

LESSON 9

Initial Surveys & Security Reviews

In this lesson we'll first discuss surveys, which are done when a facility is initially cleared and when there is any changed condition that would affect the Facility Security Clearance (FCL). These are not inspections, but often a changed condition survey and a security review will be conducted simultaneously. You and the IS Representative will be working together during the survey review process.

Section II of the Security Agreement (DD Form 441) provides for designated representatives of the government to review the security program at your facility at reasonable intervals. The NISPOM paragraph 1-207 provides additional guidance regarding these reviews and also introduces the requirement for your company to conduct formal self-inspections at intervals consistent with risk management principals.

You probably want to know how to prepare for a security review, what will the results be, etc. We'll try to answer these questions, relieve any fears you may have, and help you maintain a good security program.

Besides discussing government reviews, their elements and results, we will discuss contractor self-inspections. We will discuss the NISPOM requirements as well as reasons for conducting self inspections, and how you can use the process to improve your company's security program.

OBJECTIVES

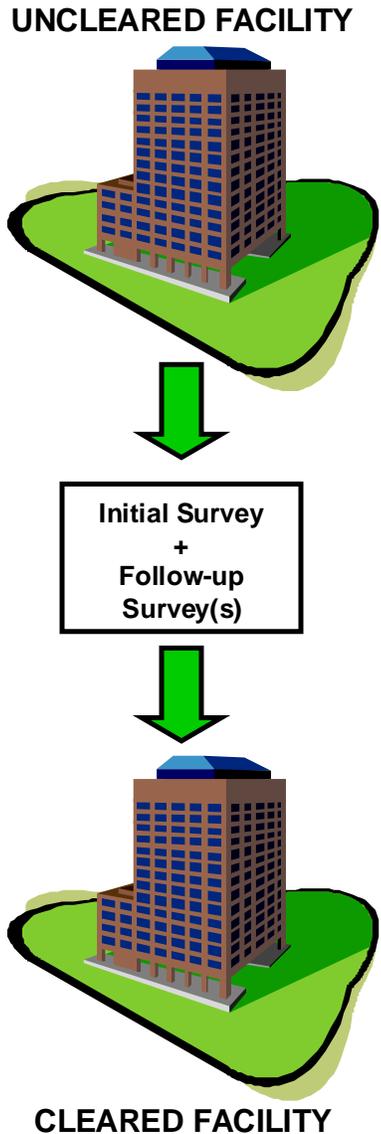
When you have finished this lesson, you should be able to do the following:

- List examples of instances where a "changed condition" survey is called for.
- List examples of when DSS will need to conduct a security review of a facility.
- Identify the areas of concern most commonly covered in the review of a non-possessing facility.
- Differentiate the ratings assigned upon completion of a review and indicate what results will be communicated to top management.
- Indicate when self-inspections are required.
- Explain how self-inspections are conducted.

THE INITIAL SURVEY

A survey is a tool used in the initial clearance of a facility and in the maintenance of that clearance. The *Initial Facility Clearance Survey* was conducted before your facility clearance was issued. The primary purpose of the initial survey was to gather information to determine that your facility was eligible for a clearance. The clearance of your firm was based on the five areas we went over in Lesson 3. The survey, however, focused on four of those areas:

- The Security Agreement
- Foreign Ownership, Control or Influence (FOCI)
- Your business structure
- Personnel Security Clearances (PCL) of Key Management Personnel (KMPs)



The initial survey began when DISCO sent out the basic facility clearance forms the DD Form 441 (the DD Form 441-1, if needed) and the SF 328. EPSQ software was also provided for your facility's KMPs to apply for PCLs. If your facility was near an IS Rep's office, he or she may have brought the forms by in person. However you received the forms, an IS Rep did come to your facility to pick up the completed forms, review the documents pertaining to your facility's business structure, and brief senior management on the National Industrial Security Program (NISP). Depending on the complexity of your facility's operations, a second visit, or *Follow-up Survey*, may have been scheduled. If needed, a third or even fourth visit might have been made. The important thing during the visit was to get your company's security program started.

When the clearances for your KMPs are ready to be granted, DISCO coordinates with the DSS Field Office and issues the Facility Security Clearance. Then DISCO electronically sends the Letters of Consent (LOC) for the KMPs coupled with the Letter of Notification of Facility Clearance (DSS FL-381-R), to your facility. At this point your facility is called, **a cleared facility**.

CHANGED CONDITION SURVEYS

Once the initial survey has been completed why should you be concerned with all of that now? Very simply, just as a personnel security clearance is an ongoing process an estimation of a person's trustworthiness subject to ongoing evaluation over time a Facility Security Clearance is based upon factors which may change over the life of the clearance. After a facility has been cleared, a *changed condition survey* may be required when a change occurs that causes the information reported in the initial survey to be invalid. When the new survey is completed, the facility's status is re-evaluated.

A new survey is prompted when you report changed conditions to your DSS Field Office. You will recall that you need to make a report, for instance when there is a change in your firm's organization (such as a change of ownership) or a physical change (such as change of location).

Not all facility-related reports lead to a new survey. The DSS Field Office determines when a new survey is required. Your responsibility as the FSO in the matter is to file the report. The IS Rep will usually arrange a special trip to your facility, unless a security review has already been scheduled.

What the IS Rep needs to see during the visit is determined by the type of change you reported. If, for example, you reported a change of operating name, the IS Rep would examine the documentation of that change; Papers filed with

the state or local government, business licenses, board resolutions, etc.

GOVERNMENT INSPECTIONS REVIEWS

A government security review is a tool used to assess the effectiveness of the contractor's industrial security program and to assist you, the FSO in directing resources toward efficient and effective security solutions.

The security review, like the survey, is conducted by an IS Rep. If your facility is large enough to warrant it, more than one IS Rep may perform the security review. In some cases the security review may be completed over several months.

FREQUENCY

How often are government security reviews conducted at your facility? Security reviews are normally conducted once a year. Security reviews are conducted every 18 months at facilities that do not possess classified material. Events that may require DSS to conduct a security review in less than a 12 month period would include:

- New counterintelligence (CI) information that indicates a new or increased threat to the facility or its technologies
- Changes in the scope of the facility's classified operations
- User agency concerns
- Major or repeated security violations which indicate that classified information is not adequately protected
- Significant changes to FOCI
- Any new international involvement

NOTIFICATION

A government security review is normally *announced*. This means that as a courtesy, approximately 30 days prior to an announced security review, you will receive written notification from your IS Rep that your security program has been scheduled for review. You may also receive notification by telephone. You will be provided the date(s) of the upcoming security review.

This advanced notification gives you, as the FSO an opportunity to prepare for the security review. You should use this opportunity to ensure that management personnel will be available for discussion with the IS Rep and for the IS Re post-review briefing, and that other employees will be available for interviews. It is recommended that the FSO notifies all employees when a government security review is scheduled. You should also use this time to prepare a list of the classified contracts on which your facility is performing and to ensure that all records pertaining to the security program are available for review.

Unannounced security reviews are conducted by the IS Rep when specific concerns or problems occur at a facility.

NOTE: An IS Rep is considered a classified visitor. The Security Agreement coupled with the IS Rep's credentials and NISPOM paragraph 6-102, provide the authorization for the IS Rep to review your security program without having sent you a visit request.

WHAT IS AN INSPECTION LIKE?

In this section, we'll look at what the government security review of a non-possessing facility entails. The review is relatively simple for facilities that do not possess classified material. The IS Rep will normally be concerned with three basic areas: The status of the facility clearance, the status of personnel security clearances/access authorizations, and the level of security education and awareness at the facility.

The status of the facility security clearance (FCL)

The status of personnel security clearances (PCL)/
access authorizations

The level of security education and awareness at the facility

There might well be additional matters of interest, such as visit control. If the facility has prepared a written Standard Practice Procedures (SPP), the IS Rep will want to review it and see how it is implemented. Even the issue of safeguarding is a concern at facilities which formerly held classified information and are now dormant.

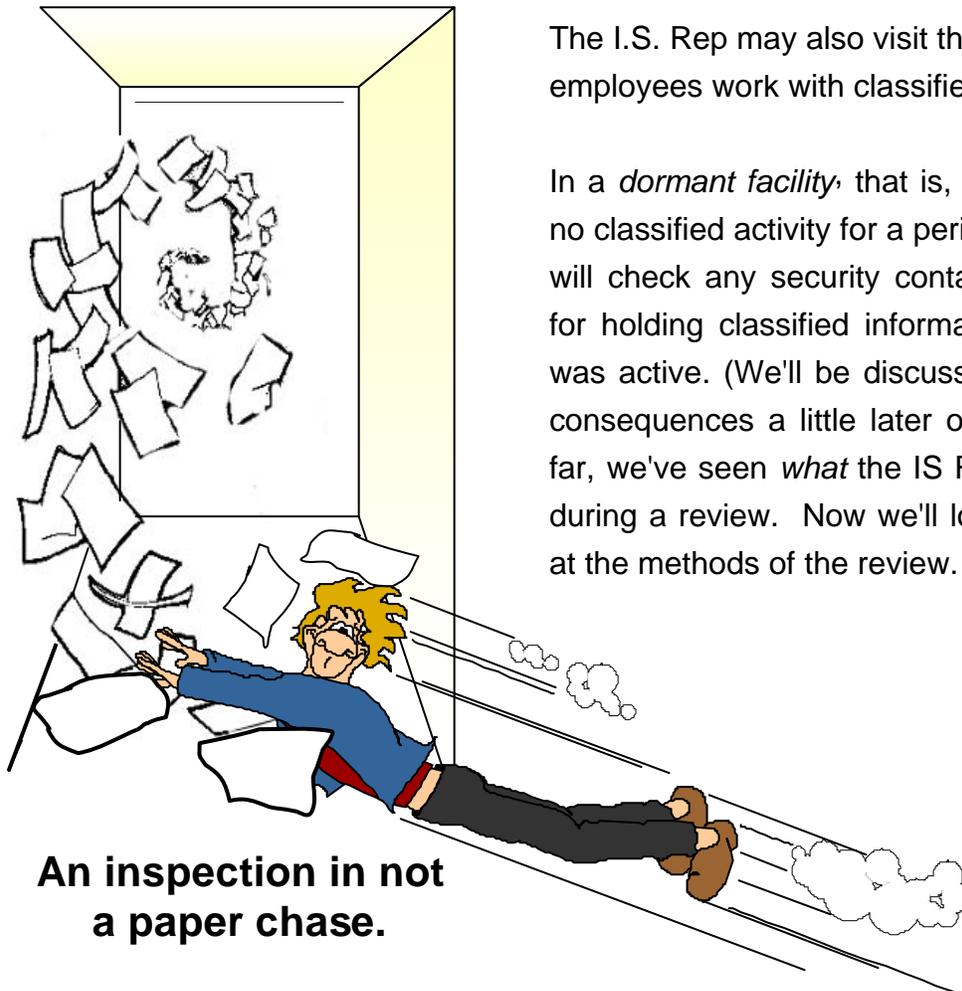
Let's look at the three basic concerns first. In determining the current status of the FCL, the IS Rep will look for any changes in the business structure and any changes affecting those personnel cleared in connection with the FCL (KMPs). The IS Rep will also be interested in whether or not any changes which have occurred have been properly reported. To determine changes in business structure, the IS Rep might look up a number of records, such as business licenses, articles of incorporation, minutes of meetings of the board of directors, minutes of stockholders meetings, and the most recent annual report. The IS Rep may look at any record(s) that tells something about the current status of the business. A knowledgeable official of your firm might be asked to review the Certificate Pertaining to Foreign Interests (SF 312), when applicable, to see if it is accurate and current and to determine any *anticipated* changes in this area.

In checking both the access authorizations and the level of security education, many factors may surface. For example, is there a true need for the clearances? Have all employees requiring clearances been granted them? Are employees holding unnecessary clearances or clearances at an inappropriate level? Have cleared employees been briefed, and are they aware of the security procedures involved in the performance of their duties? Questions of this type are best answered by the employees themselves. Security, after all, is not just a matter of paperwork. The basis for any security program is people, and in order to review your security program the IS Rep will be talking with people in your facility.

The subjects just covered (FCL, PCLs, and Security Education) form the core of any security review. Other areas are looked into as the situation demands. One of these areas almost certain to be addressed is *classified visits*. For a non-possessing facility the primary concern is outgoing visits. The I.S. Rep will be interested in any current visits and the system the FSO uses to keep track of the employees sent out. The IS Rep may also want to talk with some of the employees who have been out on classified visits. As indicated in the lesson on visits, the security responsibility rests with the host facility.

The I.S. Rep may also visit the location where the employees work with classified information.

In a *dormant facility*, that is, a facility that has had no classified activity for a period of time, the IS Rep will check any security containers that were used for holding classified information when the facility was active. (We'll be discussing dormancy and its consequences a little later on in this lesson.) So far, we've seen *what* the IS Rep will be looking for during a review. Now we'll look a bit more closely at the methods of the review.



**An inspection is not
a paper chase.**

INSPECTION TECHNIQUES

The IS Rep will arrive at your facility on the date specified in the letter. The IS Rep will first wish to make contact with you (the FSO) and senior management. During this initial get-together or entrance brief, the IS Rep will discuss the general plan of the review and solicit input from you and your management regarding any issues of security concern or areas of potential focus. In the review of a large facility that is heavily involved with the NISP, this stage is necessarily more complex and the planning of the review may, in fact, be done some days in advance.

While there are a certain number of areas to be reviewed, there is no set order of precedence in which they must be covered. This being the case, it is not possible to tell you, step-by-step, what will be looked at and who will be talked to, in any given order. We have, however, already gone over the items most commonly examined in the course of a review and can now discuss a little of the philosophy behind it.

After the initial meeting with you, the IS Rep will be involved in two types of activity, the *review of various records* and *interviewing personnel at your facility*. In order to gain an accurate picture of your security program, interviews of the employees are essential to the review process. If your facility possesses classified material, the review would take on a third dimension a concern with the physical security of the classified material. In all of these activities, you may wish to accompany the IS Rep personally or assign someone to accompany

him/her. While this is not required, it might serve as a training vehicle to you or your designee. It should be noted that the IS Rep may decide to conduct unaccompanied interviews. Certainly someone should be available to help in locating files and documents and to assist, should any problems arise.

RESULTS OF THE REVIEW

Upon completion of the review, the IS Rep will first brief you the FSO concerning the details of the review. Afterwards, a briefing is provided to senior management concerning the overall security posture of the company. The adequacy of security systems in place in your company will serve as the basis for the evaluation of the overall security posture. A rating of the security review will be assigned as follows:

Superior. A superior rating is the highest rating given to a contractor. A superior rating is given to contractors that have far exceeded the security requirements of the NISPOM when compared to other contractors of the same or similar size and complexity. This facility must have an outstanding security education program. Employee's must be fully aware of their individual security responsibilities, and demonstrate a cooperative sprit and awareness of security procedures. This rating also requires a sustained level of management support for the security program and the absence of any serious security issues.

Commendable: A commendable rating is given to contractors that have exceeded the basic security requirements of the NISPOM in one or more areas

of their security program, but do not meet the standards or level required to achieve a superior rating. Like the rating of superior, the contractor must have strong managerial support, minimal administrative findings, and the absence of any serious security issues.

Satisfactory: A satisfactory rating is the most common rating given to cleared contractors. A satisfactory rating indicates that a contractor's security program meets the basic requirements of the NISPOM. It indicates that there is minimal or no threat to the security of classified information at the cleared facility. This rating may be assigned even if there were administrative or isolated serious findings that require corrective actions.

Marginal: A marginal rating is given when serious findings are noted in one or more areas and these findings could lead to the loss or compromise of classified material if not corrected. The IS Rep will consider the size of the facility, extent of classified activity, and cause of the findings when giving a contractor a marginal rating. In addition, when a marginal rating is given, the IS Rep will normally schedule a compliance security review within 30 but no longer than 120 days.

Unsatisfactory: An Unsatisfactory rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer

preclude the disclosure of classified information to unauthorized persons.

The IS Rep will provide you a full explanation of the rationale for the assigned rating. The IS Rep will also advise you of any isolated individual failures or individual instances of non-compliance with a security requirement and will provide guidance to correct or resolve the issue. These types of issues will only be briefed to top management or included in the letter to top management if the individual or security system failure resulted in a compromise or suspected compromise or if a pattern has been identified which suggests the system is inadequate.

The IS Rep will almost certainly have found positive, even praiseworthy, facets of the security program, so this talk should provide an occasion for kudos as well. The FSO should feel free to make use of the IS Rep as a liaison between you and top management personnel. This will be an ideal time to raise important concerns/ issues about the security program that may have fallen on managers' deaf ears up to now. For instance, maybe the firm is winning more classified contracts than the FSO can properly monitor. The FSO may need an assistant to help with the workload. Tell the IS Rep. As an official representative of the U.S. Government, the IS Rep has considerable authority, and his/her voice added to yours on important issues may be just what's needed to convince management to take action.

EXIT BRIEFING

Once the IS Rep has briefed you, the FSO, the IS Rep will meet with senior management (assuming that you and senior management are not one and the same). During this exit briefing, the IS Rep will stress key issues regarding the facility's security program. The IS Rep will advise senior management of the overall security posture of the facility and explain the reason the rating was assigned. Remember, the IS Rep will only discuss instances of non-compliance with top management if a compromise or suspected compromise has occurred or the IS Rep has identified a pattern which suggests the system is inadequate. Even if there are no such problems, the exit briefing is still held to let management know what the overall security posture of the facility is and to brief them on any security topics of special interest, for example, an upcoming change to the NISPOM that affects your facility. And here again kudos from the IS Rep may be in order.

LETTER TO MANAGEMENT

Your facility's management will also be notified in writing of the results of the review. This letter will:

- Reiterate the security posture of the company.
- Highlight positive aspects.
- If appropriate, thank or commend members of the management or the security staff.
- Provide recommendations for security program improvements and stress areas of concern.

Again, this notification will only identify instances of non-compliance if a compromise or suspected

compromise has occurred or a pattern exists which suggests that the system is inadequate.

DSS FIELD OFFICE FOLLOW-UP

If the letter to management noted serious security problems, the DSS Field Office/IS Rep may conduct a special security review to determine that the problems have been corrected. Follow-up reviews are generally limited to determining and evaluating the correction of system failures.

UNSATISFACTORY RATING

The "worst-case" situation for the government security review is one where it is determined that the facility is unwilling or has consistently demonstrated an inadequacy to protect classified information. In this situation, the IS Rep may recommend to the DSS Field Office Chief revocation of the FCL Recommendation for revocation will be preceded by placing the facility in an *unsatisfactory* status and should be considered only when the contractor takes no effective action to improve their security posture. An unsatisfactory status indicates that the facility is no longer capable of protecting classified information and that revocation of the FCL is under consideration. An unsatisfactory rating is brought to the attention of the government customer(s). The Field Office may also advise these customers that the company should not be considered for any new classified work until conditions have improved. If management remains unwilling or unable to take effective corrective action, the facility's security clearance would be revoked. This is done only after a very careful review of the situation by highly-

placed, experienced NISP personnel. Fortunately, this is a very rare occurrence.

DORMANT FACILITIES

Finally, a review may reveal that a facility is dormant. A dormant facility is one that does not have active classified contracts, has not been afforded authorized access, and has no prospects for obtaining a classified contract. Unless something happens to end the facility's dormancy, DSS will administratively terminate the facility's clearance 24 months from the date of the facility's last access. The facility can be cleared "in an expeditious manner" if it again requires access.

FINAL SECURITY REVIEWS

A *final security review* is conducted when a possessing facility ends its involvement with the NISP. It may be that the contractor no longer wishes for whatever reason to perform on classified government contracts. It may be that a dormant facility's clearance is to be administratively terminated or that an unsatisfactory facility's clearance is to be revoked. Whatever the reason for conducting it, a final review is a formal review that includes other elements as well. These other elements terminate the cleared status of the facility. For example, the IS Rep will ensure that there is no classified information on site; that all cleared personnel have been (or will be) debriefed; that any outstanding classified visit authorizations have been cancelled, and that all security related files are in order. The IS Rep reviews with the FSO

which records must be maintained in the future and for how long.

SELF-INSPECTIONS

Self-inspections are conducted by you, the FSO. In the ongoing government-industry partnership, the day-to-day tasks of running a successful security program are carried out by the people at the industrial facility. While the DSS Field Office's review of the state of the company's security program is a useful evaluation tool, there is no way that the government, (IS Reps) can begin to carry out the role of overseer. The security program is ultimately the responsibility of the designated FSO. One of the best tools for monitoring and evaluating the program is the self-inspection.

FREQUENCY

You must review your security system on a continuing basis and conduct a formal self-inspection at intervals consistent with risk management principles. The word "intervals" gives you considerable latitude in deciding when to conduct a self-inspection. However, common sense should keep you from conducting it the day before or the day after a government review. It is recommended to conduct a self-inspection once a year or approximately six months following the DSS security review.

CONDUCTING A SELF-INSPECTION

You should model your self-inspection on the DSS review. The Defense Security Service Academy has prepared a guide to conducting self-

inspections for NISP contractors. *This guide, The Self Inspection Handbook for NISP Contractors* is available from your IS Rep. If your facility does not possess classified information, you will probably need to deal with only a few of its headings. The sections of the handbook on the following topics may apply to any cleared facility:

- Facility Clearance
- Access Authorizations
- Security Education
- Standard Practices Procedures
- Visit Control
- Foreign Ownership, Control, or Influence (FOCI)
- Consultants

The best way to use the *The Self Inspection Handbook for NISP Contractors* is to go down the list and ask yourself which questions apply to your facility, as well as the logical follow-ups to those questions. For example, if you're answering a question, which asks if a personnel clearance record is maintained, don't just locate the record. Read it carefully. Are there people listed who no longer require access? Does everyone listed still require access at the levels indicated?

Don't just go down the handbook's list at your desk if the question concerns the Security Agreement, locate the agreement. Like the IS Rep, you should do more than a mere paper check. It is the entire security system you are interested in, not just the related paperwork. Talk to the employees (you should be doing this on a regular basis, anyway). This needn't be a formal interrogation a friendly chat will suffice, if it gives you the information you're after.

ANALYZE AND CORRECT

When you've finished your self-inspection, what then? Obviously, you should correct any problems that surface. Don't just leave it at that. Take a good look at *what caused the problem*. Was it a single, isolated incident or was it a symptom of a flaw in the security program? If your analysis shows that your procedures are inadequate or ineffective, revise them. The whole idea of the self-inspection is to give you, the FSO, a chance to review your security program *in its entirety*. Your review should ensure that your facility's overall security posture is adequate and that you are ready for the next Government Security Review.

AN EXAMPLE OF A SELF-INSPECTION

On the following pages we have provided a sample self-inspection conducted a short time ago at EWS by Harriet Hornsby, FSO. This is hardly an all-inclusive inspection, but it may at least give you a taste of what's involved.

SELF-INSPECTION AT EWS



As she did every morning at about twenty minutes to eight, Harriet positioned her coffee and cherry pie on the corner of her desk and spread the A.M. edition of the *Wombat Heights World Herald* out before her as she glanced at her current daily planner.

Oh, heck. She thumbed through her last year's daily planner and confirmed it. It was exactly one hundred and eighty-four days ago that George

Porgee, IS Rep, had been here at EWS for the government inspection. She realized that when George came by for his next inspection in a year or so, he wouldn't be particularly concerned about the exact timing of the self-inspection.

Putting away the paper, she turned to her copy of *The Self-Inspection Handbook for NISP Contractors*.

A. Facility Clearance.

1. Are the DD Forms 441 and/or 441-1 and SF 328 properly executed and maintained in a current status?



This being a branch office, Harriet knew that EWS needed the 441-1 and a copy of the 441 for EWC. Now where did Mr. Wilbersnoot keep those things? Then Harriet remembered. They are filed with the other legal documents in his personal safe. The one for which only he and his secretary, Wanda Fishtank, had the combination.

Mr. Wilbersnoot was away for a week, which meant Wanda would have to open the safe. Harriet was a little leery of asking her. Wanda was very protective of EWS, and of Mr. Wilbersnoot in particular. And Harriet felt as though Wanda had never quite forgiven her for the two weeks when she had replaced Harriet as FSO. Wanda blamed her in some way for this, although it had been Mr. Wilbersnoot's idea.

Fifteen minutes later, Harriet peered into the small crack Wanda had opened in the safe. Balancing her coffee mug on the edge, she used both hands

to open the drawer further. It took her another five minutes to find the 441-1. She made a mental note to have a talk with Mr. Wilbersnoot about his filing system.

Harriet was so happy to have finally gotten her hands on the 441-1 that she forgot all about her mug on the edge of the safe. After she mopped off the 441-1, she realized, to her horror, that it was now a sort of Mississippi River brown. Was it still a legal document? She could make out the signatures and she supposed the color of the form didn't matter. But what would she tell Mr. Wilbersnoot? Putting the 441-1 back in the drawer, she saw the copy of EWC's 441. She went to the next question.

2. Have all changes affecting the condition of the FCL been reported to the DSS Field Office?

The only changed condition reports lately were those reporting changes in KMPs. She'd filed a report with the DSS Field Office when Wanda had replaced her as FSO. And then Wanda had filed a report when Harriet took the job back.

3. Does the home office have an FCL at the same or higher level than any cleared facility within the Multiple Facility Organization?

Harriet was well aware of EWC's TOP SECRET facility clearance, which was at a higher level than the SECRET FCLs of both EWS and Electric Widget Distributors, the other branch office in the MFO.



4. Are the senior management official, the FSO and other Key Management Personnel cleared as required in connection with the FCL?

No one other than the FSO (Harriet) and senior management official (Mr. Wilbersnoot) had been required to be cleared in connection with the FCL. There were no uncleared officials who required exclusion at EWS, so she skipped question 5 and went on to question 6. Since there were no representatives of foreign interests at EWS, Harriet skipped question 6 too.

B. Access Authorizations.

1. Is a current record maintained of all cleared employees at each facility?

All that stuff was kept in the filing cabinet in the office that the Sales and Services people shared. Opening the bottom drawer, Harriet pulled out the list of EWS's cleared employees. There were only seven, and the list was current. Harriet didn't stop with the list, though. She checked the contents of the personnel security files. These files, arranged alphabetically, were kept on all currently cleared personnel. In each file, Harriet kept the LOC and a copy of all paperwork sent to the government (DISCO) regarding the person's clearance. There had been no changes, aside from Wanda's new clearance, since Porgee's last review, and all the paperwork appeared to be in good order.



Roberta Baloon

2. Is the number of clearances held to a minimum consistent with contractual requirements?

Harriet considered. She and Mr. Wilbersnoot had to be cleared as KMPs. Wanda had been cleared for her short-lived career as an FSO. Harriet put Wanda's folder aside. She would have to get that clearance terminated. The other clearances were for the three service personnel who did work on classified projects and one for a salesman who took part in classified contract negotiations. She decided to have a talk with the four to see if they still needed their clearances. Jimbo Duggins was out today on a classified visit. Duncan Undersides was next on her list. He was down in Supplies, refilling his repair kit, so Harriet turned to Roberta Baloon, the third of the cleared service personnel. Roberta was just on her way out when Harriet caught her. "Have you been out on any classified visits lately, Bobbie?"

"Not for some months now."

"Will you be going out on any in the future?"

"Not that I know of, but you know I'm cleared in case Jimbo needs assistance on the Air Force contract."

Harriet recalled the justification for Bobbie's clearance. Sometimes it took more than one person to do a repair job. It was a valid reason.

"Where's Slick?" Harriet asked Roberta, referring to the salesman who was cleared to negotiate classified contracts.

"I don't know and I don't care," snapped Roberta, "I haven't seen that snake since last Thursday."





SLICK GIBSON

Thursday was the day of the Great Sales and Services War. Tension had been building between the two sides for a week. Sales claimed that Services had an excessive amount of floor space for a group of people who were away most of the day. Services countered that Sales tied up the telephones from morning 'til night. At first just words were exchanged. Then things really got serious. Someone made a paper airplane out of a memo and sailed it at the opposing camp. Soon memos and directives and order forms were flying in all directions. When the combatants ran out of supplies, they requisitioned any loose paper they could get their hands on. Before the day was out, the floor was littered with crumpled aircraft. And EWS's filing system was in shambles.

Each side blamed the other, which was, in short, why Roberta Baloon and Slick Gibson were not on speaking terms.

Slick was over by the water cooler.

"Hi there, beautiful! How's security biz?"

Harriet sometimes wished she and Gibson weren't on speaking terms either.

"Have you taken part in any classified negotiations lately, Slick?"

"No, but I've got a hot contract in the works with NASA. It'll be the biggest thing this little company has ever seen. And real TOP SECRET stuff."

Slick was always talking like this, so Harriet made a note to ask Mr. Wilbersnoot about this "hot

contract." In the meantime, she spotted Duncan coming out of Supplies.

"Do you do work at any classified sites, Dunc?"

"Not at the moment, but the Air Force job is due in any day and more manpower is going to be needed."

She would call her contact at the Air Force to confirm that.

As it stood now, she had one unnecessary clearance and two which were perhaps questionable. The fewer clearances she had to keep up with, the better. She read through the remaining questions about access authorizations.

3. Has a Letter of Consent (LOC) been issued for each personnel clearance (PCL)?

Yes. She had found all seven LOCs in her files check.

4. Are all pre-employment clearance applications based on a written offer and acceptance of employment?

Yes. No one was put in for a clearance before being hired "on paper" first.

5. Are all required forms and information regarding cleared personnel furnished to DISCO?

She had kept copies of all DISCO Forms 562 and other information transmitted to DISCO. There



hadn't been anything to transmit to DISCO since the last government review. If Wanda's clearance was going to be terminated, however, Harriet would have to transmit a DISCO Form 562.

6. Are employees in process for security clearances informed of their options regarding completion of the privacy portion of the SF 86 application form?

After Harriet and Wanda completed the SF 86 in EPSQ for the SECRET clearance. (Harriet downloaded the software from the DSS website, www.dss.mil). She had a little trouble at first, but after she called the Support Services Center at 1-888-347-5213, she had no problems). Harriet had validated the information before transmitting it. Except for modules 17-42. Harriet had informed Wanda of her right to privacy regarding the information she provided in those modules. Wanda had masked that information by invoking a second password. Harriet had made sure that the information in the other modules of the SF 86 in EPSQ agreed with the information on the fingerprint card she placed in the envelope to DSS. She had done a very thorough job of it, and DSS had not called requesting additional information.

7. Has the contractor elected to have PCLs issued to the home office facility (HOF) or has an alternative arrangement been approved by the DSS Field Office?

The DSS Field Office had approved EWC's request to allow PCLs to be issued to its two branch offices, so EWS kept the seven LOCs for its cleared employees. Question 8 was about the same as 5,

except that it seemed to include reports on KMPs that went to the DSS Field Office. There weren't any of them.

C. Security Education.

1. Does the contractor provide all cleared employees with security training and briefings commensurate with their involvement with classified information?

All of the cleared personnel at EWS had received a comprehensive initial security briefing, and Harriet always gave refresher briefings at least annually. She found the information posted on the DSS web site very helpful in keeping her briefings interesting. (Last year the employees complained that she said the same thing every time). She kept each year's notes on file along with the employee sign-up sheet she passed around. The cleared personnel at EWS did not need NATO, CNWDI, or other special briefings.

2. Are contractors who employ cleared persons at other locations ensuring the required security training?

The service personnel performing work at Gizmo received special briefings on site that specifically addressed the project they were working on.

3. Are SF 312s properly executed by cleared employees prior to accessing classified and forwarded to DISCO for retention?

After each initial security briefing, Harriet had required the cleared employee to sign an SF 312. As a precaution, she had made a copy of the

signed form before she sent the original to DISCO. (After receiving Industrial Security Letter 95L-1, Harriet made sure that all those SF 312s executed after July 31, 1995 were forwarded to DISCO for retention).

NOTE: NISPOM Paragraph 3-105 requires that an individual issued an initial personnel security clearance (PCL) execute an SF-312, Classified Information Nondisclosure Agreement prior to being granted access to classified information, and that the facility submit the original SF-312 to DISCO for retention. **Please note this requirement applies only to individuals granted an initial PCL.** PCL's resulting from conversions or reinstatements should not be forwarded to DISCO.

4. Are refusals to execute the SF 312 reported to DISCO?

No one at EWS had ever refused to sign the SF 312.

Question 5 asked whether initial security briefings covered everything they were required to cover, and question 6 asked whether refresher training was given. She had already answered these.

5. Are cleared employees debriefed at the time of a PCL's termination, suspension, revocation, or FCL termination?

Harriet remembered giving the termination debriefing to Willona Riggs, a former cleared employee. Thank goodness she had never had to give a debriefing under other circumstances!

Questions 8 and 9 asked about EWS's reporting awareness procedures and the reporting procedures themselves. The EWS system was simple but effective: Harriet told and reminded all cleared employees to report required information to her, and she in turn made the formal reports to the proper governmental authority. Question 10 was about DSS providing special briefings and debriefings; it did not apply to EWS. Harriet checked with the EWC personnel office to see if there were any garnishments of pay at EWS. There weren't. She had asked Mr. Wilbersnoot if he was aware of any adverse information on EWS employees. He wasn't.

6. Has the contractor established a graduated scale of administrative disciplinary action to be applied against employees who violate the Manual?

Harriet and Mr. Wilbersnoot had set up such a scale. It started with a "verbal admonishment" and ended with dismissal. Harriet was proud that, as yet anyway, no cleared employee at EWS had ever violated the Manual. She thought there were two reasons for the perfect record. First, her training and awareness activities showed the employees the right way to do things, and second, the employees wanted to do things right....widget repair or security.

7. Are employees aware of the Defense Hotline?

Harriet had posted the information on the wall in the employee lounge area:

**The Defense Hotline
The Pentagon
Washington, D.C. 20301-1900
(800) 424-9098
(703) 604-8569
hotline@dodig.osd.mil**

8. Does management support the industrial security program?

Well, Mr. Wilbersnoot had always let Harriet do as she wished on security matters. He certainly seemed to understand the importance of it all, even if he didn't care much for the time it occasionally took up. She did, however, chat regularly with him and the other cleared employees about security matters and often pointed out to him interesting cases she found in the newspaper and other security awareness publications that Mr. Porgee sent her from time to time. She was never entirely sure that he listened.

EWS had no formal written Standard Practice Procedures, so she skipped that section, and the next section, subcontracting, was of no concern to EWS. This section was directed at firms that subcontracted out.

Down to **F. Visit Control** then

Most of this section was aimed at those contractors who received visitors, not those who sent them out. Questions one through four seemed to be the only ones directed at EWS.

1. Can the contractor determine that all classified visits require access to or disclosure of classified information?

The classified visits made by EWS were usually service calls that entailed the service person having access to classified information in the form of classified equipment. Harriet returned to the file cabinet. She pulled out the middle drawer and thumbed through her copies of recent VALs. While there was no requirement to keep copies of VALs, she always did so. This allowed the visitor to be located quickly if the need arose. Where was the copy of Jimbo Duggins' current visit letter? Well, she'd look for it later. Now she wanted to finish up the rest of the self-inspection.

2. Does notification of classified visits allow sufficient lead-time for the receiver's timely approval?

Harriet always sent out the visit requests as soon as she was aware of the need for a classified visit. That usually gave Gizmo at least two weeks notice.

3. Do Visit Authorization Letters (VALs) include the required information, and are they updated to reflect changes in the status of that information?

EWS's visits were service visits. The service people did not go to GIZMO to receive classified information from someone at GIZMO during the visit. So Harriet's VALs had never included a person visited other than the GIZMO FSO, Wellington Minor. They checked in with him and he took the visitor to the equipment needing repair

or maintenance. George Porgee had said this procedure was OK. She had never needed to update VAL information.

4. Are long term Visit Authorization Letters (VALs) updated as required?

EWS had no long term VALs in effect, so this question did not apply. Looking at the question started Harriet thinking, though. Maybe it would save paperwork to set up a long term VAL with GIZMO. She would talk with Jimbo, Roberta, and Mr. Wilbersnoot to find out whether they thought it was a good idea.



G. Classification.

Since EWS didn't actually possess classified materials, their concern in this area was limited to the guidance provided by the Air Force in the DD Form 254. The current DD 254 on file was quite adequate to the needs of EWS.

H. Employee Identification.

EWS was such a small operation, everyone knew everyone else, that there was no need for a badging or I.D. Card System.

Harriet skipped **I. Foreign Ownership, Control, or Influence.** Headquarters was responsible for FOCI matters, including updating the Certificate Pertaining to Foreign Interests.

J. Public Release.

EWS received quite enough business without having to advertise. And any yearly reports that were published came out of headquarters in New York. Harriet quickly moved on.

Because EWS didn't have any classified holdings, the next seven sections could be skipped. That brought Harriet down to:

R. Classified Meetings.

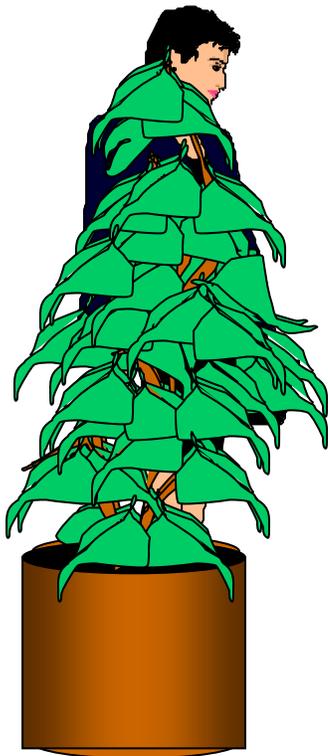
No problem, there hadn't been any.

She could pass over the sections on consultants, information systems for processing classified, and COMSEC/CRYPTO. EWS had none of that.

The next section of the handbook was **V. International Operations.** There had been talk of sending one of their service personnel to Canada to help out with a widget installation (not anything classified) but nothing had come of it. The last two sections of the handbook, OPSEC and special access programs, did not apply. Harriet was able to close her NISPOM with a smart snap, confident that she had completed a thorough self-inspection.

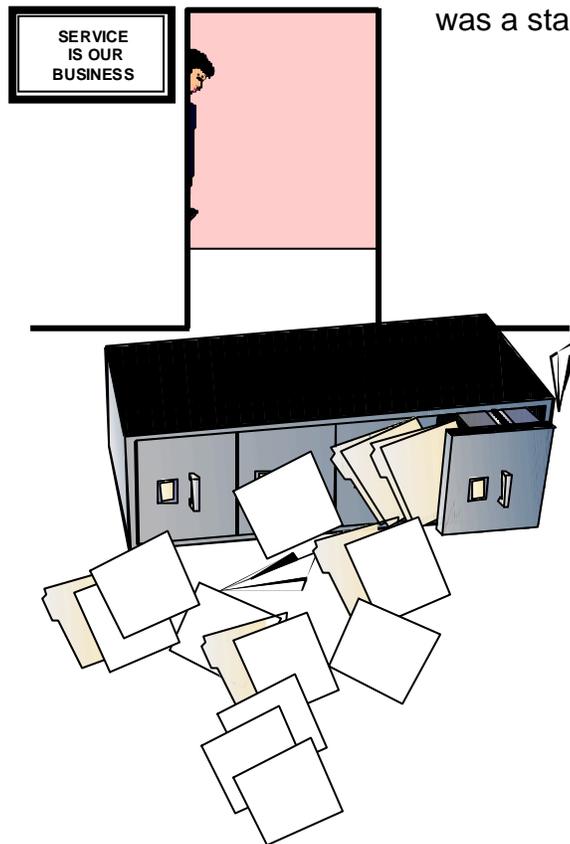
But where was that copy of the visit letter?

It had to be somewhere in the file cabinet. Harriet pulled out the top drawer. She leafed through the entire drawer of papers. No letter. Maybe it was in one of the large folders. She carried a folder back to her office. She had just reached her desk when a loud crack shattered the mid-morning silence. Suddenly she remembered why no one ever



opened all three drawers of the filing cabinet at the same time.

Wanda was looking at her accusingly when she came in to inspect the damage. The files had spilled out and slid across the linoleum all the way to the door, making a low-grade slope. The cabinet had crashed forward, closing all the drawers again. Only this time they opened to the bottom. Harriet noticed that a paper airplane had been trapped between the cabinet and the wall. A remnant, no doubt, of the Great Sales and Services War. She climbed across the files and picked it up. At least it was a start.



Two hours later, when everything had been refilled, Harriet remembered the paper airplane. Picking it up out of the trash can, she gave it a little celebratory flight. Before redepositing it in the trash, she unfolded it. It was the missing copy of Jimbo Duggins' visit letter. Harriet sat back in her

chair and reviewed the morning's events. On the whole, not bad, she thought. Maybe she should rearrange the security files so that everything was in one drawer. The only real finding was Wanda's unnecessary clearance, and she would take care of that right away. Nothing seemed basically wrong with the system itself.

Then Harriet looked up. Wanda was staring at her from behind a large philodendron. "Oh dear," Harriet wondered, "am I going to have to submit my very first adverse information report?" It really did seem as if Wanda was behaving more strangely than usual.

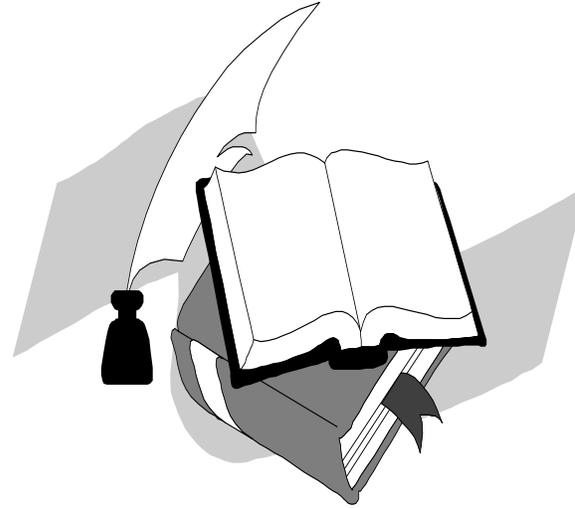
SUMMARY

Surveys and reviews play a vital role in ensuring that classified information is properly safeguarded within the NISP. The Initial Facility Clearance Survey is a means of gathering information regarding a firm's suitability for an FCL. A changed condition survey may be required when information reported in the course of the initial survey is no longer valid. Security reviews are normally conducted on an annual basis and are normally announced. The review of a non-possessing (access elsewhere) facility usually addresses at least the three basic areas: the status of the Facility Security Clearance; the status of the Personnel Security Clearances (access authorizations), and the level of security education and awareness. Other areas are reviewed as appropriate. Records may be reviewed and employees will likely be interviewed. During an exit briefing with the facility's management, the IS Rep discusses the overall security rating, any system failures, and any problems requiring their attention to resolve. A letter to management formally notifies the facility of the review results. The Field Office may follow up with a special review. In extreme situations, when a facility's management cannot or will not protect classified information, an unsatisfactory rating is assigned. If such a situation remains uncorrected,

the facility's security clearance is revoked. When a possessing facility terminates its participation in the NISP, a close-out review is usually conducted. The FSO reviews the security system at the facility from day to day and conducts a self-inspection of the system at intervals consistent with risk management principles.

9 – Review Exercises

Complete the following exercises for review and practice.



Multiple-choice questions may have one or more correct choices.

1. List two "changed conditions" that may require a changed condition survey.

a. _____.

b. _____.

2. List three events that may cause DSS to conduct a security inspection of a facility in less than the normal 12 month period.

a. _____.

b. _____.

c. _____.

3. The review of facilities that do not possess classified information will usually address, as a minimum, the following three basic areas:

a. _____.

b. _____.

c. _____.

4. Another area that is usually covered during an inspection of a non-possessing facility is v_____ c_____.

5. The FSO will always receive a letter of notification of an upcoming government review several days before the date of the inspection.

() True. () False.

6. As for any classified visit, your facility will receive a visit request for the IS Rep's review.

() True. () False.

7. The IS Rep's review will usually consist of what two types of activity?

a. _____.

b. _____.

8. For each of the following, enter the type of rating awarded when the conditions described are encountered during a review.
- a. Rating: _____. Security Program meets the basic requirements of the NISPOM. Minimal system failures that are recognized and corrected before compromise have occurred; generally good knowledge among cleared employees of security procedures.
 - b. Rating: _____. Serious findings are noted in one or more areas, which could lead to inadequate protection of classified material. Management demonstrates no support for security or takes action that hinder security
 - c. Rating: _____. Contractor has exceeded the Basic Security Requirements of the NISPOM in many areas of their program, but do not meet the standards of a superior rating. Model security education program, top management actively supports maintaining an excellent security posture.
 - d. Rating: _____. This rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer preclude the disclosure of classified information to unauthorized persons.
9. Following the review, the IS Rep will provide you with a full explanation of the rationale for the assigned rating. The IS Rep will also advise you of any isolated individual f_____ or individual instances of n_____ with a security requirement and will provide g_____ to correct or resolve the issue.
10. The types of issues noted in item 9 will only be briefed to top management or included in the letter to top management if the individual or security system failure resulted in a c_____ or s_____ c_____ or if a p_____ has been identified which suggests the system is inadequate.

11. Specifically, the letter to top management will

- a. Reiterate the s_____ p_____ of the company
- b. Highlight p_____ aspects
- c. If appropriate, t_____ or c_____ members of the management or the security staff
- d. Stress areas of c_____, if appropriate.

12. An unsatisfactory status is assigned when a facility is _____

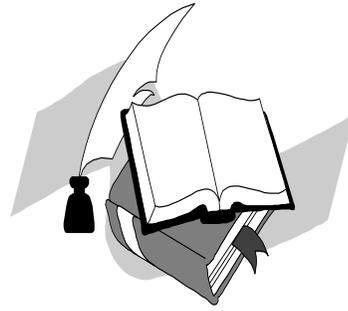
13. Your facility self-inspection must be conducted

- () a. immediately preceding government reviews.
- () b. once per month.
- () c. at intervals consistent with risk management principles.
- () d. every six months.

14. Desirable features of a facility self-inspection include:

- () a. locating and reviewing applicable documents, forms, correspondence and other paperwork.
- () b. talking to cleared personnel about any security problems you may have uncovered that relate to them and about any security difficulties they may be experiencing.
- () c. correcting any security problems you may have encountered.
- () d. analyzing the causes of the security problems that were identified and, where possible, eliminating the causes.

Solutions & References – 9



1. a. change in business structure/organization (e.g., change of name).
b. physical change (e.g., change of location).
(p. 9-3).
2. Any three of the events listed on p. 9-4 & 9-5. (p. 9-4 & 9-5).
3. a. The status of the Facility Security Clearance.
b. The status of the Personnel Security Clearances or access authorizations.
c. The level of security education and awareness.
(p. 9-6).
4. Visit control (outgoing classified visits). (p. 9-7 & 9-8).
5. False. (p. 9-5).
6. False. (p. 9-5).
7. a. Reviewing various records.
b. Interviewing personnel at your facility. (pp. 9-8 & 9-9).

- 8. a. Satisfactory
 - b. Marginal
 - c. Commendable
 - d. Unsatisfactory (p. 9-9, 9-10 & 9-11).

- 9. failure, non-compliance, guidance. (p. 9-11).

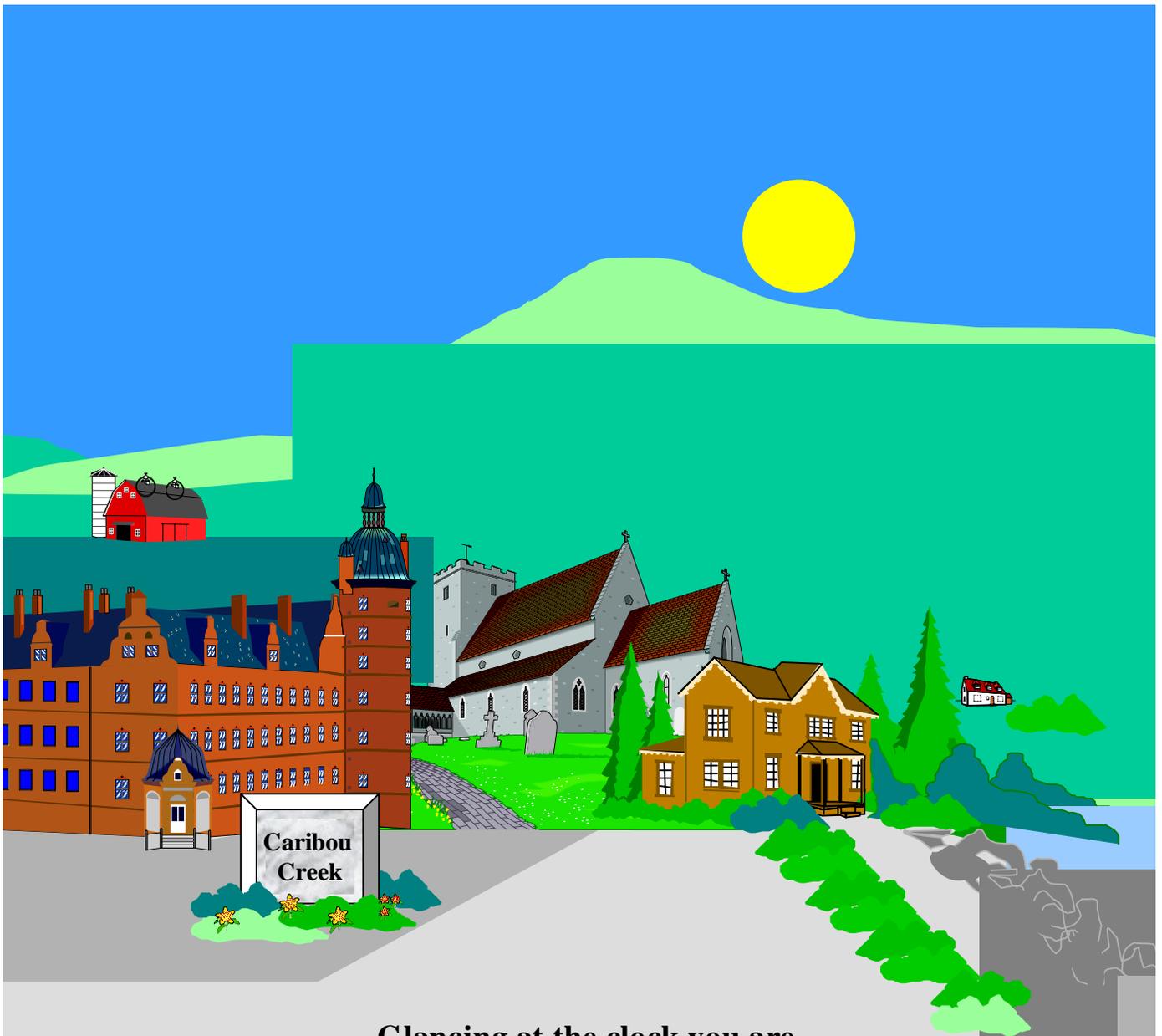
- 10. compromise, suspected compromise, pattern. (p. 9-11).

- 11. a. security posture.
 - b. positive.
 - c. thank, commend.
 - d. concern.
(p. 9-12).

- 12. cannot or will not adequately safeguard classified information. (p. 9-13).

- 13. c. (p. 9-15).

- 14. a, b, c, and d. (pp. 9-15 -17).



Glancing at the clock you are elated to discover it is time to go home! Fritz pokes his head in to tell you what a marvelous bit of work you have accomplished this first day on the job and to say that all the employees have been murmuring compliments about the new security officer. “I don’t know how you do it,” says Fritz, “but you’ve given us a morale boost for sure. We know we can count on you. See you tomorrow!! This job is going to be very rewarding, you feel, as you drive home. And the setting sun casts a warm glow over the little town of Caribou Creek.