Initial Security Briefing

NISPOM Briefing Requirements

The NISPOM requires that contractors provide cleared employees with an initial security briefing prior to their being permitted access to classified information. Employees are also required to complete the Classified Information Nondisclosure Agreement Standard Form 312 (SF 312) before they may gain access to classified information.

NISPOM (3-106) lists various subject areas to be covered in the initial briefing, but these should be considered a minimum requirement. The initial security briefing has five parts:

1. A threat awareness briefing

2. A defensive security briefing

3. An overview of the security classification system

4. Employee reporting obligations and requirements

5. Security procedures and duties applicable to the employee's job.

Briefing Topics

The briefing objectives provided in the NISPOM are necessarily general and most security professionals have found that these objectives can be adequately addressed by discussing a number of topic areas that relate directly to the employee's work experience. The following pages discuss most of what needs to be addressed in an initial security briefing. However, since many contractors have unique requirements, it is not possible to provide information for every topic area that may need to be covered. Large facilities with diverse contract requirements may find some pertinent areas are not covered, while small companies with limited classified contracts will find that many areas have limited relevance to their requirements.

Depending on the facility and its classified contracts and the audience for whom the initial security briefing is intended, security professionals may need to deal with a given topic either at length or in a more cursory manner. For example, topics such as working papers or destruction of classified information may be covered very briefly, if at all, if your audience is clerical. Many facilities will find that the level of detail provided for most topics in this section is more than adequate for the initial briefing. To further determine the level of detail required for a topic, security professionals may need to consult their contractual or program documentation such as Standard Practice Procedures (SPP). Your CSO will also be able to provide guidance.

The Non-Disclosure Agreement

The NISPOM (3-105) states that before an individual is given access to classified information, he or she must sign a nondisclosure agreement (SF 312). In addition to asking that the employee read and sign the SF 312, the security professional should verbally communicate to the employee what the agreement represents. SF 312 is essentially a lifetime contract between the employee and the U.S. Government, in which the employee agrees to protect U.S. classified information from unauthorized disclosure.

The agreement may affect the employee in a number of ways. It may require that the employee seek review and approval of any research material prior to its being presented verbally or in written format. It may limit the employee's ability to freely discuss his or her work with colleagues, relatives, and others. Violation of the agreement can result in a wide array of legal actions against the employee, ranging from civil suits to a succession of more severe penalties. The Information Security Oversight Office (ISOO) has produced an excellent briefing booklet and video describing the background and purpose of the SF 312. These are referenced in the Resource Providers folder under the heading Information Security.

The significance of the agreement between the individual and the government will be reinforced if portions of the espionage and conspiracy laws and applicable federal criminal statutes are read by, or read to, the employee. Briefly summarize and explain exactly what these laws and statutes mean.

These laws are provided in the ISOO SF 312 briefing book and can be reproduced and provided to newly indoctrinated personnel for their review. Penalties for breaking the nondisclosure contract may include loss of clearance, fines, and criminal prosecution under several statutes. The government may also bring a civil suit against the employee and seize all fees, royalties, remunerations, book and movies rights, etc., generated by the disclosure.

Threat Awareness and Defensive Security

The Foreign Intelligence Threat

The gathering of information by intelligence agents, especially in wartime, is an age-old strategy for gaining superiority over enemies. Intelligence officers, those individuals working for government intelligence services, are trained to serve their country by gathering information. Spies, on the other hand, betray their country by espionage. Preventing this kind of betrayal is the ultimate goal of the entire U.S. personnel security system.

While espionage has existed since countries began to battle, it was the events of the last few generations--the era of the Cold War--that concern us. During that period we had only one monolithic enemy, the Soviet Union. Our knowledge of Soviet Cold War espionage began with the defection of Igor Sergeievitch Gouzenko, a cipher clerk in the Soviet Embassy in Ottawa. In September 1945, he defected to Canada with documents that eventually led to the arrest of Klaus

Fuchs and, from there, to the apprehension of the Rosenbergs and their accomplices. A series of arrests and trials in the early 1950s helped set the climate for an anti-Communist campaign to root out all Communist sympathizers in government and nongovernment areas alike. Since then, motivations for espionage have changed dramatically. Ideology was supplanted by financial greed and by such other motives as disgruntlement, revenge, wanting to please others, wanting to spy simply for the thrill, or a combination of all these things.

Nobody knows exactly how many spy incidents have occurred since World War II because so many have been kept secret or have never even been prosecuted. But from research done at the Defense Personnel Security Research Center (PERSEREC) we know that at least 130 cases have been documented in the open literature. This classical form of espionage--the passing of classified information--still continues although since the end of the Cold War the recipients have changed. In a recent informal PERSEREC study of espionage cases since 1991 (found in open sources) six cases were "old" Cold War cases where the Soviet Union or Russia was the recipient, but the remaining nine involved spies who worked for a variety of countries, some of which were U.S. allies.

The New Threat

Classical espionage cases still occur, but now we are seeing a bourgeoning of a different kind of spying, an espionage based not just on the theft of classified information, but on theft of high-technology information, classified or not. This economic espionage is not a new phenomenon. It is just that in recent years its frequency has increased greatly. Estimates of current yearly U.S. loss of proprietary business information now range between $20 billion and $100 billion. This loss, and the loss of other technological information is especially detrimental to our economic vitality and may, by extension, have deleterious effects on U.S. security interests, since economic and national security are so closely linked in our highly competitive new world.

By now everyone understands that the end of the Cold War brought massive changes in the global economic structure. An intensified struggle for international economic power has taken the place of military superiority. Currently a host of foreign governments and individuals--present adversaries, former foes and traditional friends--are expending considerable resources in attempting to acquire our technological know-how through economic espionage. Economic espionage is the acquisition by foreign governments or corporations of U.S. high-technology information in order to enhance their countries' economic competitiveness. (Please note that this discussion is limited to espionage conducted by foreign governments against the U.S. Government or U.S. companies, defense-related or otherwise. We are not discussing intercorporate or industrial espionage within the U.S.--American companies spying against each other--although sometimes the methods used are similar.)

The FBI believes that nearly 100 countries are now running economic espionage operations against the U.S. Targets are shifting away from the classified military information sought in the old Cold War days toward basic research and development processes. But they also include the technology and trade secrets of U.S. high-tech companies--everything from cost analyses, marketing plans, contract bids and proprietary software to the high-tech data itself. Any

information or process--whether classified, unclassified or proprietary--that leads to cutting-edge technology is plainly in demand. Some products are bought (or stolen) in this country and then physically smuggled abroad. Often the technology is not a physical product; it may be a plan, formula or idea that can be transported on computer or fax machine, or simply carried away inside scientists' heads.

As we have said, the economic espionage threat is not confined to America's traditional adversaries. Allies can be just as interested in U.S. technological know-how as our traditional foes from the Cold War. Countries are aggressively targeting American firms at home and abroad for industrial secrets that are critical to U.S. economic security. American corporations are now facing several foreign competitors who, backed by their intelligence services, are trying to steal trade secrets and technical data on a massive scale.

What kind of people are these new spies? How do they present themselves? They may be informal representatives of their countries or people paid by their countries to spy. They may be visiting the U.S. on scientific exchanges or business tours, or with on-site inspection teams. They may be trade representatives or liaison officers at their embassies here. Some may be foreign moles placed in American companies by their country's government, or students doing research in the U.S. who serve as informal conduits to their home governments. They may be foreign business people who can manipulate long-distance the communications systems of U.S. high-tech companies. Or they may be our very own Americans, disgruntled or greedy employees of U.S. companies who, having volunteered or been recruited, are willing to sell classified, proprietary or high-tech information to other countries. (Fifty percent of attempts to misappropriate proprietary information involve U.S. employees or ex-employees.) Whoever they are, foreign or home-grown, they are generally well educated and technologically sophisticated, and certainly well able to navigate in high-tech waters.

Many U.S. high-tech industries have been targeted but, according to a recent government report, the following areas are the most vulnerable: biotechnology, aerospace, telecommunications, computer software and hardware, advanced transportation and engine technology, advanced materials and coatings including stealth technologies, energy research, defense and armaments technology, manufacturing processes, and semiconductors. Not yet classified proprietary business information is aggressively targeted. The industries listed above are of strategic interest to the U.S. because they contribute so greatly to leading-edge, critical technologies. A 1995 report by the National Counterintelligence Center adds that foreign collectors have also exhibited an interest in government and corporate financial and trade data.* Clearly, this list does not cover every high-tech area that is being targeted, but it provides a sense of some of the areas that are vulnerable.

For more threat information pertinent to the defense industry, refer to the Defense Investigative Service's Counterintelligence Center (CIC). The CIC annually publishes its own list based on an industry survey. Of particular interest to FSOs is the CIC's "Recognition of Potential Counterintelligence Issues" published in 1996. This For Official Use Only report is highly recommended to all FSOs. It discusses awareness of the foreign threat, recognition of potential CI issues and reporting CI issues.

The Methods of Espionage

Economic espionage is often conducted by using basic business intelligence-gathering methods. The Internet and dozens of commercial databases are widely available, along with such sources as trade journals and company newsletters and annual reports. So much technical information is available in the U.S. in open sources that it hardly would seem necessary to resort to illegal means; in effect, much of science and technology in this country is here for the taking. There are vast repositories of technical information with the National Technical Information Service (NTIS) and the Defense Technical Information Center (DTIC). Foreigners can make direct requests to the Department of Defense and, of course, a great deal of information is published in academic and technical journals and in newspapers and trade publications, available to anyone.

It is when we get into the gray areas involving such activities as extracting information from executives of competing companies under the guise of job interviews, or hiring away an employee from a competitor just to acquire that person's knowledge, that employees need to be alert.

In a world becoming more and more interconnected, systems for exchanging information are clearly necessary for research and commerce to thrive. The U.S. invites foreign scientists to its research institutes and laboratories in programs designed to enhance knowledge through the cross-fertilization of ideas. And we enter into exchange agreements with other countries to foster research and development, provide security or technical assistance, and so forth. Less economically developed countries--both allies and foes--do take advantage of the openness of our system. Some caution and wariness are suggested in order to prevent too much information from being disclosed.

A major means for foreign governments to obtain information is by sending their representatives to the U.S. on fact-finding visits or for training. Participants in scientific meetings, trade delegations and trade shows can easily assimilate useful information during their stays here. Other arrangements such as visitor programs, cultural exchanges and military exchanges are also utilized. One fruitful method is sending students and scholars to U.S. universities, or to government research laboratories where they are trained and also participate in research as guests of the U.S. Government. High-tech data, acquired by scientists participating in such programs, is easily transferred back to home countries, through fax, telephone, and the written word, or by memory.

Foreign governments or their representatives often attempt to acquire high-tech information by establishing joint venture companies with Americans. This allows them direct access to U.S. know-how not always available in the public domain, especially if the companies conduct classified work. Other standard business practices in this general category include mergers, strategic alliances, licensing agreements, and corporate technology agreements. It must be noted, however, that joint ventures are often encouraged by the U.S. For example, the Bureau of Export Administration in the U.S. Department of Commerce has programs to encourage such ventures with the newly independent states of the former Soviet Union, as a way to expand U.S. trade in those areas.

Another way of acquiring high-tech information is to purchase U.S. high-tech companies, preferably those with government contracts, or for foreigners to set up their own companies in the U.S. to collect information on certain technologies and to train their own personnel. Related to establishing companies in the U.S. is the commonly used device of creating front companies. These are companies set up to undertake "legitimate" business, but used by the foreign government to further its own economic espionage purposes.

Often foreigners acquire proprietary information under the guise of market research, sending surveys from abroad to ferret out product information. Even personal telephone calls, letters and fax inquiries from abroad can elicit useful information. Callers may pretend to be someone other than who they are; in the parlance of the business intelligence fraternity this is known as pretext calling.

Some economic espionage cases resemble typical old-style espionage operations conducted with the full panoply of tradecraft. Indeed, the very words used to describe the roles of participants in an economic espionage crime are borrowed directly from the classic espionage lexicon: spies, moles, recruiters, defectors.

The "best" way to acquire information from an organization or company is--in classic spy style--to recruit a mole on the inside or to send one of your own people in on a ruse, posing as someone else. Another method is to blackmail vulnerable employees of U.S. companies or to recruit foreign nationals working in U.S. subsidiaries abroad. Not all spies have been recruited. Some, perhaps disgruntled or troubled employees, past or present, of U.S. companies, have stolen materials and then sold them to foreign companies--the volunteer of classic espionage.

Equally as unscrupulous, and also patently illegal, is the outright bribing of employees to steal plans, reports and other proprietary documents, or hiring so-called consultants to spy on competitors, a practice that can include bugging competitors' offices. Other methods include theft and smuggling of goods, theft of intellectual property, tampering with companies' electronics, bribery, and so forth.

The Damage

At the industry and company level, the compromise of industrial technology often translates into lost contracts, loss of trade secrets and loss of technology--in the billions--and in the loss of technological edge over our competitors. In this age of shrinking budgets and tighter control over expenses, economic espionage can be very profitable; the less money a company has to spend on research, the greater its profit margin.

The Old Threat Still Lingers

All this discussion of economic espionage does not mean, as we pointed out earlier, that traditional, classical espionage has ceased. It only means that espionage has shifted to some

degree--away from stealing classified information to a new interest in acquiring high-tech information that might be advantageous to a foreign country. We continue to have our classical spy cases, the most famous case, of course, being Aldrich Ames, a veteran CIA intelligence officer, who volunteered highly secret and sensitive CIA information to Soviet and Russian intelligence from 1985 to 1994. It is known that at least 11 agents lost their lives and that Ames gave the KGB tens of thousands of classified documents, in what will surely be the spy case of the century. On the heels of Ames came a second CIA case, Harold Nicholson, arrested at the end of 1996 on espionage charges that he had sold secrets to Moscow for 29 months. Nicholson was a CIA operations officer.

There have been several other cases recently, involving individuals who were caught before they could do any real harm. For example, John Charlton, a retired engineer, was arrested in May 1995 for trying to sell secret documents stolen from his company at the time of his retirement. Between July and September 1993 he tried to sell the information for $100,000 to a FBI agent posing as a representative of a foreign government. In April 1996 he was sentenced to 2 years in prison and fined $50,000.

Another case in 1996 concerns a Navy machinist mate who sold an undercover FBI agent top secret information on nuclear submarines. The Petty Officer 1st Class, an instructor at the Naval Nuclear Power School in Orlando, Florida, was charged after he was video-taped turning over documents to a FBI agent posing as a Russian. The young instructor, unbeknownst to him, was dealing all the time with a FBI agent, not a foreigner. His trial is still pending.

In another recent and aborted attempt, a civilian Navy intelligence official, a naturalized American, was accused of spying for his native country in Asia after he was arrested by the FBI. This individual is charged with transferring classified information to an agent of a foreign government.

For materials on new espionage cases for inclusion in security awareness briefings, the Department of Defense Security Institute (DoDSI) publishes quarterly Recent Espionage Cases, Summaries & Sources, in which articles in the press on recent espionage cases are abstracted.

Losses caused by theft of U.S. military secrets can be massive. In times of crisis such losses can weaken and even destroy the country's national defense by alerting enemies of our military plans and new weaponry. Often the damage that results from the compromise of military secrets is impossible to repair. The information supplied to the Russians by John Walker, for example, enabled them to gain access to our weapons and sensory data, naval tactics, submarine and airborne training, military operations, and intelligence activities. In short, it permitted the Russians to measure the true capability and vulnerability of the U.S. Navy and to dramatically improve their own military positions.

Indicators of Espionage

Studies of traditional espionage cases have revealed a pattern of warning signs displayed by several of the spies in varying degrees. The most common indicators of an individual's espionage

activity or potential vulnerability to espionage are mentioned below and should be a matter of concern to security and supervisory personnel.

Signs that an individual might be involved in espionage include attempts to gain access to classified information without a valid need-to-know or without the required security clearance. Other indicators might be unauthorized reproduction or removal of classified material from the work area and secret destruction of documents. Unexplained affluence can be a possible tip-off to ongoing espionage if a legitimate source of increase income cannot be found. Sudden prosperity might be of particular concern when it follows a period of financial difficulties.

Foreign travel, on a regular basis and without sufficient explanation, might be another sign of espionage when individuals with access to classified information are involved. Job and career dissatisfaction or deep grudges against the company or the U.S. Government have also figured as predisposing elements in some cases.

Facing the Challenge

In summary, espionage against the U.S., both economic and classical, continues to occur, and the threat it poses to U.S. national security and economic well-being is immense. Increasingly, economic espionage efforts directed against the U.S. come, not only from present foes but from friends and allies, all in search of U.S. high-tech and commercial secrets. With billions of dollars invested in research and development, the U.S. is a tempting target for friendly nations, former foes, and traditional adversaries alike.

The current challenge for security professionals is to make employees understand that, despite the vast political changes around the globe, foreign intelligence activities really do continue to be directed against the U.S. Many people believe that there is no longer an espionage danger. Many believe, for example, that it is no longer necessary to restrict the flow of scientific and technical information to our highly industrialized allies or to newly emerging democracies. However, experience has shown that the U.S. often gives away far more than it gets and that scientific "exchange" is more likely than not to be a one-way street. The cheapest way to gain access to economic and scientific information is to take what is freely given (by the U.S.), or to steal it. Employees of the U.S. Government and U.S. industry must be aware of this still-present danger and be able to recognize all warning signals. Moreover, they must understand their responsibilities to report any suspicions they may have of workmates or visitors so that the appropriate authorities can investigate the situation.

- National Counterintelligence Center (1995, July). Annual report to Congress on foreign economic collection and industrial espionage. Washington, DC: Author.

Overview of Security Classification System

Classified Information Definition

As outlined by the new Executive Order 12958, classified information is official government information that has been determined to require protection in the interest of national security. All classified information (with only one exception) is under sole ownership of the U.S. Government, and employees possess no right, interest, title, or claim to such information.

Classified information exists in many forms. It may be a piece of hardware, a photograph, a film, recording tapes, notes, a drawing, a document or spoken words. Material is classified by the originator. It comes to industry via security classification guides. The degree of safeguarding required depends on the information's classification category. Three levels have been established based on the criticality of the information or material to national interests.

1. **TOP SECRET**: Information or material whose unauthorized disclosure could be expected to cause exceptionally grave damage to the national security.

2. **SECRET**: Information or material whose unauthorized disclosure could be expected to cause serious damage to the national security.

3. **CONFIDENTIAL**: Information or material whose unauthorized disclosure could be expected to cause damage to the national security.

NSI is any information that requires protection against unauthorized disclosure. The levels TOP SECRET, SECRET and CONFIDENTIAL designate this information.

The CSA has security cognizance over government classified material or information. There are also other categories of classified information that require special access authorization. Some of these are listed below.

Restricted Data (RD) is Department of Energy data concerning design, manufacture or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy.

Formerly Restricted Data (FRD) is classified information jointly determined by DOE (or its predecessors) and the DoD to be related primarily to the military utilization of atomic weapons, and removed by DOE from the Restricted Data category. It is safeguarded as National Security Information (NSI) and is subject to the restriction on transmission to other countries and regional defense organizations that apply to Restricted Data.

Information concerning these categories of classified information will be provided by the customer. Employees may hear terms such as Sensitive Compartmented Information (SCI), or Special Access Program (SAP). Assure them that if they need to know about such programs they will be told.

There are two other categories of information which, while not classified, also deserve mention.

For Official Use Only (FOUO) is unclassified government information which is exempt from general public disclosure and must not be given general circulation.

Company private or proprietary information is business information not to be divulged to individuals outside the company. Examples of this kind of information are salary and wage lists, technical and research data, and trade secrets. You may want to describe the minimum security requirements for such information. CSAs generally recommend that facilities and their employees refrain from labeling company proprietary information as CONFIDENTIAL, SECRET, etc., since confusion between these and official government classification markings may result. Use markings such as COMPANY PROPRIETARY or PRIVATE, etc.

Access Requirements

Authorized access to classified information may be granted only when two conditions are met. First, the recipient must have a valid and current security clearance at a level at least as high as the information to be released. Second, the recipient must demonstrate the need for access to the classified information. This is referred to as need-to-know.

Before granting access to classified information, security must establish that the individual has a genuine need to know, that this information is necessary for the performance of the individual's job duties on a classified contract or program. This applies to everyone regardless of rank, position, or amount of clearances and access.

Need-to-know is integrally related to clearance level. But a security clearance alone is not sufficient for access to classified information. Access to classified information is determined based on (1) the level of clearance and (2) the need for access in order to perform official or contractual duties of employment.

It is the responsibility of the possessor of classified information to ensure the proper clearance and need-to-know of the recipient. The possessor must also advise the recipient of the classification of the information disclosed.

Need-to-know confirmation for both internal employees and visitors should come from a security department advisor or representative. If there is doubt as to whether or not a person has a need-to-know, the employee should check with the proper authority prior to release of any classified information. Establishment of need-to-know is essential. Explain that it is far better to delay release to an authorized person than to disclose classified information to one who is unauthorized.

Employee Reporting Requirements

The NISP is based to a large extent on individual trust and responsibility, and employee reporting requirements are a critical element in the program. Employees are required to report any contacts of a suspicious nature; adverse types of information; the possible loss, compromise or suspected compromise of classified information; and any change in employee status. Employee reporting requirements are designed to protect the employee and to counter any possible foreign intelligence threat. Employees need to recognize that it is their personal responsibility to understand and report these conditions to the security office as circumstances warrant.

Suspicious Contacts

Employees are required to report any suspicious behavior or occurrences that may occur at any time. This includes all contacts with known or suspected intelligence officers from any country, or any contact that suggests the employee may be the target of an attempted exploitation by a foreign intelligence service (NISPOM 1-302b). More specifically, employees must report to security any of the following events:

- Any efforts, by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified or sensitive unclassified information
- Any efforts, by any individual, regardless of nationality, to compromise a cleared employee
- Any contact by a cleared employee with a known or suspected intelligence officer from any country
- Any contact which suggests an employee may be the target of an attempted exploitation by the intelligence services of another country.

If there is any problem as to whether any specific situation is reportable, questions should be taken to the security office.

Adverse Information

The NISPOM (1-302a) requires that cleared contractor employees report to their respective security department adverse information regarding other cleared employees. As a general rule, adverse information is that which reflects unfavorably on the trustworthiness or reliability of the employee and suggests that the person's ability to safeguard classified information may be impaired (see illustration).

Illustration
Adverse Information Examples

- Arrest for any serious violation of the law

- Excessive use of alcohol or abuse of prescription drugs
- Any use of illegal drugs
- Bizarre or notoriously disgraceful conduct
- Sudden unexplained affluence
- Treatment for mental or emotional disorders

Security professionals have found that convincing employees to report adverse information on coworkers is one of their most difficult tasks. Employees find it hard to be objective in assessing the impact of personal problems on job performance or continuing clearance eligibility. Many employees feel that by reporting such behavior they are playing a policing role, a role they have no desire to perform. Inform employees that they should be vigilant and not turn a blind eye to the questionable behavior or practices of coworkers. On the other hand, warn employees against creating an atmosphere of suspicion or intrusiveness in the work place.

The Aldrich Ames case provides a lesson on what can happen if adverse information is not reported. Ames, a CIA employee, had clear signs of adverse behavior including excessive drinking and unexplained affluence. While noticed, these behaviors were not reported until much too late. In 1984, motivated by financial troubles, Ames volunteered highly SECRET and sensitive CIA information to Soviet and Russian intelligence. After 9 years of selling secrets for over $2.5 million, Ames showed signs of living beyond the means afforded by his government income. As a result of this compromise 11 agents lost their lives and a large amount of information regarding the CIA's Soviet Intelligence efforts was lost.

Your human resources staff can assist in developing this portion of the briefing. They will be able to inform you about legal constraints as well as company policy and procedures relating to employee support. This is a good opportunity to mention the resources provided by the company and community to aid employees with personal problems. Many of these services will be free or covered by benefit plans.

Human resources and administrative personnel are also in a position to furnish you with reportable information not available to other employees. These personnel should be reminded of their responsibility to do so. Wage garnishments, for example (excepting those resulting from court-ordered child support), are considered adverse information that should be reported.

Explain the process for handling adverse information reports. Stress the confidentiality aspects involved and the anonymity granted to the source of such information. Emphasize the thoroughness of the investigation which is conducted to validate the information and the protection which is afforded the individual being investigated. By discussing an actual event and walking your audience through the process and the safeguards in place, many common questions will be answered.

While the security professional should take into consideration the points made above, he or she should not lose sight of security-driven objectives behind this reporting requirement. Adverse information should be reported to protect the individual from being placed in a position where he or she could be exploited and persuaded to commit a security violation, or even espionage. There are many espionage cases in which a human weakness was exploited by hostile intelligence

agents. If employees are unsure whether certain behavior requires reporting, they should consult their security office.

Loss or Compromise

Employees are required to report any loss, compromise or suspected compromise of classified information, foreign or domestic, to the appropriate security office (NISPOM 1-303). Reporting provides employees with an opportunity to extricate themselves from a compromising situation and enhances the protection of national security information. Ideally, the facility's security posture should be enhanced after a security infraction, because security professionals will have an opportunity to address and correct any problems. When an employee covers up a known security infraction, the security education process is undermined because mistakes have been made and security has not been able to learn from them. The relationship of mutual trust between the contractor and the CSA is also jeopardized. In addition, not reporting a known security compromise may in itself constitute a major security violation, regardless of the severity of the unreported incident.

Violations may include acts such as misplacing, losing, improperly storing, improperly transmitting, and leaving classified material unattended. Employees should be provided with a list of security violations to clarify any uncertainties in this area.

Changes in Personal Status

Cleared employees are required to report any changes in their personal status. These are listed in detail in the NISPOM (1-302c and d) and include:

- Change in name
- Termination of employment
- Change in marital status
- Change in citizenship
- Possibility of future access to classified information has been reasonably foreclosed
- New status as a Representative of a Foreign Interest (RFI)
- Change in RFI status.

Other Reporting Requirements

In addition to the above, employees are required to report any act of sabotage or possible sabotage, espionage or attempted espionage, and any subversive or suspicious activity. Employees should also be encouraged to report any attempts to solicit classified information, unauthorized persons on company property, citizenship by naturalization (NISPOM 1-302e), unwillingness to work on classified information (NISPOM 1-302f), and disclosure of classified information to an unauthorized person, along with any other condition that would qualify as a security violation or which common sense would dictate as worth reporting.

Security Procedures

Safeguarding Classified Information

One of the most fundamental requirements of the NISP is the proper safeguarding and storage of classified information. It is essential that classified information be at all times properly safeguarded or stored in accordance with the requirements of the NISPOM. A useful way to describe safeguarding is to divide the topic into two: safeguarding when classified materials are in use, and when they are not.

When In Use

It is the responsibility of cleared individuals with classified documents to safeguard the material at all times (NISPOM 5-100). While in use, classified material should be given sufficient protection to reasonably ward against loss or compromise. As a starting point, inform all cleared employees that classified information cannot be discussed over unsecured telephones, in public places, or in any manner that may allow transmittal or interception by unauthorized persons (NISPOM 5-101). This includes not working on classified material on unapproved computers. Following are some suggestions for protective measures to be used when working with classified information.

Classified material should never be left unsecured or unattended. Constant surveillance by an authorized individual who is able to exercise direct control over the classified material will provide reasonable security. The authorized individual must have the appropriate clearance and need-to-know, and must take action to prevent access to the material when others who do not have the appropriate clearance and need-to-know are present.

When working with classified material in an unsecured area, any open curtains or doors should be closed. It is prudent to also post a sign, declaring "CLASSIFIED WORK IN PROGRESS". If a visitor or unauthorized employee is present, a classified document must be protected by either covering it, turning it face down, or placing it in an approved storage container.

The security professional should give special attention to the proper protection of classified material during lunch period, coffee breaks, and other work breaks. When employees are working on classified material and leave their desk, the documents must be locked in an approved storage container. They must never be tucked in a desk drawer, file cabinet, credenza, key-lock file, etc., for even the briefest period. Note that this regulation also covers the typewriter ribbons being used for classified material. Remind employees that proper protection of classified information is not afforded at their home. Classified material should never be taken

home. In general, classified information should be stored as soon as possible after it has been used.

When Not In Use

When not in use, classified material should be properly secured in an approved container, unless it is being guarded by another properly cleared person with a need-to-know. The storage of classified material in anything other than an approved container is strictly prohibited.

Approved storage containers should remain locked unless they are under constant surveillance and control. The employee should always shield the combination from the sight of others when opening a classified container. Combination padlocks must be stored inside or locked on the container when it is open. This prevents tampering or replacement of the padlock by an unauthorized person.

Combinations to classified storage containers and controlled areas are themselves classified and must therefore be protected at the same level of the data they are protecting. Combinations to classified containers should be committed to memory. If written down, the slips of paper may not be kept in desks, wallets, notebooks, etc.; they must be secured at the same level as the data. In addition, they cannot be written down in a coded form, such as backwards, out of order, etc. Only in certain circumstances can combinations be written down and safeguarded as a piece of classified material. In choosing a combination, employees should avoid persons, places or things that can be easily identified with them, such as a birthday, spouse's name, favorite sports team, license plate, etc. At many facilities, there is a strict prohibition against sharing safe combinations, since only those authorized to have access to the container may know the combination. Most importantly, combinations should be changed periodically depending on the type of material being protected. For example NATO requires annual combination changes. The combination must be changed whenever anyone with access leaves the organization or transfers to another group.

Some of the above precautions may not apply if employees are working with classified material in a closed area or Sensitive Compartmented Information Facility (SCIF). If SCIF working procedures are different, they should be explained. If circumstances prevent an employee from storing material in the prescribed container or document control center (i.e., after working hours), then the procedures for delivering the material to the security office or other secure storage facility should be described. Company policy regarding the storage of unclassified documents with classified materials should also be clarified. Company-specific policy regarding the administration of combinations, the safeguarding of classified combinations, and the changing of combinations may also need to be discussed.

Security Markings

All classified material should be marked in a conspicuous manner by the originator of the material. These markings inform recipients of the classification level and the degree of protection

the material requires. Classification marking can be an elaborate process and unique requirements exist for different types of materials. Inform employees how to obtain a marking guide and who to contact for additional information if their assignments require guidance in that area. The initial security briefing may represent a good opportunity to hand out any marking instruction booklets that employees may need in performing their jobs.

If indoctrinated employees are likely to be exposed to classified information on a regular basis, they should be shown examples of properly marked classified materials. A brief overview of the markings for different materials employees are likely to encounter would be helpful. Identification markings, the overall classification marking, portion and page markings, and other page markings should also be described.

The level of detail on marking guidance provided during the initial briefing will largely be determined by local conditions and the time allotted. At many facilities it will only be necessary to instruct people on the significance of classified markings and how to recognize them when properly used. Security professionals have expressed satisfaction with the NISPOM marking supplement and the ISOO marking guide. Because of this and the wide availability of marking instructional materials, a section devoted to classified markings will not be provided in this Guide.

Reproduction of Classified Material

Copies of classified materials are subject to the same security controls as original classified material. You need to emphasize that no reproduction of classified materials is allowed without prior approval from the contracting authority, meaning the individual or office responsible for classified document accountability. In most instances, only certain levels of classified information may be reproduced without written authorization from the contracting activity.

The procedure for initiating a reproduction request in medium and larger facilities typically requires the employee to complete a request for classified reproduction, obtain appropriate signatures authorizing the reproduction, and bring the material to a reproduction clerk. Copies of TOP SECRET documents will then be numbered, marked, and logged as required. Describe the reproduction control system in place at your facility and how it ensures that reproduction of classified materials is kept to an absolute minimum.

Another important point is that copying classified documents on office photocopiers is prohibited unless the machines are designated for such use and proper controls are in place. While no longer a requirement, convenience copiers in the facility should be labeled to warn individuals against copying classified information on them. Employees should be told where the only authorized copiers for classified information are located so that there can be no uncertainty regarding this issue.

Employees who are found with unauthorized or bootleg copies of classified information will face stiff penalties. Confiscation of the materials and the recording of a security violation may be two of the least serious consequences.

Security Violations Policy

Some employees may take the rules described in the indoctrination briefing more to heart if the consequences of not following them are fully explained. It may be a good idea to inform employees of your company's policy regarding violations.

An excellent way to introduce the subject is to detail the common security violations at your facility in the last year or so. Such narratives, based on actual events of immediate relevance, can make a lasting impression on the newly indoctrinated employee. Common violations such as combination locks not being spun off correctly, classified material being left out, bootleg copies of classified information, recording combinations for retention in wallets or purses, granting unauthorized persons access to classified information, etc., will probably feature prominently in any such list (see illustration).

Illustration
Common Security Violations

- Classified material left out
- Unsecured, unattended security containers
- Unsecured combinations
- Removal without approval
- Lost classified information
- Copying or destroying classified material
- Unauthorized/improper transmission of classified material
- Disclosure of/permitting access to classified information to an unauthorized person
- Generating briefing handouts for classified material on a non-approved computer

end of Illustration

The distinction between inadvertent and deliberate violations (or acts of omission and acts of commission) should be made and the relative gravity of the latter should be emphasized. Generally the type of penalty given employees will depend upon the seriousness of the violation, the number of their previous violations, and whether the violation was a deliberate act. Since violation policies differ considerably among companies, you should describe the system of penalties in place at your facility within the Standard Practices and Procedures.

Employees should know that any perceived or suspected violation will be investigated to ascertain whether or not a compromise of classified material occurred. If a compromise is suspected, a report which identifies the party at fault must be submitted to DIS. An adverse information report identifying the individual responsible will also be filed and noted in the employee's records. Violations have a negative impact on both the employee and the company. The ability of the employee to receive and retain new clearances or accesses may be affected. In situations where the violation is sufficiently grave, the company may choose to terminate the employee. Each violation has a negative effect on the company's ability to compete in the classified marketplace.

Visitor Control Procedures

The procedures surrounding visitor control for cleared employees making classified visits to other cleared facilities or hosting visits involving classified information should be described. Employees needing access to classified information at an outside facility will have to submit a Visit Authorization Letter (VAL) with enough lead time for processing by their security office and forwarding to the receiving facility for approval (NISPOM 6-101). The lead time required will vary depending on the facility and the visit destination. VALs certify, among other things, the clearance status of the visitor, the visitor's need-to-know, and the type and level of information to be accessed.

If classified material will be needed at the facility to be visited, it will generally have to be mailed ahead. If the material is to be hand-carried, then additional authorization and a hand courier briefing may be required. The different categories of classified visits may be described, i.e., contract related and non-contract related visits. Certain categories of visits, such as not-contract related visits, will require user agency authorization (NISPOM 6-109).

All cleared employees should know something about the badge-issuing policies of visitor control and what the different colors or codes signify. It is especially important that employees recognize the badges that require escorts and those that don't. Remind employees that classified information should only be discussed among people with appropriate clearance levels and a need-to-know.

Additional points can be discussed: What to do when classified information is acquired outside the facility, and how to process visitors arriving with hand held classified information. The specific forms and procedures followed in controlling incoming and outgoing visits will vary from one facility to another, and any employee requiring such information should be instructed to contact the security office.

Transmittal of Classified Material

The transmittal of classified material outside of and within cleared facilities will generally be performed by members of the security staff, so most employees will not need to be briefed in this area. For the few cases in which cleared employees perform these duties, the following is provided.

Classified Document Control

The transmittal of classified material at cleared facilities will generally be performed by a document control office. At larger facilities a classified document control center may exist, while at smaller facilities document control will most likely be performed out of the security office, perhaps by the FSO. Identify for your employees the office responsible (hereafter referred to as

the document control office) and who they should contact for questions on transmittal. As a general rule, no employee or visitor will be allowed to bring classified material in or out of a cleared facility without first logging in the material at the document control office.

Each facility is required to maintain complete records for all TOP SECRET and NATO material and foreign government information in its possession. In most facilities the accountability system will be managed by the document control office. Explain how the accountability system functions at your facility.

Formal accountability for SECRET material is no longer required. The NISPOM (5-201) simply states that the facility must have an information management system (IMS) for retrieval of SECRET material when the contract is over. Despite these relaxed requirements, many facilities still account for SECRET and CONFIDENTIAL material.

Methods for transmittal of classified information depend on the material's classification and its destination. A convenient way in which to structure a discussion of the topic is by addressing separately transmittal within and outside the facility.

Transmittal Within the Facility

Classified material transmitted within a facility must be ensured a degree of protection adequate for the level of classification involved. Generally, this means that before any transmittal the sender must determine that the prospective recipient has the proper clearance and a need-to-know. Depending on the facility, direct transfers of classified material from one employee to another may or may not be authorized. Explain your company's policy on this issue, as well as what approved communications circuits may be available for within-facility transmission.

In facilities where SECRET and above material may be directly transferred or loaned from one employee to another, the completion of hand receipts establishing accountability for the material is recommended. For TOP SECRET materials, hand receipts are required. When filling out a hand receipt, the recipient should always verify that the information contained therein is accurate. When direct transfer of classified material between employees is prohibited, the document control will serve as the focal point for the receipt and reissue of these materials.

Delivery within the facility may require that the material be double wrapped and carried by a properly cleared and authorized company employee or messenger. The procedures for double-wrapping are easy to understand and basic enough to be covered in the initial briefing.

Clarify whether transmittal via the facility's internal mail system is allowed. If permitted, caution employees that such material must be delivered to the recipient and never left unattended in a mailbox. Describe the physical areas of the facility in which the authorized transport of classified material is permitted and prohibited. Though procedures for transmitting classified information may vary considerably across facilities, sufficient protection must always be afforded to ensure that no unauthorized disclosure takes place.

Transmittal Outside the Facility

Classified material that is transmitted outside the facility must be safeguarded in a manner that prevents loss or unauthorized access (NISPOM 5-400). Any outgoing classified material should be processed through the facility's document control office to ensure proper authorization, wrapping, and transmittal. Written authorization of the user agency is always required prior to transmitting TOP SECRET material outside the facility (NISPOM 5-402). Additional restrictions that apply to the transmittal of TOP SECRET material should also be mentioned. For example, use of the U.S. Postal Service for transmittal of TOP SECRET materials is prohibited.

NISPOM regulations allow SECRET and CONFIDENTIAL material to be transmitted within the United States using the U.S. Postal Service and other DIS authorized couriers (commercial, military, etc.). SECRET material may be sent by U.S. Registered Mail or U.S. Express Mail (NISPOM 5-403). CONFIDENTIAL material may be sent by U.S. Registered, Express, or Certified Mail (NISPOM 5-404). (For more information, refer to ISL 95-1 #17.) Your facility may prohibit the use of the U.S. Postal Service for mailing classified information. If so, make sure your audience knows. Transmission over COMSEC circuits will also be allowed if authorized by the user agency. Classified material must be double wrapped and properly marked prior to its physical transmittal outside the facility.

Classified information being sent to or from a foreign government must come through government channels, e.g., DIS. Transmission directly to or from a foreign government is NOT authorized.

Hand Carrying Classified Material

Because of the hazards associated with hand carrying classified material outside the facility, this form of transmittal is discouraged. When hand carrying is absolutely necessary, several security criteria must be met. These include making sure that the courier has the appropriate security clearance and has been briefed on his or her responsibility for safeguarding the classified information. The courier must maintain physical custody of the package until it is properly signed for or stored. In addition, it should be verified that the firm being visited has the capability to safeguard classified material. If an overnight stop is required, arranging for storage of the material at an appropriate authorized facility should be made ahead of time. Classified material may not be stored in a hotel room or safe, public locker or residence.

The hand carrying of classified documents outside the facility requires coordination among all parties involved and may entail advance notification requirements, completion of a courier authorization form, the procurement of a classified material pass, along with several authorizing signatures, and other measures depending on the facility and the specific circumstances. All couriers, escorts and hand carriers must possess an identification card (NISPOM 5-410).

If the classified material is to be hand carried aboard a commercial passenger aircraft, further requirements will apply, including the requirement for a Letter of Authorization. Other

requirements will be found in the NISPOM (5-411) and do not need to be detailed in the initial briefing.

When faced with the pressures of travel, people sometimes forget or neglect their safeguarding responsibilities. There are many instances in which TOP SECRET and SECRET materials have been left in airports, restaurants, and rental cars. Regrettably, many of these violations take place on the return leg of an otherwise successful and profitable trip. In most cases, however, classified material can be mailed back to the home facility. This ensures secure transmittal of the material and helps the traveler avert many of the security inconveniences associated with hand carrying.

Stress to your audience that classified material cannot be studied on an airplane or in any public vehicle. The courier should not voluntarily reveal the existence of classified material or draw attention to it. If classified material cannot be maintained under the courier's personal custody, the incident must be reported to the security officials at the facility upon return. Since hand carrying of classified material outside facilities is not a common or encouraged activity, it will not be referred to anywhere else in the Guide.

Transmittal Outside the United States

Classified material may be transmitted outside the United States, Puerto Rico, or a U.S. Possession or Trust Territory only under the provisions of a classified contract or with written authorization from the user agency. In general, contractors are not allowed to transmit classified material directly to a foreign interest. Such transmission must be made through established government-to-government channels.

Some of the methods of transmittal for SECRET and CONFIDENTIAL material outside the United States include registered mail through U.S. Army, Navy, or Air Force postal facilities, or an appropriately cleared contractor employee designated by the contractor.