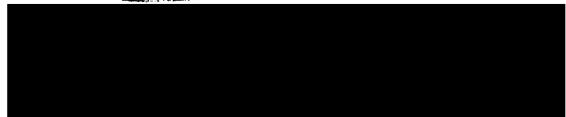


~~CONFIDENTIAL~~

3154

UNITED STATES GOVERNMENT



WAR DEPARTMENT

25X1A9a

STRATEGIC SERVICES UNIT

SECURITY REGULATIONS

PART ONE

| | | | | | |
|------------|-----|----------|----------|-----------|---------|
| DOC | 2 | REV DATE | 7 MAY 80 | BY | 025251 |
| ORIG COMP | 777 | OPI | 31 | TYPE | 11 |
| ORIG CLASS | C | PAGES | 9 | REV CLASS | C |
| JUST | 22 | NEXT REV | 2010 | AUTH: | HR 10-2 |

April 25, 1946

~~CONFIDENTIAL~~

SECURITY REGULATIONS - Part One

SECURITY is defined as "freedom from exposure to danger". It is essential to the conduct of any Intelligence Organization. It must be maintained and protected continuously, for when it is once lost it is lost forever. SECURITY is not a condition that can exist partially--it must be complete.

SECURITY is easily lost. Any employee of Strategic Services Unit, is in a position to and can become responsible for jeopardizing the value of the enormous amount of study and energy that has been spent and will be spent collectively by the members of the Unit. Any employee may open the door through which vital information may fall into the hands of foreign powers. Any employee may endanger the operations and the lives of members of this Unit who are in the field.

The American people have rarely been made conscious of the need for SECURITY. Danger is unknown to most of us in the sense of the word that it is known to the people of Europe and Asia. We have had so much personal liberty that we have taken it for granted and many Americans did not recognize the threats to personal liberty from Germany and Japan until the whole world became insecure. That situation has been rectified but it now becomes even more imperative that we be at all times security conscious. We knew who our enemies were during the war, we do not now. We must assume that there are some fifty-two "possible" enemies seeking to penetrate us for vital information. Self-discipline is the essential element of success in the field of intelligence. Anyone of the people who are employed by this intelligence organization will jeopardize its success unless he or she learns the true meaning of self-discipline. The men and women who constitute SSU personnel must not prove themselves inadequate.

Over a great many years the Army and the Navy have developed certain

25X1A9a

June 4-1946

These rules are stringent. Disobedience receives severe punishment. The Security Division, SSU, has drawn freely upon the long experience of the Armed Services in formulating this set of regulations which are easy and simple to follow. Every staff member must find the desire and character to obey these regulations. If you do not understand the need for never breaking any SECURITY regulation, it is because your understanding of the nature of the work of SSU and of Security is limited.

Real SECURITY can result only from the continuously sustained efforts of each individual. Security enforcement by the Security Office and by guards can never bring to the unit any fraction of the SECURITY which can be established by a constantly thoughtful, cooperative and conscientious security attitude on the part of each employee.

SECURITY REGULATIONS

1. Personal Security is simply a matter of habit; the habit of discretion and care which has become second nature through constant usage. Insecurity is therefore plain carelessness. A considered indiscretion would be treachery, not insecurity. It is the responsibility of each individual to train himself in security and secure procedures.

The most secure person is the one who does not seek or want to know anything which does not concern the performance of his own duties. This is not easy, because the most important classified items naturally cause the most curiosity. "What you don't know won't hurt you" nor will it hurt the work of SSU. If you do know something which actually happens to be none of your business, it becomes a burden to you and an additional possibility of danger to others.

The habit of Security must be thorough in all circumstances. When foreign powers are trying to obtain valuable information, it is certain that they will do it in the most insidious fashion so that you will least suspect

25X1A9a

11-11-46

1. Therefore, it is given personal care in every day routine and conversation, where danger is least apparent that makes for the greatest security.

2. The first rule of personal Security is obvious. Nothing that is learned within the office should be discussed outside the office. That is to say, discuss business within official SSU office space only. Your greatest efforts to speak softly when conversing with another member of SSU, either directly or by implication, regarding classified material in public places such as cafeterias, busses, trolleys, or taxicabs, can never justify the security risk involved. No one can presume to judge what part of his knowledge is important or secret; it is the small bits of seemingly harmless information that can be pieced together which are of value to foreign powers. Do not be led into a discussion of your work or of the personalities of other individuals in the organization. Let your friends and acquaintances consider you a bore on such subjects; let them think that your work is not important. Personal vanity has no place in such serious work of this nature.

25X1A9a

3. Nothing should be done to arouse the curiosity of other people regarding your own work or the work of our organization. If asked what type of work the Unit does, you may use the statement that the work is "the preparation of war records for the War Department". If asked what you do, select the kind of answer that will discourage curiosity such as "filing", "analysis", "stenographic work", or "statistics", whichever fits your level of employment.

4. The habit of Security must be carried out even on the premises. Casual discussions of office subjects with other members must be wholly discouraged. Your work and the plans of your branch should be discussed only with those who have a real part in them.

5. Security in Office Routine. Since Security is a matter of habit, the office must be run upon a set routine which will insure Security. The most important elements are:

June 4/1946

(A) Telephone. The presumption must be that every telephone conversation is being overheard by unauthorized persons. Top secret, secret and confidential material should never be discussed on the telephone. No telephone wires can be thoroughly protected, not even those carrying interoffice calls.

Telephone Conversations should be so guarded in tone, as to eliminate the possibility of being overheard by unauthorized persons who may be within the immediate area. In answering the telephone merely say "Extension 123" and let the caller identify himself. If the caller asks for someone not on your extension, answer, "I'm sorry you have the wrong number", and hang up--do NOT identify who may be reached by your extension. If the person being called is out of town answer by saying, "I'm sorry but he is out of the office" or "He has gone for the day." Do NOT furnish information to anyone calling as to the whereabouts of the Subject being called. When in doubt as to the identity of a caller or the propriety of his questions, return the call for verification--always be certain with whom you are talking.

(B) Documents. The safekeeping of documents classified "top secret", "secret", and "confidential" is of prime importance. Only a locked safe will provide Security, and classified documents (including secretarial notes, carbons, and stencils which contain confidential and secret matter) are not to be put in locked desks, locked filing cabinets or any other substitute. Classified documents must never be left unattended except in a locked safe or safe type filing cabinet. Naturally no classified material may ever be taken home at night. Night work should be done in the office where this material can be fully protected.

Never let the papers on which you are working be read by an unauthorized person. The habit of turning them face down on your desk is a good one.

7/10/61 19/116

scrap, which will be picked up and safeguarded [REDACTED]

25X1A

Rooms must not be left empty at any time during the working day. If such a situation is unavoidable, lock up all classified material in your safe.

(C) Other Classified Material. Remember that documents are not the only form of vital information. Cables, telegrams and mail are often classified because of their contents. Realize, however, that the names and addresses of both sender and receiver may be equally important to conceal. Cameras may carry films and films may convey secret information. Maps, charts, books, dictaphone records, etc. are often secret or confidential. Radios and other equipment may be secret in nature; all should be safeguarded in the office and in transit with the same zealous care given to documents.

(D) Transmittal of all Classified Material. Regulations have been laid down to maintain the SECURITY of classified material when it leaves your office for any destination, whether another office, another building, or another city. When in doubt consult those in authority in your Branch.

It is the definite responsibility of each Branch to control the movement of all types of classified material in conformity with the best security practices. The essential points in safeguarding classified material are:

- (a) To maintain as a secret both its existence and the information it contains.
- (b) To make certain that it is handled only by official couriers, or members authorized to handle it and accustomed to that type of responsibility.
- (c) When it becomes unfeasible for such members to handle classified material, to use only the most secure authorized alternatives in the form of registered mail, etc.
- (d) To make certain that all mail and packages containing classified

material which are being sent to [REDACTED]

25X1A9a

ime 4/25 1946

secret, are so dispatched as to maintain that secrecy.

(e) To maintain those records covering the sending and receipt of each piece of classified material so that responsibility for its possession and safeguarding may be clearly understood by all at all times.

(E) Combinations to Safes should be carried in the head and not on paper. Combinations are revealed to authorized subordinates by the person in charge of the office and definite responsibility for locking each safe at the end of the day is lodged with a particular custodian and alternate whose names and addresses are on file at the Security Office. These custodians are responsible for the safe and for the actions of the persons to whom they may delegate responsibility for closing and opening it. If a safe is reported insecure at any time or if classified material is found exposed in a room, it is the responsibility of the custodian to return to the office at once and conduct an "on the spot" investigation immediately and to cooperate with the Security Office in remedying the violation regardless of the time of day or night at which the violation is discovered. To assist in protecting the contents of safes always notify the Security Office immediately when a safe is moved or its custodianship is changed. All combinations should be changed reasonably often and for any good reason such as personnel shifts. On request, the Security Division will change combinations.

6. Building Security. It is imperative that all unauthorized persons be kept out of the buildings.

(A) Identification credentials. Members of this organization are identified by their credentials. It is obviously most important that your credential should not fall into improper hands. Never allow anyone else to use your credential. Do not print or write your name or anything else on your identification credential. Exhibit it properly to the guard upon entering and departing from any SSU building. Exhibit it so that the guard can see it. Keep

25X1A9a

June 4th 1946

it concealed at all times outside SSU Buildings. This is for your protection and to insure a safe identification system. Surrender your badge to the Security Division or building guard for safe-keeping if you are to be away from your office for an extended period of time and/or before leaving the city. Your credential may be recovered on your return by visiting the Security Division.

(B) Visitors having official business to transact at SSU may enter SSU buildings only by obtaining a visitor's card. A visitor should never be left alone in an SSU office.

(C) Identification in the Office. Always assure yourself of the identity of the person with whom you are talking. Any visitor in an office should have identification which he can exhibit. If such is lacking or does not satisfy, call the Security Division.

(D) The Guards are under instructions to enforce Security Regulations with firmness and courtesy. These guards are in uniform and are doing their duty. As our first line of defense their standards must be kept high for the benefit of our organization and all its employees. You can assist greatly by informing the Security Division whenever any guard is not sufficiently strict or alert. Do not complain to the Security Division if when you break a rule you intend to divert the issue by a discussion of the manner in which the guard asked you to do your duty.

(E) Both building and office security are jeopardized by open or unlocked windows after office hours, or by failure to follow any of the other common sense rules that spell good secure housekeeping.

7. No individual shall be admitted to SSU buildings for the purpose of performance of duty until he or she has been given full Security Approval by the Security Division.

8. Security Regulations. The Security Division issues regulations, instructions and directions from time to time. Obey the spirit of

25X1A9a

11,111,111 17th 1946

Many of them cover in detail subjects merely mentioned herein. If confronted with a Security problem, consult your superior or in his absence communicate with your Branch Chief or the Security Division.

25X1A9a

11 NOV 1946