ISO_UFO PDF Legends

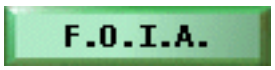
The following legends are applicable for Adobe PDF Files with ISO_UFO presentations:

Go to top of file or to next pdf up-arrow marker

Go to bottom of file or to next pdf down-arrow marker

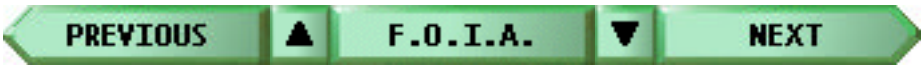
Go to previous pdf file

Go to next pdf file



Return to Freedom of Information Act Page

Note: Any typos found in this document are transposition errors due to retyping and not necessarily an error in the original document.



[According to the Phrack editor, this is the complete manual, except that it is, of course, missing the NSA director's photo. According to subsequent investigation, it was found that the manual is indeed the real thing. NSA says it is not classified, but could only be officially obtained through Freedom of Information Act action. History of dissemination, according to Jeff Davis:

Chris Goggans received the NSA Employee's Manual anonymously in the mail. He digitized it and published it in Phrack. Grady ward found it there and posted it to Usenet. The NSA called him to find out where he got it.

At that point, Jeff Davis mass mailed it to all the media contact email

adresses listed in Adam Gaffin's "EFF's Guide to the Internet".]

Subject: NSA employee's security manual

From: Phrack Magazine issue #45 30 March 94

Editor:

Chris Goggans (aka Erik Bloodaxe)
603 W. 13th #1A-278
Austin, TX 78701
erikb@mindvox.phantom.com

(This reputedly is from the NSA new employee security manual) posted to Usenet talk.politics.crypto and alt.politics.org.nsa Phrack is archived at Len Rose's anonymous ft site ftp.netsys.com

SECURITY GUIDELINES

This handbook is designed to introduce you to some of the basic security principles and procedures with which all NSA employees must comply. It highlights some of your security responsibilities, and provides guidelines for answering questions you may be asked concerning your association with this Agency. Although you will be busy during the forthcoming weeks learning your job, meeting co-workers, and becoming accustomed to a new work environment, you are urged to become familiar with the security information contained in this handbook. Please note that a listing of telephone numbers is provided at the end of this handbook should you have any questions or concerns.

INTRODUCTION

In joining NSA you have been given an opportunity to participate in the activities of one of the most important intelligence organizations of the United States Government. At the same time, you have also assumed a trust which carries with it a most important individual responsibility—the safeguarding of sensitive information vital to the security of our nation.

While it is impossible to estimate in actual dollars and cents the value of the work being conducted by this Agency, the information to which you will have access at NSA is without question critically important to the defense of the United States. Since this information may be useful only if it is kept secret, it requires a very special measure of protection. The specific nature of this protection is set forth in various Agency security regulations and directives. The total NSA Security Program, however, extends beyond these regulations. It is based upon the concept that security begins as a state of mind. The program is designed to develop an appreciation of the need to protect information vital to the national defense, and to foster the development of a level of awareness which will make security more than routine compliance with regulations.

At times, security practices and procedures cause personal inconvenience. They take time and effort and on occasion may make it necessary for you to voluntarily forego some of your usual personal perogatives. But your compensation for the inconvenience is the knowledge that the work you are accomplishing at NSA, within a framework of sound security practices, contributes significantly to the defense and continued security of the United States of America.

I extend to you my very best wishes as you enter upon your chosen career or assignment with NSA.

Philip T. Pease
Director of Security

INITIAL SECURITY RESPONSIBILITIES

ANONYMITY

Perhaps one of the first security practices with which new NSA personnel should become acquainted is the practice of anonymity. In an open society such as ours, this practice is necessary because information which is generally available to the public is available also to hostile intelligence. Therefore, the Agency mission is best accomplished apart from public attention. Basically, anonymity means that NSA personnel are encouraged not to draw attention to themselves nor to their association with this Agency. NSA personnel are also cautioned neither to confirm nor deny any specific questions about NSA activities directed to them by individuals not affiliated with the Agency.

The ramifications of the practice of anonymity are rather far reaching, and its success depends on the cooperation of all Agency personnel. Described below you will find some examples of situations that you may encounter concerning your employment and how you should cope with them. Beyond the situations cited, your judgement and discretion will become the deciding factors in how you respond to questions about your employment.

ANSWERING QUESTIONS ABOUT YOUR EMPLOYMENT

Certainly, you may tell your family and friends that you are employed at or assigned to the National Security Agency. There is no valid reason to deny them this information. However, you may not disclose to them any information concerning specific aspects of the Agency's mission, activities, and organization. You should also ask them not to publicize your association with NSA.

Should strangers or casual acquaintances question you about your place of employment, an appropriate reply would be that you work for the Department of Defense. If questioned further as to where you are employed within the Department of Defense, you may reply, "NSA." When you inform someone that you work for NSA (or the Department of Defense) you may expect that the next question will be, "What do you do?" It is a good idea to anticipate this question and to formulate an appropriate answer. Do not act mysteriously about your employment, as that would only succeed in drawing more attention to yourself.

If you are employed as a secretary, engineer, computer scientist, or in a clerical, administrative, technical, or other capacity identifiable by a general title which in no way indicates how your talents are being applied to the mission of the Agency, it is suggested that you state this general title. If you are employed as a linguist, you may say that you are a linguist, if necessary. However, you should not indicate the specific language(s) with which you are involved.

The use of service specialty titles which tend to suggest or reveal the nature of the Agency's mission or specific aspects of their work. These professional titles, such as cryptanalyst, signals collection officer, and intelligence research analyst, if given verbatim to an outsider, would likely generate further questions which may touch upon the classified aspects of your work. Therefore, in conversation with outsiders, it is suggested that such job titles be generalized. For example, you might indicate that you

are a "research analyst." You may not, however, discuss the specific nature of your analytic work.

 ANSWERING QUESTIONS ABOUT YOUR AGENCY TRAINING

During your career or assignment at NSA, there is a good chance that you will receive some type of job-related training. In many instances the nature of the training is not classified. However, in some situations the specialized training you receive will relate directly to sensitive Agency functions. In such cases, the nature of this training may not be discussed with persons outside of this Agency.

If your training at the Agency includes language training, your explanation for the source of your linguistic knowledge should be that you obtained it while working for the Department of Defense.

You Should not draw undue attention to your language abilities, and you may not discuss how you apply your language skill at the Agency.

If you are considering part-time employment which requires the use of language or technical skills similar to those required for the performance of your NSA assigned duties, you must report (in advance) the anticipated part-time work through your Staff Security Officer (SSO) to the Office of Security's Clearance Division (M55).

VERIFYING YOUR EMPLOYMENT

On occasion, personnel must provide information concerning their employment to credit institutions in connection with various types of applications for credit. In such situations you may state, if you are a civilian employee, that you are employed by NSA and indicate your pay grade or salary. Once again, generalize your job title. If any further information is desired by persons or firms with whom you may be dealing, instruct them to request such information by correspondence addressed to: Director of Civilian Personnel, National Security Agency, Fort George G. Meade, Maryland 20755-6000. Military personnel should use their support group designator and address when indicating their current assignment.

If you contemplate leaving NSA for employment elsewhere, you may be required to submit a resume/job application, or to participate in extensive employment interviews. In such circumstances, you should have your resume reviewed by the Classification Advisory Officer (CAO) assigned to your organization. Your CAO will ensure that any classified operational details of your duties have been excluded and will provide you with an unclassified job description. Should you leave the Agency before preparing such a resume, you may develop one and send it by registered mail to the NSA/CSS Information Policy Division (Q43) for review. Remember, your obligation to protect sensitive Agency information extends beyond your employment at NSA.

THE AGENCY AND PUBLIC NEWS MEDIA

>From time to time you may find that the agency is the topic of reports or articles appearing in public news media—newspapers, magazines, books, radio and TV. The NSA / CSS Information Policy Division (Q43) represents the Agency in matters involving the press and other media. This office serves at the Agency's official media center and is the Director's liaison office for public relations, both in the community and with other government agencies. The Information Policy Division must approve the release of all information for and about NSA, its mission, activities, and personnel. In order to protect the aspects of Agency operations, NSA personnel must refrain from either confirming or denying any information concerning the Agency or its activities which may appear in the public media. If you are asked about the activities of NSA, the best response is "no comment." You should the notify Q43 of the attempted inquiry. For the most part, public references to NSA are based upon educated guesses. The Agency does not normally make a practice of issuing public statements about its activities.

GENERAL RESPONSIBILITIES

 ESPIONAGE AND TERRORISM

During your security indoctrination and throughout your NSA career you will become increasingly aware of the espionage and terrorist threat to the United States. Your vigilance is the best single defense in protecting NSA information, operations, facilities and people. Any information that comes to your attention that suggests to you the existence of, or potential for, espionage or terrorism against the U.S. or its allies must be promptly reported by you to the Office of Security.

There should be no doubt in your mind about the reality of the threats. You are now affiliated with the most sensitive agency in government and are expected to exercise vigilance and common sense to protect NSA against these threats.

CLASSIFICATION

Originators of correspondence, communications, equipment, or documents within the Agency are responsible for ensuring that the proper classification, downgrading information and, when appropriate, proper caveat notations are assigned to such material. (This includes any handwritten notes which contain classified information). The three levels of classification are Confidential, Secret and Top Secret. The NSA Classification Manual should be used as guidance in determining proper classification. If after review of this document you need assistance, contact the Classification Advisory Officer (CAO) assigned to your organization, or the Information Policy Division (Q43).

NEED-TO-KNOW

Classified information is disseminated only on a strict “need-to-know” basis. The “need-to-know” policy means that classified information will be disseminated only to those individuals who, in addition to possessing a proper clearance, have a requirement to know this information in order to perform their official duties (need-to-know). No person is entitled to classified information solely by virtue of office, position, rank, or security clearance.

All NSA personnel have the responsibility to assert the “need-to-know” policy as part of their responsibility to protect sensitive information. Determination of “need-to-know” is a supervisory responsibility. This means that if there is any doubt in your mind as to an individual’s “need-to-know,” you should always check with your supervisor before releasing any classified material under your control.

FOR OFFICIAL USE ONLY

Separate from classified information is information or material marked “FOR OFFICIAL USE ONLY” (such as this handbook). This designation is used to identify that official information or material which, although unclassified, is exempt from the requirement for public disclosure of information concerning government activities and which, for a significant reason, should not be given general circulation. Each holder of “FOR OFFICAL USE ONLY” (FOUO) information or material is authorized to disclose such information or material to persons in other departments or agencies of the Executive and Judicial branches when it is determined that the information or material is required to carry our a government function. The recipient must be advised that the information or material is not to be disclosed to the general public. Material which bears the “FOR OFFICIAL USE ONLY” caveat does not come under the regulations governing the protection of classified information. The unauthorized disclosure of information marked “FOR OFFICIAL USE ONLY” does not constitute an unauthorized disclosure of classified defense information. However, Department of Defense and NSA regulations prohibit the unauthorized disclosure of information designated “FOR OFFICIAL USE ONLY.” Appropriate administrative action will be taken to determine responsibility and to apply corrective and/or disciplinary measures in cases of unauthorized disclosure of information which bears the “FOR OFFICIAL USE ONLY” caveat. Reasonable care must be exercised in limiting the dissemination of “FOR OFFICIAL USE ONLY” information. While you may take this handbook home for further study, remember that is does contain “FOR OFFICIAL USE ONLY” information which should be protected.

PREPUBLICATION REVIEW

All NSA personnel (employees, military assignees, and contractors) must submit for review any planned articles, books, speeches, resumes, or public statements that may contain classified, classifiable, NSA-derived, or unclassified protected information, e.g., information relating to the organization, mission, functions, or activities of NSA. Your obligation to protect this sensitive information is a lifetime one. Even when you resign, retire, or otherwise end your affiliation with NSA, you must submit this type of material for prepublication review. For additional details, contact the Information Policy Division (Q43) for an explanation of prepublication review procedures.

PERSONNEL SECURITY RESPONSIBILITIES

Perhaps you an recall your initial impression upon entering an NSA facility. Like most people, you probably noticed the elaborate physical security safeguards—fences, concrete barriers, Security Protective Officers, identification badges, etc. While these measures provide a substantial degree of protection for the information housed within our buildings, they represent only a portion of the overall Agency security program. In fact, vast amounts of information leave our facilities daily in the minds of NSA personnel, and this is where our greatest vulnerability lies. Experience has indicated that because of the vital information we work with at NSA, Agency personnel may become potential targets for hostile intelligence efforts. Special safeguards are therefore necessary to protect our personnel.

Accordingly, the Agency has an extensive personnel security program which establishes internal policies and guidelines governing employee conduct and activities. These policies cover a variety of topics, all of which are designed to protect both you and the sensitive information you will gain through your work at NSA.

ASSOCIATION WITH FOREIGN NATIONALS

As a member of the U.S. Intelligence Community and by virtue of your access to sensitive information, you are a potential target for hostile intelligence activities carried out by or on behalf of citizens of foreign countries. A policy concerning association with foreign nationals has been established by the Agency to minimize the likelihood that its personnel might become subject to undue influence or duress or targets of hostile activities through foreign relationships.

As an NSA affiliate, you are prohibited from initiating or maintaining associations (regardless of the nature and degree) with citizens or officials of communist-controlled, or other countries which pose a significant threat to the security of the United States and its interests. A comprehensive list of these designated countries is available from your Staff Security Officer or the Security Awareness Division. Any contact with citizens of these countries, no matter how brief or seemingly innocuous, must be reported as soon as possible to your Staff Security Officer (SSO). (Individuals designated as Staff Security Officers are assigned to every organization; a listing of Staff Security Officers can be found at the back of this handbook).

Additionally, close and continuing associations with any non-U.S. citizens which are characterized by ties of kinship, obligation, or affection are prohibited. A waiver to this policy may be granted only under the most exceptional circumstances when there is a truly compelling need for an individual's services or skills and the security risk is negligible.

In particular, a waiver must be granted in advance of a marriage to or cohabitation with a foreign national in order to retain one's access to NSA information. Accordingly, any intent to cohabitate with or marry a non-U.S. citizen must be reported immediately to your Staff Security Officer. If a waiver is granted, future reassignments both at headquarters and overseas may be affected.

The marriage or intended marriage of an immediate family member (parents, siblings, children) to a foreign national must also be reported through your SSO to the Clearance Division (M55).

Casual social associations with foreign nationals (other than those of the designated countries mentioned above) which arise from normal living and working arrangements in the community usually do not have to be reported. During the course of these casual social associations, you are encouraged to extend the usual social amenities. Do not act mysteriously or draw attention to yourself (and possibly to NSA) by displaying an unusually wary attitude.

Naturally, your affiliation with the Agency and the nature of your work should not be discussed. Again, you should be careful not to allow these associations to become close and continuing to the extent that they are characterized by ties of kinship, obligation, or affection.

If at any time you feel that a "casual" association is in any way suspicious, you should report this to your Staff Security Officer immediately. Whenever any doubt exists as to whether or not a situation should be reported or made a matter of record, you should

decided in favor of reporting it. In this way, the situation can be evaluated on its own merits, and you can be advised as to your future course of action.

CORRESPONDENCE WITH FOREIGN NATIONALS

NSA personnel are discouraged from initiating correspondence with individuals who are citizens of foreign countries. Correspondence with citizens of communist-controlled or other designated countries is prohibited. Casual social correspondence, including the "penpal" variety, with other foreign acquaintances is acceptable and need not be reported. If, however, this correspondence should escalate in its frequency or nature, you should report that through your Staff Security Officer to the Clearance Division (M55).

EMBASSY VISITS

Since a significant percentage of all espionage activity is known to be conducted through foreign embassies, consulates, etc., Agency policy discourages visits to embassies, consulates or other official establishments of a foreign government. Each case, however, must be judged on the circumstances involved. Therefore, if you plan to visit a foreign embassy for any reason (even to obtain a visa), you must consult with, and obtain the prior approval of, your immediate supervisor and the Security Awareness Division (M56).

AMATEUR RADIO ACTIVITIES

Amateur radio (ham radio) activities are known to be exploited by hostile intelligence services to identify individuals with access to classified information; therefore, all licensed operators are expected to be familiar with NSA/CSS Regulation 100-1, "Operation of Amateur Radio Stations" (23 October 1986). The specific limitations on contacts with operators from communist and designated countries are of particular importance. If you are an amateur radio operator you should advise the Security Awareness Division (M56) of your amateur radio activities so that detailed guidance may be furnished to you.

UNOFFICIAL FOREIGN TRAVEL

In order to further protect sensitive information from possible compromise resulting from terrorism, coercion, interrogation or capture of Agency personnel by hostile nations and/or terrorist groups, the Agency has established certain policies and procedures concerning unofficial foreign travel.

All Agency personnel (civilian employees, military assignees, and contractors) who are planning unofficial foreign travel must have that travel approved by submitting a proposed itinerary to the Security Awareness Division (M56) at least 30 working days prior to their planned departure from the United States. Your itinerary should be submitted on Form K2579 (Unofficial Foreign Travel Request). This form provides space for noting the countries to be visited, mode of travel, and dates of departure and return. Your immediate supervisor must sign this form to indicate whether or not your proposed travel poses a risk to the sensitive information, activities, or projects of which you may have knowledge due to your current assignment.

After your supervisor's assessment is made, this form should be forwarded to the Security Awareness Director (M56). Your itinerary will then be reviewed in light of the existing situation in the country or countries to be visited, and a decision for approval or disapproval will be based on this assessment. The purpose of this policy is to limit the risk of travel to areas of the world where a threat may exist to you and to your knowledge of classified Agency activities.

In this context, travel to communist-controlled and other hazardous activity areas is prohibited. A listing of these hazardous activity areas is prohibited. A listing of these hazardous activity areas can be found in Annex A of NSA/CSS Regulation No. 30-31, "Security Requirements for Foreign Travel" (12 June 1987). From time to time, travel may also be prohibited to certain areas where the threat from hostile intelligence services, terrorism, criminal activity or insurgency poses an unacceptable risk to Agency employees and to the sensitive information they possess. Advance travel deposits made without prior agency approval of the proposed travel may result in financial losses by the employee should the travel be disapproved, so it is important to obtain approval prior to committing yourself financially. Questions regarding which areas of the world currently pose a threat should be directed to the Security Awareness Division (M56).

Unofficial foreign travel to Canada, the Bahamas, Bermuda, and Mexico does not require prior approval, however, this travel must still be reported using Form K2579. Travel to these areas may be reported after the fact.

While you do not have to report your foreign travel once you have ended your affiliation with the Agency, you should be aware that the risk incurred in travelling to certain areas, from a personal safety and/or counterintelligence standpoint, remains high. The requirement to protect the classified information to which you have had access is a lifetime obligation.

MEMBERSHIP IN ORGANIZATIONS

Within the United States there are numerous organizations with memberships ranging from a few to tens of thousands. While you may certainly participate in the activities of any reputable organization, membership in any international club or professional organization/activity with foreign members should be reported through your Staff

Security Officer to the Clearance Division (M55). In most cases there are no security concerns or threats to our employees or affiliates. However, the Office of Security needs the opportunity to research the organization and to assess any possible risk to you and the information to which you have access.

In addition to exercising prudence in your choice of organizational affiliations, you should endeavor to avoid participation in public activities of a conspicuously controversial nature because such activities could focus undesirable attention upon you and the Agency. NSA employees may, however, participate in bona fide public affairs such as local politics, so long as such activities do not violate the provisions of the statutes and regulations which govern the political activities of all federal employees. Additional information may be obtained from your Personnel Representative.

CHANGES IN MARITAL STATUS/COHABITATION/NAMES

All personnel, either employed by or assigned to NSA, must advise the Office of Security of any changes in their marital status (either marriage or divorce), cohabitation arrangements, or legal name changes. Such changes should be reported by completing NSA Form G1982 (Report of Marriage / Marital Status Change / Name Change), and following the instructions printed on the form.

USE AND ABUSE OF DRUGS

It is the policy of the National Security Agency to prevent and eliminate the improper use of drugs by Agency employees and other personnel associated with the Agency. The term "drugs" includes all controlled drugs or substances identified and listed in the Controlled Substances Act of 1970, as amended, which includes but is not limited to: narcotics, depressants, stimulants, cocaine, hallucinogens ad cannabis (marijuana, hashish, and hashish oil). The use of illegal drugs or the abuse of prescription drugs by persons employed by, assigned or detailed to the Agency may adversely affect the national security; may have a serious damaging effect on the safety and the safety of others; and may lead to criminal prosecution. Such use of drugs either within or outside Agency controlled facilities is prohibited.

PHYSICAL SECURITY POLICIES

The physical security program at NSA provides protection for classified material and operations and ensures that only persons authorized access to the Agency's spaces and classified material are permitted such access. This program is concerned not only with the Agency's physical plant and facilities, but also with the internal and external procedures for safeguarding the Agency's classified material and activities. Therefore, physical security safeguards include Security Protective Officers, fences, concrete barriers, access control points, identification badges, safes, and the compartmentalization of physical spaces. While any one of these safeguards represents only a delay factor against attempts to gain unauthorized access to NSA spaces and material, the total combination of all these safeguards represents a formidable barrier against physical penetration of NSA. Working together with personnel security policies, they provide "security in depth."

The physical security program depends on interlocking procedures. The responsibility for carrying out many of these procedures rests with the individual. This means you, and every person employed by, assign, or detailed to the Agency, must assume the responsibility for protecting classified material. Included in your responsibilities are: challenging visitors in operational areas; determining "need-to-know;" limiting classified conversations to approved areas; following established locking and checking procedures; properly using the secure and non-secure telephone systems; correctly wrapping and packaging classified data for transmittal; and placing classified waste in burn bags.

THE NSA BADGE

Even before you enter an NSA facility, you have a constant reminder of security—the NSA badge. Every person who enters an NSA installation is required to wear an authorized badge. To enter most NSA facilities your badge must be inserted into an Access Control Terminal at a building entrance and you must enter your Personal Identification Number (PIN) on the terminal keyboard. In the absence of an Access Control Terminal, or when passing an internal security checkpoint, the badge should be held up for viewing by a Security Protective Officer. The badge must be displayed at all times while the individual remains within any NSA installation.

NSA Badges must be clipped to a beaded neck chain. If necessary for the safety of those working in the area of electrical equipment or machinery, rubber tubing may be used to insulate the badge chain. For those Agency personnel working in proximity to other machinery or equipment, the clip may be used to attach the badge to the wearer's clothing, but it must also remain attached to the chain.

After you leave an NSA installation, remove your badge from public view, thus avoiding publicizing your NSA affiliation. Your badge should be kept in a safe place which is convenient enough to ensure that you will be reminded to bring it with you to work. A good rule of thumb is to afford your badge the same protection you give your wallet or your credit cards. DO NOT write your Personal Identification Number on your badge.

If you plan to be away from the Agency for a period of more than 30 days, your badge should be left at the main Visitor Control Center which services your facility.

Should you lose your badge, you must report the facts and circumstances immediately to the Security Operations Center (SOC) (963-3371s/688-6911b) so that your badge PIN can be deactivated in the Access Control Terminals. In the event that you forget your badge when reporting for duty, you may obtain a "non-retention" Temporary Badge at the main Visitor Control Center which serves your facility after a co-worker personally identifies your and your clearance has been verified.

Your badge is to be used as identification only within NSA facilities or other government installations where the NSA badge is recognized. Your badge should never be used outside of the NSA or other government facilities for the purpose of personal identification. You should obtain a Department of Defense identification card from the Civilian Welfare Fund (CWF) if you need to identify yourself as a government employee when applying for "government discounts" offered at various commercial establishments.

Your badge color indicates your particular affiliation with NSA and your level of clearance. Listed below are explanations of the badge colors you are most likely to see:

Green (*) Fully cleared NSA employees and certain military assignees.

Orange (*) (or Gold) Fully cleared representative of other government agencies.

Black (*) Fully cleared contractors or consultants.

Blue Employees who are cleared to the SECRET level while awaiting completion of their processing for full (TS/SI) clearance. These Limited Interim Clearance (LIC) employees are restricted to certain activities while inside a secure area.

Red Clearance level is not specified, so assume the holder is uncleared.

* - Fully cleared status means that the person has been cleared to the Top Secret (TS) level and indoctrinated for Special Intelligence (SI).

All badges with solid color backgrounds (permanent badges) are kept by individuals until their NSA employment or assignment ends. Striped badges ("non-retention" badges) are generally issued to visitors and are returned to the Security Protective Officer upon departure from an NSA facility.

AREA CONTROL

Within NSA installations there are generally two types of areas, Administrative and Secure. An Administrative Area is one in which storage of classified information is not authorized, and in which discussions of a classified nature are forbidden. This type of area would include the corridors, restrooms, cafeterias, visitor control areas, credit union, barber shop, and drugstore. Since uncleared, non-NSA personnel are often present in these areas, all Agency personnel must ensure that no classified information is discussed in an Administrative Area.

Classified information being transported within Agency facilities must be placed within envelopes, folders, briefcases, etc. to ensure that its contents or classification markings are not disclosed to unauthorized persons, or that materials are not inadvertently dropped enroute.

The normal operational work spaces within an NSA facility are designated Secure Areas. These areas are approved for classified discussions and for the storage of classified material. Escorts must be provided if it is necessary for uncleared personnel (repairmen, etc.) to enter Secure Areas, an all personnel within the areas must be made aware of the presence of uncleared individuals. All unknown, unescorted visitors to Secure Areas should be immediately challenged by the personnel within the area, regardless of the visitors' clearance level (as indicated by their badge color).

The corridor doors of these areas must be locked with a deadbolt and all classified information in the area must be properly secured after normal working hours or whenever the area is unoccupied. When storing classified material, the most sensitive material must be stored in the most secure containers. Deadbolt keys for doors to these areas must be returned to the key desk at the end of the workday.

For further information regarding Secure Areas, consult the Physical Security Division (M51) or your staff Security Officer.

ITEMS TREATED AS CLASSIFIED

For purposes of transportation, storage and destruction, there are certain types of items which must be treated as classified even though they may not contain classified information. Such items include carbon paper, vu-graphs, punched machine processing cards, punched paper tape, magnetic tape, computer floppy disks, film, and used typewriter ribbons. This special treatment is necessary since a visual examination does not readily reveal whether the items contain classified information.

PROHIBITED ITEMS

Because of the potential security or safety hazards, certain items are prohibited under normal circumstances from being brought into or removed from any NSA installation. These items have been groped into two general classes. Class I prohibited items are those which constitute a threat to the safety and security of NSA/CSS personnel and facilities. Items in this category include:

a. Firearms and ammunition
b. Explosives, incendiary substances, radioactive materials, highly volatile materials, or other hazardous materials
c. Contraband or other illegal substances
d. Personally owned photographic or electronic equipment including microcomputers, reproduction or recording devices, televisions or radios.

Prescribed electronic medical equipment is normally not prohibited, but requires coordination with the Physical Security Division (M51) prior to being brought into any NSA building.

Class II prohibited items are those owned by the government or contractors which constitute a threat to physical, technical, or TEMPEST security. Approval by designated organizational officials is required before these items can be brought into or removed from NSA facilities. Examples are:

a. Transmitting and receiving equipment
b. Recording equipment and media
c. Telephone equipment and attachments
d. Computing devices and terminals
e. Photographic equipment and film

A more detailed listing of examples of Prohibited Items may be obtained from your Staff Security Officer or the Physical Security Division (M51).

Additionally, you may realize that other seemingly innocuous items are also restricted and should not be brought into any NSA facility. Some of these items pose a technical threat; others must be treated as restricted since a visual inspection does not readily reveal whether they are classified. These items include:

a. Negatives from processed film; slides; vu-graphs
b. Magnetic media such as floppy disks, cassette tapes, and VCR videotapes
c. Remote control devices for telephone answering machines
d. Pagers

EXIT INSPECTION

As you depart NSA facilities, you will note another physical security safeguard—the inspection of the materials you are carrying. This inspection of your materials, conducted by Security Protective Officers, is designed to preclude the inadvertent removal of classified material. It is limited to any articles that you are carrying out of the facility and may include letters, briefcases, newspapers, notebooks, magazines, gym

bags, and other such items. Although this practice may involve some inconvenience, it is conducted in your best interest, as well as being a sound security practice. The inconvenience can be considerably reduced if you keep to a minimum the number of personal articles that you remove from the Agency.

REMOVAL OF MATERIAL FROM NSA SPACES

The Agency maintains strict controls regarding the removal of material from its installations, particularly in the case of classified material.

Only under a very limited and official circumstances classified material be removed from Agency spaces. When deemed necessary, specific authorization is required to permit an individual to hand carry classified material out of an NSA building to another Secure Area. Depending on the material and circumstances involved, there are several ways to accomplish this.

A Courier Badge authorizes the wearer, for official purposes, to transport classified material, magnetic media, or Class II prohibited items between NSA facilities. These badges, which are strictly controlled, are made available by the Physical Security Division (M51) only to those offices which have specific requirements justifying their use.

An Annual Security Pass may be issued to individuals whose official duties require that they transport printed classified materials, information storage media, or Class II prohibited items to secure locations within the local area. Materials carried by an individual who displays this pass are subject to spot inspection by Security Protective Officers or other personnel from the Office of Security. It is not permissible to use an Annual Security Pass for personal convenience to circumvent inspection of your personal property by perimeter Security Protective Officers.

If you do not have access to a Courier Badge and you have not been issued an Annual Security Pass, you may obtain a One-Time Security Pass to remove classified materials / magnetic media or admit or remove prohibited items from an NSA installation. These passes may be obtained from designated personnel in your work element who have been given authority to issue them. The issuing official must also contact the Security Operations Center (SOC) to obtain approval for the admission or removal of a Class I prohibited item.

When there is an official need to remove government property which is not magnetic media, or a prohibited or classified item, a One-Time Property Pass is used. This type of pass (which is not a Security Pass) may be obtained from your element custodial property officer. A Property Pass is also to be used when an individual is removing personal property which might be reasonably be mistaken for unclassified Government property. This pass is surrendered to the Security Protective Officer at the post where the material is being removed. Use of this pass does not preclude inspection of the item at the perimeter control point by the Security Protective Officer or Security professionals to ensure that the pass is being used correctly.

 EXTERNAL PROTECTION OF CLASSIFIED INFORMATION

On those occasions when an individual must personally transport classified material between locations outside of NSA facilities, the individual who is acting as the courier must ensure that the material receives adequate protection. Protective measures must include double wrapping and packaging of classified information, keeping the material under constant control, ensuring the presence of a second appropriately cleared person when necessary, and delivering the material to authorized persons only. If you are designated as a courier outside the local area, contact the Security Awareness Division (M56) for your courier briefing.

Even more basic than these procedures is the individual security responsibility to confine classified conversations to secure areas. Your home, car pool, and public places are not authorized areas to conduct classified discussions—even if everyone involved in he discussion possesses a proper clearance and "need-to-know." The possibility that a conversation could be overheard by unauthorized persons dictates the need to guard against classified discussions in non-secure areas.

Classified information acquired during the course of your career or assignment to NSA may not be mentioned directly, indirectly, or by suggestion in personal diaries, records, or memoirs.

REPORTING LOSS OR DISCLOSURE OF CLASSIFIED INFORMATION

The extraordinary sensitivity of the NSA mission requires the prompt reporting of any known, suspected, or possible unauthorized disclosure of classified information, or the discovery that classified information may be lost, or is not being afforded proper protection. Any information coming to your attention concerning the loss or unauthorized disclosure of classified information should be reported immediately to your supervisor, your Staff Security Officer, or the Security Operations Center (SOC).

USE OF SECURE AND NON-SECURE TELEPHONES

Two separate telephone systems have been installed in NSA facilities for use in the conduct of official Agency business: the secure telephone system (gray telephone) and the outside, non-secure telephone system (black telephone). All NSA personnel must ensure that use of either telephone system does not jeopardize the security of classified information.

The secure telephone system is authorized for discussion of classified information. Personnel receiving calls on the secure telephone may assume that the caller is authorized to use the system. However, you must ensure that the caller has a "need-to-know" the information you will be discussing.

The outside telephone system is only authorized for unclassified official Agency business calls. The discussion of classified information is not permitted on this system. Do not attempt to use "double-talk" in order to discuss classified information over the non-secure telephone system.

In order to guard against the inadvertent transmission of classified information over a non-secure telephone, and individual using the black telephone in an area where classified activities are being conducted must caution other personnel in the area that the non-secure telephone is in use. Likewise, you should avoid using the non-secure telephone in the vicinity of a secure telephone which is also in use.

HELPFUL INFORMATION

SECURITY RESOURCES

In the fulfillment of your security responsibilities, you should be aware that there are many resources available to assist you. If you have any questions or concerns regarding security at NSA or your individual security responsibilities, your supervisor should be consulted. Additionally, Staff Security Officers are appointed to the designated Agency elements to assist these organizations in carrying out their security responsibilities. There is a Staff Security Officer assigned to each organization; their phone numbers are listed at the back of this handbook. Staff Security Officers also provide guidance to and monitor the activities of Security Coordinators and Advisors (individuals who, in addition to their operational duties within their respective elements, assist element supervisors or managers in discharging security responsibilities).

Within the Office of Security, the Physical Security Division (M51) will offer you assistance in matters such as access control, security passes, clearance verification, combination locks, keys, identification badges, technical security, and the Security Protective Force. The Security Awareness Division (M56) provides security guidance and briefings regarding unofficial foreign travel, couriers, special access, TDY / PCS, and amateur radio activities. The Industrial and Field Security Division (M52) is available to provide security guidance concerning NSA contractor and field site matters.

The Security Operations Center (SOC) is operated by two Security Duty Officers (SDOs), 24 hours a day, 7 days a week. The SDO, representing the Office of Security, provides a complete range of security services to include direct communications with fire and rescue personnel for all Agency area facilities. The SDO is available to handle any physical or personnel problems that may arise, and if necessary, can direct your to the appropriate security office that can assist you. After normal business hours, weekends, and holidays, the SOC is the focal point for all security matters for all Agency personnel and facilities (to include Agency field sites and contractors). The SOC is located in Room 2A0120, OPS 2A building and the phone numbers are 688-6911(b), 963-3371(s).

However, keep in mind that you may contact any individual or any division within the Office of Security directly. Do not hesitate to report any information which may affect the security of the Agency's mission, information, facilities or personnel.

SECURITY-RELATED SERVICES

In addition to Office of Security resources, there are a number of professional, security-related services available for assistance in answering your questions or providing the services which you require.

The Installations and Logistics Organization (L) maintains the system for the collection and destruction of classified waste, and is also responsible for the movement and scheduling of material via NSA couriers and the Defense Courier Service (DCS). Additionally, L monitors the proper addressing, marking, and packaging of classified material being transmitted outside of NSA; maintains records pertaining to receipt and transmission of controlled mail; and issues property passes for the removal of unclassified property.

The NSA Office of Medical Services (M7) has a staff of physicians, clinical psychologists and an alcoholism counselor. All are well trained to help individuals help themselves in dealing with their problems. Counseling services, with referrals to private mental health professionals when appropriate, are all available to NSA personnel. Appointments can be obtained by contacting M7 directly. When an individual refers himself/herself, the information discussed in the counseling sessions is regarded as privileged medical information and is retained exclusively in M7 unless it pertains to the national security.

Counselling interviews are conducted by the Office of Civilian Personnel (M3) with any civilian employee regarding both on and off-the-job problems. M3 is also available to assist all personnel with the personal problems seriously affecting themselves or members of their families. In cases of serious physical or emotional illness, injury, hospitalization, or other personal emergencies, M3 informs concerned Agency elements and maintains liaison with family members in order to provide possible assistance. Similar counselling services are available to military assignees through Military Personnel (M2).

GUIDE TO SECURITY

M51 PHYSICAL SECURITY 963-6651s/688-8293b (FMHQ)

968-8101s/859-6411b (FANX)

CONFIRM and badges
(963-6611s/688-7411b)

Prohibited Items

Locks, keys, safes and alarms
Security/vehicle passes
Visitor Control
Inspections
Red/blue seal areas
Pass Clearances (963-4780s/688-6759b)

SOC (963-3371s/688-6911b)

NSA facility protection and compliance

New Construction

M52 INDUSTRIAL AND FIELD SECURITY

982-7918s / 859-6255b

Security at contractor field site facilities

Verification of classified mailing addresses for contractor facilities

M53 INVESTIGATIONS 982-7914S/859-6464B

Personnel Interview Program (PIP)
Military Interview Program (MIP)
Reinvestigations
Special investigations

M54 COUNTERINTELLIGENCE 982-7832s / 859-6424b

Security counterintelligence analysis
Security compromises

M55 CLEARANCES 982-7900s / 859-4747b

Privacy Act Officer (For review of security files)
Contractor / applicant processing
Continued SCI access
Military access

M56 SECURITY AWARENESS 963-3273S/688-6535B

Security indoctrinations / debriefings
Associations with foreign nationals
Security Week
Security posters, brochures, etc.
Embassy visits
Briefings (foreign travel, ham radio, courier, LIC, PCS, TDY, special access, etc.)
Foreign travel approval
Military contractor orientation
Special Access Office (963-5466s / 688-6353b)

M57 POLYGRAPH 982-7844s / 859-6363b

Polygraph interviews

M509 MANAGEMENT AND POLICY STAFF 982-7885s / 859-6350b

STAFF SECURITY OFFICERS (SSOs)

Element	Room	Secure / Non-Secure
A	2A0852B	963-4650 / 688-7044
B	3W099	963-4559 / 688-7141
D / Q / J / N / U	2B8066G	963-4496 / 688-6614
E / M	D3B17	968-8050 / 859-6669
G	9A195	963-5033 / 688-7902
K	2B5136	963-1978 / 688-5052
L	SAB4	977-7230 / 688-6194
P	2W091	963-5302 / 688-7303
R	B6B710	968-4073 / 859-4736
S / V / Y / C / X	C2A55	972-2144 / 688-7549
T	2B5040	963-4543 / 688-7364
W	1C181	963-5970 / 688-7061

GUIDE TO SECURITY-RELATED SERVICES

Agency Anonymity	968-8251 / 859-4381
Alcohol Rehabilitation Program	963-5420 / 688-7312
Cipher Lock Repair	963-1221 / 688-7119
Courier Schedules (local)	977-7197 / 688-7403
Defense Courier Service	977-7117 / 688-7826
Disposal of Classified Waste	
· Paper only	972-2150 / 688-6593
· Plastics, Metal, Film, etc	963-4103 / 688-7062
Locksmith	963-3585 / 688-7233
Mail Dissemination and Packaging	977-7117 / 688-7826
Medical Center (Fort Meade)	963-5429 / 688-7263
(FANX)	968-8960 / 859-6667
(Airport Square)	982-7800 / 859-6155
NSA / CSS Information Policy Division	963-5825 / 688-6527
Personnel Assistance	
· Civilian	982-7835 / 859-6577
· Air Force	963-3239 / 688-7980
· Army	963-3739 / 688-6393
· Navy	963-3439 / 688-7325
Property Passes (unclassified material)	977-7263 / 688-7800
Psychological Services	963-5429 / 688-7311

FREQUENTLY USED ACRONYMS/DESIGNATORS

ARFCOS	Armed Forces Courier Service (now known as DCS)
AWOL	Absent Without Leave
CAO	Classification Advisory Officer
COB	Close of Business
CWF	Civilian Welfare Fund
DCS	Defense Courier Service (formerly known as ARFCOS)
DoD	Department of Defense
EOD	Enter on Duty
FOUO	For Official Use Only
M2	Office of Military Personnel
M3	Office of Civilian Personnel
M5	Office of Security
M7	Office of Medical Services
NCS	National Cryptologic School
PCS	Permanent Change of Station
PIN	Personal Identification Number
Q43	Information Policy Division
SDO	Security Duty Officer
SOC	Security Operations Center
SPO	Security Protective Officer
SSO	Staff Security Officer

TDY	Temporary Duty
UFT	Unofficial Foreign Travel

A FINAL NOTE

The information you have just read is designed to serve as a guide to assist you in the conduct of your security responsibilities. However, it by no means describes the extent of your obligation to protect information vital to the defense of our nation. Your knowledge of specific security regulations is part of a continuing process of education and experience. This handbook is designed to provide the foundation of this knowledge and serve as a guide to the development of an attitude of security awareness.

In the final analysis, security is an individual responsibility. As a participant in the activities of the National Security Agency organization, you are urged to be always mindful of the importance of the work being accomplished by NSA and of the unique sensitivity of the Agency's operations.