?			
8-307.	Are the general users responsibilities identified and under	erstood?			
	System Security P	lan (SSP)			
8-402.	What protection level (PL) is authorized? PL 1	PL2 PL3 PL4 PL4			
8-401.	Highest level of data processed? Cont	fidential 🗌 Secret 🗌 Top Secret 🗌			
	User Requirem	nents		1	
Table 4.	Clearance level of privileged users Confid	ential 🗌 Secret 🗌 Top Secret 🗌			
Table 4.	Clearance level of general users Confic	lential 🔲 Secret 🗌 Top Secret 🗌			
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 Biometrics	Personal identification			
	If passwords are used, does the user understand his/her deletion, changing, and length?				
8-311.	Is the "user" involved in configuration management (i.e., etc)?				
8-311.	If yes, does the user understand and following the config	uration management plan?			

	IS Hardware					
NISPOM REF:	Question:	YES	NO	N/A		
8-311a.	Does the SSP reflect the current hardware configuration?					
8-311d.	If not, do 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 🗌 IS Defined Perimeter Boundary Area (Restricted Area) 🗌 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?					
5-306b.	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?					
	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?					
	If seals are used to detect unauthorized modification, are the website guidelines followed?					
	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					
	Are contractor personnel that handle system or security related software appropriately cleared?					
8-302a.	Are the installation procedures identified in the SSP being followed?					
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 relevant 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?					

NISPOM REF:	DSSHQ Self Inspection Guide UpdatedSoftware Question:	YES	NO	N/A
		TES	NO	IN/A
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 separate media maintained for periods processing?			
	Media			
8-306.	Is media marked to the classification level of the data?			
5-300.	Is media appropriately safeguarded when not in use?			
	Are approved procedures followed when unclassified media is introduced into the system?			
	Security Audits	·		
	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 Daily			
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	Are audit Logs/Records retained for 12 months?			
	Security Awareness			<u> </u>
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?			
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	Does the user follow approved procedures when doing a trusted download?			
8-310	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?			1
8-304a.	If yes, is need-to-know enforced?			1
8-304b.	Is maintenance done at the contractor's facility with uncleared personnel?		1	1
8-304b.	If yes: are the maintenance personnel U.S. citizens?			1
8-304b	Does the escort understand his/her responsibilities?			+

October 2006

	Maintenance and Repair			
NISPOM REF:	Question:	YES	NO	N/A
	Does the audit log reflect the escort's name?			
	Is diagnostic or maintenance done from a remote location using secured/nonsecured comm.			
	lines?			
	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)?			
	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?			
	If yes, does the user annotate the audit records?			
8-502.	Ask the user to describe or step through the procedure?			
	Is an approved overwrite utility used to clear or sanitize magnetic media?			
	If yes, does the user annotate the audit records?			
IA Website.	Does the contractor have approved procedures for the destruction of non-magnetic media (e.g. Optical Disks)?			
	What level magnetic tape is used? Type I 🗌 Type II 🗌 Type III 🔲 Unknown 🗌			
	Does the contractor use an approved tape degausser to sanitize magnetic 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, is the tape degausser within NSA specifications?			
	Are approved procedures followed for clearing/sanitizing Printers?			
	STU-III			
	Is a STU-III used for classified data transmission?			1
	If yes, are users briefed on proper use and security practices?			
	Are installed terminals supported by a COMSEC account or hand carry receipt?			1
	Are installed terminals in controlled areas?			
	Does the SSP reflect the outside STU-III connections?			1
	If yes, has someone verified the outside connections are authorized and accredited?		1	1

	Networks			
NISPOM REF:	Question:	YES	NO	N/A
8-700.	Are all outside network connections known, authorized and accredited?			
8-700e(3).	If the network leaves the contractor's facility, are NSA approved encryption device(s) used?			
8-700b.	Is this a unified network?			
8-700c.	Is this an interconnected network?			
8-700c.	If yes: does each participating system or network have an ISSO?			
8-700c.	Does the network have a controlled interface?			
8-610a.	Is the contractor following a network security plan?			
8-700.	Is this a contractor only network?			
8-700.	If no, is a DISN circuit being used or has the customer obtained a waiver from DISA?			
	If the network is not contractor only, has a MOU been coordinated between all DAAs?			
	Are data transfers (receipt and dispatch) across the network audited?			

Note: New ISL will address changes to Chapter 8.

U. COMSEC / CRYPTO

The NISPOM does not provide detailed guidance for protection of COMSEC material.

The primary source of information for COMSEC inspections is the NSA, CSS Policy Manual No. 3-16, November 2005.

If you require training and audit information, contact the NSA.

V. INTER	RNATIONAL OPERATIONS			
NISPOM	Question:	YES	NO	N/A
REF:				
	Disclosure of U.S. Information to Foreign Interests			
If YES	Does your company have any classified contracts with foreign interests?			
Continue!				
10-200	Was appropriate export authorization obtained prior to disclosure of			
10-202	classified information?			

Remember that an export authorization is required before the contractor makes a proposal to a foreign person that involves eventual disclosure of U.S. classified information. [10-202]

10-200	Is proper disclosure guidance provided by the Government Contracting Activity?		
10-201	Are requests for export authorizations of significant military equipment or classified material accompanied by Department of State, Form DSP-83, Non-Transfer and Use Certificate?		
10-202	Have the required security provisions and classification guidance been incorporated into the subcontract document for all direct commercial arrangements with foreign contractors involving classified information?		

	Possession of Foreign Classified Information			
NISPOM	Question:	YES	NO	N/A
REF:				
10-300	Has your DSS IS Rep been notified of all contracts, awarded by foreign governments, which involve access to classified information?			
10-302a	Is foreign government information provided protection equivalent to that required by the originator?			
10-304a	Are U.S. documents containing foreign government classified information marked as required by the NISPOM?			
10-306	Is foreign government material stored in a manner that prevents its mingling with other material?			

The receipt of classified material from a foreign source through non-government channels shall be promptly reported to the DSS IS Rep. [10-311]

10-312	Is the subcontracting of contracts involving access to foreign government		
	information conducted in accordance with the NISPOM?		

	International Transfers			
NISPOM REF:	Question:	YES	NO	N/A
10-401	Do all international transfers of classified material take place through channels approved by both governments?			
10-401	Is an appropriate transportation plan prepared for each contract involving international transfer of classified material via freight forwarder or commercial carrier?			
10-404	Does the use of freight forwarders for the transfer of classified material meet the requirements of the NISPOM?			
10-405	Is classified material hand carried outside of the U.S.? If so, is such action always approved by the CSA?			
10-405 b-c	Are couriers provided with a Courier Certificate and do they execute a Courier Declaration before departure?			

Paragraphs (10-405a thru j) provide detailed requirements for employees acting as couriers when hand carrying classified across international boundaries.

10-406	Are all international transfers of classified controlled by a system of continuous receipts?		
10-408	Is adequate preparation and documentation provided for international transfer of classified pursuant to commercial or ITAR exemption? NOTE: For FMS the GCA is responsible for the preparation and approval of the transportation plan.		

	International Visits and Control of Foreign Nationals			
NISPOM REF:	Question:	YES	NO	N/A
10-500	Has a TCP been established to control access to all export controlled information? If yes, are these procedures current?			
10-501 10-506 10-507	Have you established procedures to monitor/control international visits by your employees and by foreign nationals?			

Visit authorizations shall not be used to employ the services of foreign nationals to access export controlled materials; an export authorization is required in such situations. 10-501b

10-506	Are requests for visits abroad submitted on a timely basis?		

The Visit Request format is contained in Appendix B.

10-508	Do you properly control access to classified by on-site foreign nationals?		
10-509			

All violations of administrative security procedures or export control regulations by foreigners shall be reported to the CSA. [10-510]

	Contractor Operations Abroad			
NISPOM REF:	Question:	YES	NO	N/A

The storage, custody, and control of classified information required by U.S. contractor employees abroad are the responsibility of the U.S. Government. Contractors are NOT allowed to store classified information overseas – all storage MUST be under the auspices of the U.S. government.

10-604	Are employees assigned abroad properly briefed on the security requirements of their assignment?		
10-603	Has all transmission of classified information to cleared employees overseas been conducted through U.S. Government channels?		

	NATO Information Security Requirements			
NISPOM	Question:	YES	NO	N/A
REF: 10-706	Are briefings/debriefings of employees accessing NATO classified conducted in accordance with the NISPOM, and are the appropriate certificates and records on file?			

Remember that a personnel clearance is not required for access to NATO RESTRICTED, although a Facility Security Clearance is required. (NISPOM 10-702 & 10-704).

10-709	Are all classified documents properly marked?		
10-710	Have you received adequate classification guidance?		
10-712a	Are NATO classified documents kept separate from other classified documents?		
10-712b	Have the combinations to containers holding NATO classified been changed annually as a minimum?		
10-713	Has all NATO classified been properly received and transmitted?		
10-717	Are the accountability records for NATO classified maintained as required?		
10-721	Are visits of persons representing NATO properly handled and is the visit record maintained as required?		

W. OPS	W. OPSEC				
NISPOM	Question:	YES	NO	N/A	
REF:					
None	Are OPSEC requirements implemented in accordance with contractual				
	documentation provided by the GCA?				

X. SPECIAL	X. SPECIAL ACCESS PROGRAMS (SAP)				
Reference:	Question:	Yes	No		
NISPOM, NISPOM Supplement and DoD	Is this a potential site for arms control inspections under START, OPEN SKIES, Chemical Weapons Convention (CWC) or International Atomic Energy Agency (IAEA)?				
Overprint to the NISPOM Supplement	If Yes: Is the DoD component sponsoring or acting as the executive agent for a SAP providing arms control implementation guidance and direction? Reference: 11-704 DoD Overprint to the NISPOM Supplement				

Is there any Special Access Program contract activity at your company? Note: The FSO should discuss this with the senior management official of the facility.
If Yes: Remember that such programs are subject to NISPOM, NISPOM Supplement, DoD Overprint to the NISPOM Supplement and Program Security Guide requirements. A self inspection of the SAP(s) is required annually IAW 1-206e of the DoD Overprint to the NISPOM Supplement. The Security Review Checklist is found in Appendix J of the Overprint.
If Yes : During the self-inspection it is important for the FSO to coordinate with the internal Contractor Program Security Officer (CPSO) to ensure that individual program security requirements are being followed.

Suggested Questions When Interviewing Uncleared Employees:

- □ What is classified information?
- □ Have you ever seen classified information?
- □ If you found classified information unprotected, what would you do?
- Have you ever heard classified information being discussed?
- Have you ever come into possession of classified materials? How?

Suggested Questions When Interviewing Cleared Employees:

- □ What is your job title/responsibility?
- □ Which contract or program requires the use of your clearance? How?
- □ What is the level of your security clearance?
- How long have you been cleared?
- □ IF RECENTLY CLEARED, WHAT WAS THE PROCESS/STEPS IN APPLYING FOR YOUR SECURITY CLEARANCE ?
- □ When was your last access to classified information and at what level?
- Have you ever accessed classified information outside of this facility?
- □ What are the procedures for going on classified visits? How about visitors coming here for a classified visit?
- Did anyone else from the facility accompany you on this visit?
- □ What procedures did you follow prior to your classified visit?
- Did you take any classified notes or classified information back to the facility?
- □ What procedures were followed to protect this information?
- □ Where is this information now?
- Have you ever allowed visitors to have access to classified information?
- How did you determine their need-to-know?
- Have you ever been approached by anyone requesting classified information?
- Do you ever work overtime and access classified information?
- □ When was the last time that you had a security briefing?
- □ What can you recall from this briefing?

	Can you recall any of the following being addressed in briefings?
	Risk Management Job Specific Security Brief
	 Public Release Adverse Information Counterintelligence Awareness
_	
Ц	What is meant by the term adverse information and how would you report it?
	Can you recall any other reportable items? INSERT QUESTION ABOUT SUSPICIOUS CONTACT REPORTS/REPORTING THIS MAY BE AN UNDEREMPHASIZED/UNDERREPORTED ASPECT
	Have you ever been cited for a security violation, or infraction, or incident?
	What would you do if you committed a security violation or infraction or discovered one?
	Do you know the combination to any storage containers, Closed Areas, etc.?
	WHAT ARE THE SECURITY REQUIREMENTS REGARDING COMBINATIONS TO SECURITY CONTAINERS?
	Who other than yourself has access to these containers?
	HOW TO YOU KEEP TRACK OR MAINTAIN YOUR KNOWLEDGE OF THE COMBINATION?
	Is a record maintained of the safe combination? If so, where?
	Do you generate classified INFORMATION? TELL ME ABOUT IT.
	If so, what controls are established?
	HOW TO YOU KNOW IT'S CLASSIFIED?
	Where do you typically work when you generate classified information?
	What procedures do you follow to protect classified while working on it?
	WHAT DO YOU DO WITH CLASSIFIED INFORMATION? Do you ever use a computer to generate classified information?
	How do you mark this information? WHAT INFORMATION OR REFERENCES TO YOU USE WHEN CLASSIFYING INFORMATION?
	Please produce the classification guidance that you used. Is it accurate?
	Are you aware of the procedures for challenging classification guidance?
	What are the security procedures for publishing classified papers, etc.?
	What procedures do you employ when hand carrying classified material?
	Have you ever reproduced classified information? Describe the procedures.

Have you ever destroyed classified information? What procedures were used?

Do you have any questions regarding security?

NOTE: In addition to asking questions, it is a good idea to ask cleared employees to demonstrate how they perform their security-related tasks, e.g., "Show me how you begin when you work with classified information on your computer" or "Show me how you prepare a package for shipment." This will allow you not only to verify what the correct procedures are, but to ensure those procedures are being carried out and that classified information is being protected.

The Program Specific Self-Inspection Process

Both independent study courses, *Essentials of Industrial Security Management* and *Protecting Secret and Confidential Documents*, identified the security concerns addressed during the self-inspections of non-possessing and possessing facilities. The scenarios described for you the self-inspection efforts of Harold Huxtable, FSO at the Electric Widget Company (EWC). Because EWC is a small facility which performs on one classified contract, any self-inspection effort would be, by default, a program specific inspection.

Are there any benefits to using the program specific approach when conducting the selfinspection of a larger facility with substantial classified involvement on a variety of programs? The program specific self-inspection can help you gain a better understanding of what your company's responsibility is for a particular classified program in addition to providing you insight as to what each person contributes to the effort. The following is provided to explain the program specific self-inspection.

Your DSS IS Rep puts great emphasis on providing recommendations and suggestions to *improve* your security practices. But this can only be accomplished when you have a good grasp of your operations and the manner in which classified information is handled. By taking a detailed look at one or more classified programs and interviewing key individuals to determine what they do and how they handle classified information, you will be able to evaluate how well your facility's *overall* security program is functioning. Many classified programs require a variety of taskings such as manufacturing, report writing, testing, receipt, and transmission, etc. In a program specific inspection, you select one or more programs to be closely examined. This process usually begins with the interview of the program manager (in some facilities this could even be the President) to learn what the program or contract is all about.

Start by asking for a layman's overview of the program, and question the level of classified access required, the procedures for classifying information, what, if any, problems have been experienced, and who in the facility is responsible for what on the program. This leads to interviews with other employees including technical, clerical, and secretarial personnel. During these interviews, you should explore all security requirements connected with the employee's responsibility in the program such as classified material controls, classified storage, markings, classification management, transmission, disposition, security education, and reproduction. Elements of a more administrative nature, relating to the facility's security program, such as the review of visit authorization letters and briefing statements, are ordinarily covered by reviewing your records within the Security Office. The main rule is: if an element is applicable to your facility's classified involvement, cover the element in your self-inspection and, whenever possible, consider using the program specific techniques illustrated below.

You may find that exploring one classified program is not enough to give you a "feel" for how well your security program is functioning. One program may represent only a small part of the classified activity that takes place at your facility. If that's the case, you will want to examine several, if not all, of your classified programs in detail. It's important that you explore each inspection element thoroughly to ensure that your facility is in compliance with the NISPOM. Your underlying concern is that classified information and materials are properly protected and that your employees are knowledgeable of their security responsibilities.

A Program Specific Self-Inspection Scenario

The following scenario illustrates a self-inspection conducted on a specific program. For the purpose of this example, it is not an all-inclusive inspection.

Fenster Dinwiddie, FSO of Capabilities Limited (CL) has decided to focus his self-inspection on the SCUD Intercept Countermeasure (SIC) Project, one of three classified contracts awarded to CL. As we join Fenster, he has accomplished most of the administrative portion of the inspection. He has reviewed Letters of Consent, Briefing Statements, Personnel Security Clearance Change Notifications, etc., and has completed his inventory of all classified materials and records. He has already touched base with the President of CL to make sure there were no recent organizational changes or foreign involvement that he should report. Certain elements like <u>Subcontracting</u>, <u>Consulting</u>, <u>COMSEC</u>, and <u>International Operations</u> do not apply.

Emulating the inspection techniques formerly used by his IS Rep, Fenster has decided to go out on the floor and find out what the employees do and how knowledgeable they are about their security responsibilities.

The Program Manager Interview

Fenster recalled that his IS Rep began each inspection by interviewing the person most knowledgeable about a particular contract. In this case it means talking to Conrad Floot, the lead engineer on the SIC Project.

Fenster went upstairs to "Engineering Row" to locate Conrad. "Fenster!" cheered the engineers as he entered the department. Fenster is always tickled to receive such a salutation. He feels honored to maintain such a congenial relationship with the engineers. After all, he does represent the security department.

"Say, Conrad, can you fill me in on this SIC Project of yours? I'm doing my recurring selfinspection and decided to focus in on your program." Conrad is impressed. No one has ever expressed that much interest in his project before. And he loves to talk, especially about the SIC Project, his "baby" as he prefers to call it. "Sure, what do you need to know, Fence?"

"Well, why don't you start by giving me a program update? You know, what we're doing for the customer, what's classified about it, and things like that. But keep it simple, okay?" Conrad is thrilled. He proceeds to give Fenster a detailed overview of the program, its history, and current status. Fenster is thinking, "You know this is pretty interesting stuff. I should get out on the floor more often."

During the interview, Fenster took careful notes. He discovered that eight other engineers plus a contingent of secretarial and support personnel are working on at least some portion of the program. He decided he would interview each individual over the next couple of days. They discussed the classified design modifications which were being tested down the hall. Fenster had Conrad describe each step of the test procedure including whether aspects of the tests themselves were classified. He asked what makes the design modifications classified, how they're protected, who protects them, how and where they're tested, etc. To his relief, he found that all the procedures at least appeared to be in conformance with the NISPOM. Later, he would interview key members of the test and evaluation staff individually. He never realized there were so many security considerations!

Conrad identified his customer point-of-contact just in case Fenster or the IS Rep needed to call. They spent a lot of time on classification management. Fenster wanted to know what classification guidance had been provided by the customer and whether he felt that it was adequate. He asked what Conrad would do if they were to experience problems in determining what should be classified. They reviewed classified marking procedures, the kind of classified information that's been received, who is allowed access, procedures for generating classified information, reproduction, disposition, transmission, public release, and access authorizations. By the time he was done, Fenster had a pretty good idea of what the SIC Project was all about and whom to talk to for more information.

In addition to addressing the program-specific security concerns, Fenster remembered to question Conrad regarding important overall security program-related issues such as security education, adverse information, and foreign travel.

Employee Interviews

Next, Fenster interviewed each of the engineers on the project. He asked many of the same questions, but this time he was more interested in learning exactly what each person's responsibilities were and how they handled classified information. He already knew a great deal about the program just by talking to Conrad. It was time to "zero in" on the nuts and bolts of the SIC Project. His first stop was at Elmo Platz's office. According to Conrad, Elmo has been involved in the program from the start and, as the assistant program head, has major responsibilities.

First, Fenster asked Elmo to explain his job and how it relates to the SIC Project. Fenster asked what level of access he needed for the job, how he obtained his classification guidance and whether there were any problems in this area that he should be aware of.

There were other questions as well, all designed to determine whether Elmo and his SIC Project staff were following the requirements of the NISPOM. Fenster asked:

How often and under what circumstances did Elmo access classified information?

- □ Was he aware of his adverse information reporting responsibilities?
- Did he generate classified material in-house and, if so, on what equipment?
- How was the information protected?
- Did he have knowledge of the combination to the security container? Was the combination properly safeguarded?
- Did he attend any classified meetings at the customer's site or at CL? Did anyone else from CL attend?

- Did he reproduce classified material? On what equipment?
- □ Was he familiar with the rules on retention, hand carrying, "need-to-know," marking, accountability, and disposition of classified information?
- □ Was he aware of any unreported security violations?
- Did any of his classified work require a special briefing, e.g., NATO?
- □ Was there anything relating to security that he thought Fenster should know about?
- Did he have any classified information that was not logged into the facility's accountability or Information Management System? Where did it come from?

You can see that Fenster was trying to cover all of the relative inspection elements listed in the self-inspection handbook during his interview. This line of questioning was continued with each of the major participants in the SIC Program, from the engineering staff to the mailroom personnel. When he was done, Fenster had covered every pertinent self-inspection element and had discovered only one or two administrative errors. His self-inspection was a success. **We hope yours is, too!**

Security Education, Training and Awareness Directorate Defense Security Service Academy 938 Elkridge Landing Road Linthicum, MD 21090 www.dss.mil