

LESSON 6

Reports

For the National Industrial Security Program to work, there must be communication between government and industry. On the government's part, this communication takes the form of directives and guidance, as well as security reviews to see that the program is working on site. On the part of industry, this communication largely takes the form of reports to the government. These reports are simply your way of letting DSS know what's going on. In a cooperative venture like the NISP, it's necessary that all parties be informed.

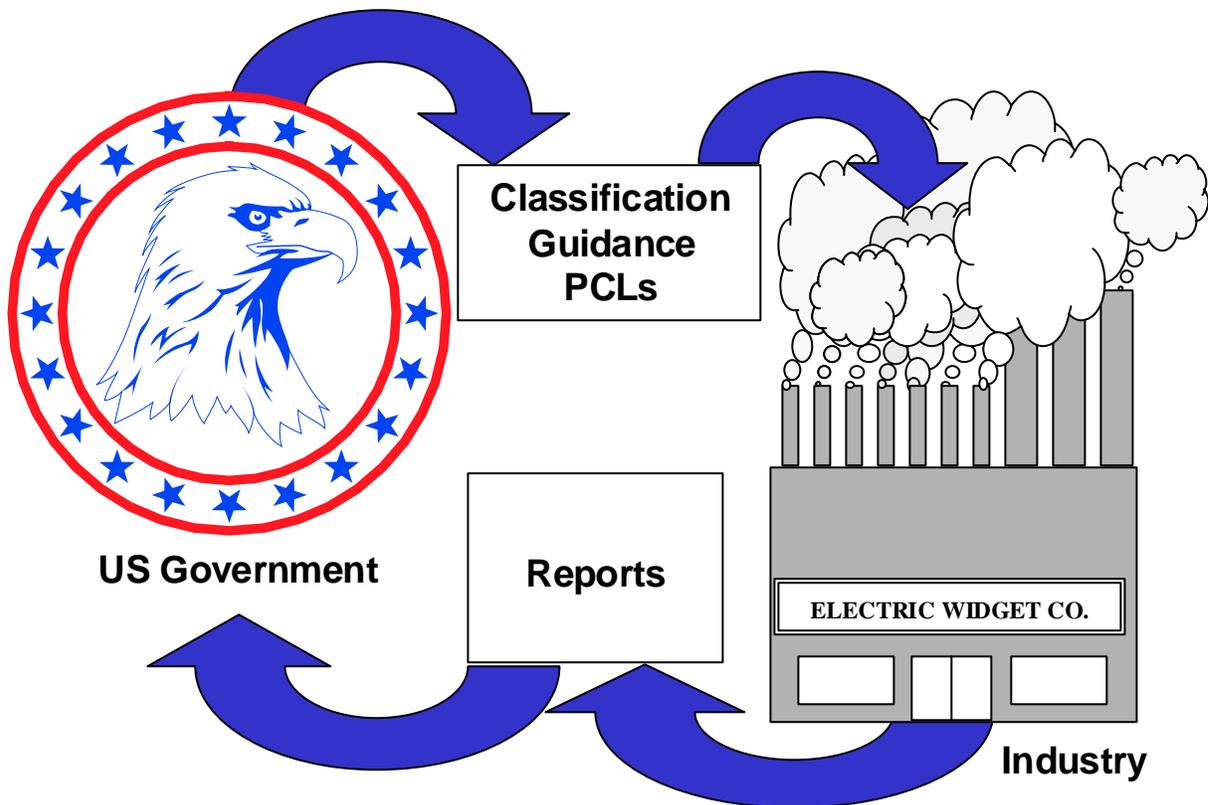
OBJECTIVES

At the end of this lesson you should be able to do the following:

- Describe the reporting requirements.
- Explain the definition of adverse information and where to send the report.
- Locate the proper reporting requirement, given a certain situation, and complete the appropriate reporting requirement.
- Differentiate between reports sent to the DSS Field Office or reports sent to DISCO.

REPORTING REQUIREMENTS UNDER THE NISP

One of your most important duties as an FSO is to make required reports to the government. These reports are a link in the government/industry relationship that we outlined in Lesson 1. While there are a number of specific reports required by the NISP, these reports generally fall into three categories. This should make it easier for you to determine when a report is warranted and to determine how to make that report.



The first category of reports concerns *changes*: **changes affecting cleared personnel** and **changes that affect the Facility Security Clearance**. If there is any change pertaining to your company's FCL or PCLs you should check paragraph 1-302 of the NISPOM to see if the changed condition requires that a report be sent. We will look at some examples of these reports and how to make them later in the lesson.

The second category is **adverse information** reporting. This report reflects a changed condition that affects an individual's personnel security clearance (PCL) which falls under the first category. We're treating adverse information reporting as a separate type of report because of its extreme importance to the National Industrial Security Program. This lesson provides a good opportunity to explain

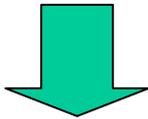
the philosophy of adverse information reporting, its purpose, and some of the legal implications of this report for industry.

The third reporting category concerns classified information directly. These are reports that are made when there is *loss, compromise, or suspected compromise* of classified information.

HOW THE NISPOM IS ARRANGED FOR REPORTING REQUIREMENTS



EMPLOYEES



FSO

DSS Field Office

DISCO

FBI

How reports get to the Government

Section 3 of the NISPOM divides the reports in terms of *where they are sent*. Reports regarding espionage, sabotage, or subversive activities are sent to the Federal Bureau of Investigation (FBI), as described in paragraph **1-301**. Reports sent to the Cognizant Security Agency (CSA) are listed in 1-302. Paragraphs 1-303 indicate reports sent to your DSS Representative. Paragraph 1-304 outlines reports that are sent to DISCO.

Much confusion stems from the use of the term "CSA" (a high-level term that refers to any one of the four major government players of the NISP). What the report writer needs to know are low-level terms that specify where to send the various reports. The high-level term is "CSA," which stands for "Cognizant Security Agency." The CSA is, the DOE, the NRC, the CIA, or the DoD, which ever is your CSA. DSS is a part of DoD.

Cognizant Security Office. The "CSA" also includes two elements of DSS: DISCO and your DSS Field Office. *You actually send the reports for the "CSA" to DISCO or your DSS Field Office.* Throughout this lesson, we'll point out which CSA reports go to which DSS element.

WHAT IS A REPORT?

A report may take a number of different forms. In some cases it is merely the act of notification, by letter or telephone, or e-mail that something has occurred. Other reports have more specific procedures such as use of a certain form or requirements for a detailed listing of information. Once you have determined what information needs to be reported, you can easily check the charts provided in this lesson for that reporting requirement and determine how it should be reported.

PEOPLE CHANGES AND FACILITY CHANGES

All 1-302 reports that reflect changes affecting *Personnel Security Clearances* are sent to DISCO. Most often you will use DISCO Form 562, (Personnel Security Clearance Change Notification), to make your reports to DISCO. DISCO Form 562 is the "CSA designated form" mentioned in 1-302c and 1-302e. It is used to report a name change, termination of employment, termination of clearance, etc. Otherwise, a letter report to DISCO is called for.

Example of a Changed Condition: Name change of a cleared employee.

BEFORE



Dr. Jekyll

AFTER



Mr. Hyde

NOTE: There could also be a potential adverse information report here.

All paragraph 1-302 reports that reflect changes regarding the *Facility Security Clearance* are sent, in writing, *to the DSS Field Office*. Most reports to the DSS Field Office will be made by letter. These are the 1-302h reports that we discussed in Lesson 3; those that advise the DSS Field Office of changed conditions that affect your FCL. You will recall that only one type of report to the DSS Field Office entails submitting a SF 328 report form: as discussed in paragraph 1-302h(5) of the NISPOM. This requirement to report any change in foreign ownership, control, or influence (FOCI) is met through the submission of a *revised SF 328*. SF 328 is the enigmatic "CSA designated form" mentioned in 1-302h (5). The form is all that's required; however, a cover letter explaining the reason for submission of any form is always helpful.

Reports to the CSA under 1-303 also go *to the DSS Field Office*. Paragraph 1-303 has two basic purposes: 1) To establish an "in-house" reporting system to ensure that the FSO is aware of any loss, compromise, or suspected compromise of classified information and 2) to outline the reporting requirements should such an event occur. There should, of course, be a system already in place to notify the FSO of any changes affecting the FCL, or any changes affecting PCLs (and LAAs), or any changes or conditions that appear likely to affect the facility's ability to safeguard classified information. As you might expect, though, reports of individual culpability (blame or guilt) for a security violation, described in 1-304, go *to DISCO!*

So there you have it. Reports on people go to DISCO; reports on the facility go to the DSS Field Office. The only snag is when the *person* is also identified with the *facility* as a Key Management Person (KMP). As we pointed out in Lesson 3, a KMP has a direct bearing on the Facility Security

Clearance. So reports about changes in the information previously submitted for your facility's KMPs are sent *to the DSS Field Office* under NISPOM, 1-302h(3). In all other respects, reporting on KMPs is the same as for any cleared employee. If any of the employee reporting situations occurs such as suspicious contact, death, termination of employment, becoming an RFI, etc. then you are to report the matter *to DISCO (with a courtesy copy to your DSS Field Office)*. It's still a very simple formula to remember:

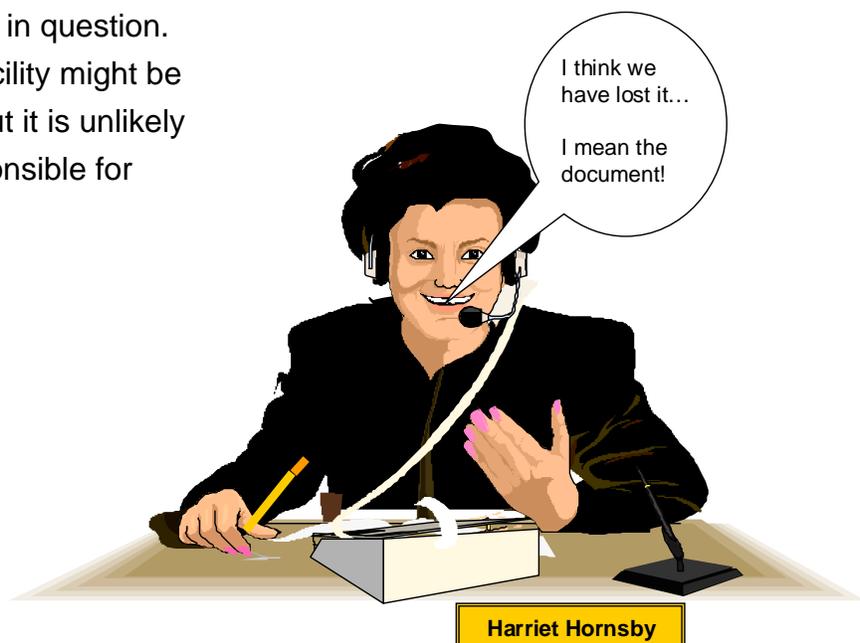
Reports on people, *including KMPs*, go to DISCO (copy to DSS Field Office).

Reports on the facility, *including KMPs*, go to the DSS Field Office.

REPORTS OF LOSS, COMPROMISE, OR SUSPECTED COMPROMISE

As this module is directed mainly at the non-possessing facility, we will not dwell in any great detail on reports of loss, compromise, or suspected compromise. Such reports would most commonly be generated by the facility possessing the classified information in question.

A non-possessing facility might be involved indirectly, but it is unlikely that it would be responsible for this report.



The basis for a report of loss, compromise, or suspected compromise (NISPOM, 1-303) is essentially the journalist's "big six; "**Who, What, When, Where, Why, and How.** Upon initial discovery that some piece of classified information or material has been lost, compromised, or suspected to have been compromised, the FSO must initiate a **preliminary inquiry** to ascertain all of the circumstances surrounding the reported loss, compromise, or suspected compromise and notify the DSS Field Office immediately. This notification may be accomplished by a telephone call or email to the Industrial Security Representative (ISR). The **initial report** to the DSS Field Office should give the facts as they are then known. The **final report** will be submitted upon completion of the *contractor's* inquiry—normally within 15 days after submission of the **initial report**. The DSS ISR will provide a suspense date to the FSO for submission of the **final report**. The required contents of the final report are shown in the chart on the next page.

If your DSS Field Office determines that more information is necessary to fully describe the situation, an IS Rep may be sent to the facility to conduct an Administrative Inquiry. If the completed report indicates loss, compromise, or suspected compromise of classified information, the User Agency (Government Contracting Agency) will be notified and asked to evaluate the classified information and to assess the damage done.

CONTENTS OF FINAL REPORT

Required Contents of Final Report to the CSA (DSS Field Office) for Incidents of Loss, Compromise, or Suspected Compromise:

Reference the initial report.

Describe material involved to include originating activity or contractor (name and address), date of origin, document title, number of pages, description of contents, contract or program under which material was received or produced and classification level of the information.

Give the essential facts of the incident: Where, when and how it occurred and any contributing factors.

Give the name, position, social security number, date and place of birth and date of PCL or LAA of individual(s) primarily responsible for the incident, along with a listing of any previous such incidents or any previous failure to comply with the NISPOM for which the individual was responsible.

Identify the person who first reported the incident and state when and to whom it was first reported.

State what action was taken to secure the material and to limit any damage after the violation was discovered. Include names and dates.

Describe when, for how long and under what circumstances classified information was vulnerable to unauthorized disclosure. List any unauthorized persons who may have had access to the information at that time.

Identify any classified documents or materials which are lost or unaccounted for.

Give specific reasons concluding that:

- 1) Loss or compromise occurred *or*
- 2) Compromise is suspected *or*
- 3) The probability of compromise is considered remote *or*
- 4) Compromise did not occur.

State what actions have been taken to prevent any recurrence of similar incidents.

State what disciplinary action, if any, was taken against the individual(s) responsible.

State whether or not the SPP (if applicable) was followed. Was the SPP adequate? If not, how was it inadequate and who was responsible for the inadequacy?

ADVERSE INFORMATION REPORTING

Of all the reports you, as FSO, are responsible for, the report of adverse information (NISPOM, 1-302a) may well be the most important.

WHAT IS AN ADVERSE INFORMATION REPORT?

Essentially, it is a report concerning a cleared person, reflecting upon that person's ability to safeguard classified information. Many aspects of an individual's character are considered before he or she is granted a clearance for access to classified information. Considerations include:

- the cleared employee's financial situation,
- reliability as evidenced on the job,
- reliance on drugs or alcohol,
- criminal convictions,
- indeed, *any* factor affecting a person's judgment, suitability, or reliability.

You will note that the examples given here are the same as those given in Lesson 4. This is because the PCL process, as we explained in that lesson, is an ongoing process not a final determination. The adverse information report is simply another way of ensuring that a cleared person may continue to be trusted with classified information.

WHO MAKES THE REPORT AND HOW IS IT MADE?

Ultimately, the FSO makes the report. But first, the information has to get to the FSO. A system must be put in place to forward information to the FSO. The basis of this system is the education of the employees. An employee who does not understand the nature or purpose of the report, who does not comprehend its importance to the national security, who fears exposure or reprisal for making the report and therefore fails to report, will jeopardize the effectiveness of adverse information reporting as a tool in protecting the national defense.

It is necessary, therefore, to reassure employees that an adverse information report will be treated as a confidential report, if so requested under the Privacy Act. The subject of the report need never know who the originator was.

Employees aware of adverse information often fear that their report will result in the firing of the subject, who may well be a friend as well as a co-worker. This almost never happens. An adverse information report is looked at as only a part of the overall picture. If the disclosed information warrants it, a report may generate the reinvestigation of a person's background, not unlike the periodic reinvestigations which are already part of many clearances. If the investigation turns up evidence of untrustworthiness, the PCL may be terminated. Whether this action has any bearing on that person's continued employment at the facility is a matter for that company's management to determine.

To re-emphasize: *A single adverse information report is unlikely to result in the revocation of a PCL or the subsequent loss of a person's job.* As for educating employees to the importance of adverse information reporting to the maintenance of security, this is part of your most important job, the education and training of the people in your company. If they understand the importance of maintaining national security, if they understand how they fit into the larger scheme of things, if they understand specifically how they, in the course of their duties, protect and safeguard classified information, then they can understand and respect the need for adverse information reporting and they will make those reports called for by paragraph 1-302a of the NISPOM.

In addition to education of employees, there are other methods to ensure adverse information is reported to the FSO. Many of these systems require absolutely no judgment calls on the part of any individual. For example, garnishment of wages, a situation generally known by the Personnel Officer, should be made the subject of an automatic report to the FSO. The same would apply to any knowledge of a criminal conviction. Other situations are trickier. Voluntary enrollment in an alcohol rehabilitation program is not cause for the generation of an automatic adverse information report. However, failing to maintain sobriety on the job, whether or not the individual is enrolled in a rehabilitation program, is.

DO ADVERSE INFORMATION REPORTS REALLY DO ANY GOOD?

Unquestionably, they do. They act as a barometer to help identify individuals whose continued access to classified information requires reassessment. Frequently adverse information reports *do* result in reinvestigations, and in some cases clearances *are* terminated.

CAN ADVERSE INFORMATION REPORTS PREVENT SPIES?

Going back to examples of espionage that we know have occurred in the past, we can see clear instances of where adverse information reporting *might* have prevented or decreased the resultant damage.

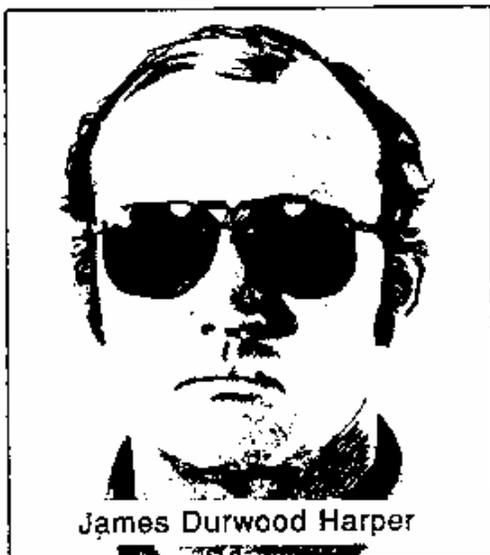
Take the case of William Holden Bell. It was known to at least a few of his fellow workers that he had financial difficulties (which suddenly disappeared) and that he was associating with a Polish national. Both were circumstances that could have been reported. Bell's case points out an important aspect of adverse information reports concerning finances: It isn't only the conspicuous display of newly acquired wealth, which is revealing. The sudden and unexplained removal of large debts and financial obligations also says a great deal about a

person's financial situation. Had either Mr. Bell's finances or his association with Marion Zacharski, (a polish national) been reported, a reinvestigation of Mr. Bell would almost certainly have ensued. It is impossible to state that the reinvestigation would have uncovered the espionage, but surely, at the very least, just knowing that he was being investigated would have dampened Mr. Bell's enthusiasm for spying.



William Holden Bell

An even more blatant example of a situation where adverse information reporting should have occurred was provided by Ruby Louise Schuler. She was the wife of James Durwood Harper. While he was the "mastermind" and handled all the James Bondian matters, *she* was the one with access to classified information. Mr. Harper did not have a Personnel Security Clearance or the means to directly access any of this nation's classified information. But through his wife, who held a clearance with a defense contractor, he was able to get his hands on 200 pounds of classified documents. It was his wife, Ruby, who should have been the subject of an adverse information report. As it happens, she wasn't, in spite of the fact that her alcoholism was well known to her co-workers. She was seen during the day drinking from a miniature bottle of vodka which she kept in her purse. An adverse information report filed on Ruby's alcohol problem could have led to the revocation of her clearance long before she met and married Harper. If nothing else, it would have put her on notice that her behavior and conduct were being observed, which would in turn have made Harper more cautious. And such concern might have helped Ruby. She died of cirrhosis of the liver.



James Durwood Harper



Ruby Louise Schuler

CHART OF REPORTS

On the following pages you will find a chart of the reports required by the NISPOM. The chart tells you the NISPOM reference, the title of the report, the circumstances under which it is sent, the format of the report, and where to send it.

BASELINE REPORTS



NISPOM	Report Title	When to Send	Form of Report	To
1-301	"Espionage," "Sabotage" or "Subversive Activity"	Upon learning of existing or threatened espionage, sabotage, or subversive activities at any of the contractor's sites	Letter. If the matter is urgent, make an initial report by phone. Follow up with written report. Send a copy to the DSS Field Office	FBI or DSS Field Office
1-302a	"Adverse Information"	<p>Upon learning information that adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may not be in the interest of national security, such as</p> <ul style="list-style-type: none"> • Criminal activities • Treatment for mental or emotional disorders • Excessive use of intoxicants • Use of illegal, controlled substances, such as marijuana, heroin, cocaine, and hashish • Excessive indebtedness or recurring financial difficulties <p><i>Reports based on rumor or innuendo should not be made.</i></p>	<p>Letter, on company letterhead or with company's names and address, addressed to DISCO, ATTN: Chief Special Programs Branch, to include:</p> <ul style="list-style-type: none"> • Date of submission • Subject's last name, first name and middle name • Social security number • Date and place of birth • Clearance level and date of clearance • Home address • Facility code where the clearance is held • Reporting facility's code • Subject's physical worksite • Employment status (if terminated, add termination date) • Adverse information being reported (If garnishment, please list date of garnishment, court, amount and complainant, or attach a copy of the garnishment order) • Name and telephone of the person to contact for further information • Signature, typed name and title of the person submitting the report. 	<p>D</p> <p>I</p> <p>S</p> <p>C</p>
1-302b	"Suspicious Contacts"	<p>When any individual, regardless of nationality, tries to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.</p> <p>_____ or _____</p> <p>When there is contact by a cleared employee with known or suspected intelligence officers from any country.</p> <p>_____ or _____</p> <p>When there is any contact which suggests the employee may be a target of an attempted exploitation by the intelligence officers of another country.</p>	Letter. If the matter is urgent, make an initial report by phone. Follow up with written report.	<p>O</p>



BASELINE REPORTS 3

NISPOM	Report Title	When to Send	Form of Report	To
1-302h	"Changed Condition Affecting the Facility Security Clearance"	1) Change of ownership 2) Change of name or address 3) Change to information previously submitted for KMPs 4) Termination of business 5) Change in FOCI: <ul style="list-style-type: none"> - Anticipated change - Actual change 	Letter Letter Letter to include: <ul style="list-style-type: none"> • Names of KMPs being replaced (if any) • New KMPs date and place of birth, social security number and citizenship • Whether new KMPs have been excluded from access, or temporarily excluded pending granting of their PCLs Letter. Letter. Letter. Include copy of Schedule 13 D if received. Revised SF328	D S S F I E L D O F F I C E
1-302m	"Employee Information in Compromise Case"	Upon written request of DSS Field Office	Letter. Contents determined by DSS Field Office	
1-303	"Loss," "Compromise," or "Suspected Compromise"	Upon loss, compromise, or suspected compromise of classified information	See discussion and report contents, pp.6-6-7.	
1-304	"Individual Culpability Report"	When individual responsibility for a security violation can be determined and one or more of the following factors are evident: <ul style="list-style-type: none"> • Deliberate disregard of security requirements • Gross negligence in the handling of classified material • A pattern of negligence or carelessness 	Letter that includes a statement of the administrative actions against the employee.	D I S C O

EXAMPLES OF VARIOUS TYPES OF REPORTS



To close, we're going to look at some examples of conditions and circumstances that require reports of one sort or another. It's up to our friend Harriet (the FSO) to decide if a report is, in fact, needed and how that report should be made.

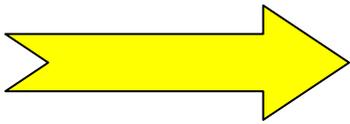
1) **Jimbo Duggins**, a widget repairman cleared SECRET, has been having financial troubles. As a result, his wages have been garnished. Harriet is aware of this because Wanda Fishtank, who handles personnel matters, has been instructed to keep Harriet apprised of problems of this sort.

JIMBO DUGGINS

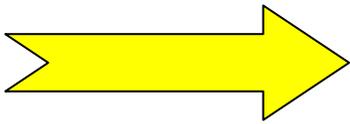
- 2) **Electric Widget Services** will be moving in four months from Wombat Heights to Drawstring Hollow. Harriet just received the mimeographed memo that was sent out to all employees. She's very busy right now and wonders if she can put matters off a bit.
- 3) **Roberta Baloon** has a CONFIDENTIAL clearance and has just had her name legally changed to Bobbie Baloon.



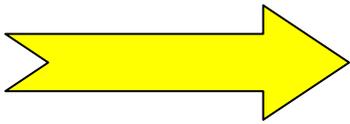
ROBERTA BALOON



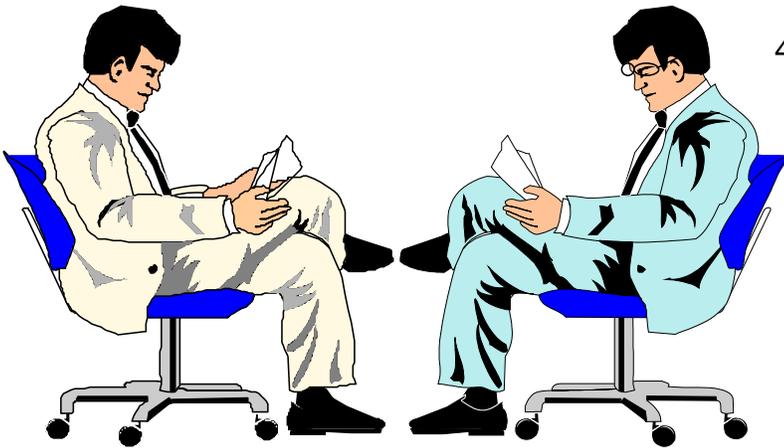
Harriet should file an adverse information report with DISCO, providing all of the information required by **1-302a** and paying particular care to see that the required details concerning the garnishment are all included. **(1-302a, NISPOM)**



She should let the DSS Field Office know right away, by letter, before it slips her mind. The records will be amended at the DSS Field Office to reflect the forthcoming change of address. An IS Rep will conduct a new survey/review when EWS moves in. **(1-302h(2), NISPOM)**



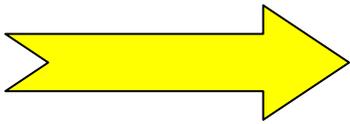
A simple DISCO Form 562 noting Roberta's name change will suffice. This should be transmitted to DISCO using EPSQ. **(1-302c, NISPOM)**



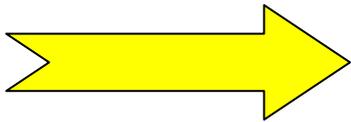
4) **Walter Wilbersnoot**, Harriet's boss, tells her that his twin brother **Waldo**, the world traveler, has started an oriental rug business in Bucharest, Romania. Waldo has asked Walter to represent the firm in marketing the products it is planning to export to the United States.

5) After thirty years with the company, **Willona Riggs** is retiring. She has held a **CONFIDENTIAL** clearance for three years.

6) **The Electric Widget Company** is considering distribution of some of their unclassified widgets to Eastern European countries. Does Harriet have to concern herself in this matter?



Since Mr. Wilbersnoot is cleared (at the SECRET level), Harriet needs to submit a 1-302d report, Representative of a Foreign Interest, to DISCO. The report should describe the nature and extent of his activities on behalf of his brother's foreign firm. (1-302d, NISPOM)



Harriet must debrief Willona (3-108, NISPOM). Then Harriet needs to complete a DISCO Form 562 (Termination of employment) and transmit it to DSS using EPSQ. (1-302c, NISPOM)



No. EWS is a branch office of the Electric Widget Company. The report, in the form of an advisory letter to the DSS Field Office, will be submitted by Harold Huxtable, EWC's FSO. (1-302h(5), NISPOM) Matters will be handled by the DSS Field Office in Harold's region. If the distribution plan goes through, then Harry would submit a new SF 328 to the DSS Field Office. Should the change in FOCI be enough to adversely affect the control of EWC (an unlikely event in this case), the DSS Field Office would work with EWC to attempt to negate the FOCI, if at all possible. (2-305, NISPOM)

7) Mr. Wilbersnoot thinks Harriet is overworked. Being FSO is only one of her many jobs. He tells her that he's appointing Wanda in her place.





Harriet needs to report a change in KMPs to her DSS Field Office. Since EWS is a branch office, the only personnel considered KMPs are the branch manager and the FSO. As Wanda is going to be the Facility Security Officer, she should be included in the report. (Wanda held the post for two weeks, until she realized just how much work was involved in being an FSO. She subsequently resigned. Harriet is once again the FSO.) (1-302h(3), NISPOM)



SUMMARY

The FSO informs appropriate government elements (the FBI, the DSS Field Office, DISCO) of significant events and circumstances at the facility by submitting various reports and documents. There are three basic categories of reports; 1) those concerning changes that affect the FCL or PCLs; 2) those conveying adverse information; and 3) those reporting the loss, compromise, or suspected compromise of classified information. As a general rule, reports on people, including KMPs, go to DISCO, while reports on the facility, including any change to the information previously submitted for KMPs, go to the DSS Field Office. The most common reports to DISCO are made on DISCO Form 562, while most reports to the DSS Field Office are made by letter. Adverse information reports provide an important means of identifying individuals whose continued access to classified information may require reassessment.

6 – Review Exercises

Complete the following exercises for review and practice.

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



1. The three basic categories of reports are 1) those concerning c_____ that affect cleared personnel or the facility security clearance, 2) those concerning a_____ i_____; and 3) those concerning l_____, c_____, or s_____ c_____ of classified information.
2. Adverse information reports are important to the NISP because they
 - () a. are the sole basis authorized for revoking the PCL of a cleared person.
 - () b. enable cleared facilities to identify and discharge unproductive employees.
 - () c. permit the NISP to compel the subject of the report to undertake counseling, rehabilitation or other measures to correct the subject's difficulties.
 - () d. help identify individuals whose continued access to classified information requires reassessment.
3. Reports on people, including KMPs, go to DISCO, while reports on the facility, including KMPs, go to the DSS Field Office.
 - () True.
 - () False.

For the following questions, refer to the charts on pages 6-13, 14, and 15.

4. Ozbak Pleebo, an immigrant alien with a CONFIDENTIAL LAA, is anxiously waiting to become a US citizen. When this happens, who must be notified? _____
By what means? _____

5. Tragedy struck the annual Digital Widgets-Gizmo Corp. softball game. While rounding third, old Mr. Appleby, the Treasurer at Digital, dropped dead. "It's how he would have wanted to go," said Mrs. Appleby. What sort of report(s) must be made and where should the report(s) be sent?

6. Mr. Wilbersnoot told Harriet, our FSO, that he was off to a meeting of the Association of Widget Engineers (AWE). The topic this year is "A Fuller Life Through Widgets." The meeting will be in Melbourne, Florida. Only members of the Association will be in attendance and all Association members are American citizens. Does Harriet have anything to report?

7. Hank Windles, an engineer holding a SECRET clearance at Digital Widgets, was found face down on his desk. At first, his fellow workers attributed this to boredom. Then they saw the bottle of peach brandy. This was not the first time that Hank had been discovered in this condition at work. In fact, these incidents were becoming quite frequent. What actions should be taken?

8. George Porgee, IS Rep, drove out to Widget Wiring Supplies in Wahoo, Wyoming for that facility's government review. He turned his car into the lot and saw, to his dismay, absolutely nothing! Widget Wiring had moved the month before. What should the company have done before the time of the move?

9. "It was right here a minute ago!" wailed Leonard. But no one could find the classified widget. Who must be notified of the loss?

10. Mild-mannered Miss Violetta Lambkins had worked as a cleared secretary at Gizmo for 35 years. It was therefore quite upsetting when Mr. Henway walked in on Violetta as she was taking photographs of a classified document with a tiny camera. Who should be told of this shocking incident?

11. When Harriet answered the telephone at three o'clock in the morning, she was surprised to hear Mr. Wilbersnoot on the other end. He sounded awfully shaken. He and some of his fellow AWE members had chartered a plane down in Florida to do a little post-conference sight-seeing. And one of the group, after too many margaritas, had hijacked the craft to Cuba. Luckily, they were all quickly returned to the US. Not, however, before the Cubans questioned Mr. Wilbersnoot rather thoroughly about his line of work. What does Harriet do now?

6 - Solutions & References



1. changes, adverse information, loss, compromise, suspected compromise.
(pp. 6-2,)
2. d. (p. 6-9,10)
3. True. (p. 6-5)

The NISPOM references given below are on pp. 6-14,15,16.

4. DISCO. DISCO Form 562. (1-302e, NISPOM)
5. A DISCO Form 562 (death of employee) should be sent to DISCO (1-302c, NISPOM)
6. No.
7. The employees should notify the FSO and the FSO, in turn, should send an adverse information report to DISCO. (1-302a, NISPOM)
8. A changed condition report (change of operating address) should have been sent to the DSS Field Office. (1-302h(2), NISPOM)
9. The FSO, who should then notify the DSS Field Office. Immediately. (1-303, NISPOM)
10. The FBI should be notified immediately, by telephone and followed up in writing with a copy to the DSS Field Office, (1-301, NISPOM).
11. She should send a report of the matter to DISCO. (1-302b, NISPOM)