



DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
BUMEDINST 5510.7C
BUMED-M09B13
JUN 03 2015

BUMED INSTRUCTION 5510.7C

From: Chief, Bureau of Medicine and Surgery

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAMS

Ref: (a) SECNAVINST 5510.30B
(b) SECNAV M-5510.30
(c) SECNAVINST 5510.36A
(d) SECNAV M-5510.36
(e) Navy Telecommunications Directive 11-08
(f) Homeland Security Presidential Directive-12 (NOTAL)
(g) BUMED Memo 6000 Ser M09B/10UM0934000031 of 11 Mar 10

Encl: (1) Acronyms

1. Purpose. To establish policy and procedures for implementing the Information and Personnel Security Programs (ISP and PSP) at the Bureau of Medicine and Surgery (BUMED) Headquarters (HQ), per references (a) through (g). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. BUMEDINST 5510.7B.

3. Scope. This instruction applies to all BUMED HQ personnel (active duty, reservist, civilian, and contract staff) and Detachments.

4. Objectives

a. Clarify position sensitivity requirements, background investigation requirements, and national security responsibilities for all BUMED HQ employees.

b. Mitigate risk of security related incidents, compromises, and violations by establishing BUMED HQ specific procedures for the protection of classified material against loss, theft, compromise, espionage, or sabotage.

5. Definitions

a. Case Adjudication Tracking System (CATS) is an information

JUN 03 2015

technology system created for investigative and adjudicative case management. CATS is integrated into the Defense Information Security System enterprise architecture which will eventually replace the Joint Personnel Adjudication System (JPAS).

b. Department of Defense Central Adjudication Facility (DODCAF). DODCAF is responsible for determining who within the Department of Defense (DoD) is eligible to hold a security clearance, to have access to Sensitive Compartmentalized Information (SCI), or to be assigned to sensitive duties.

c. Defense Industrial Security Clearance Office (DISCO). DISCO makes personnel security eligibility determinations for individuals in private industry (contractors) who need access to classified information in order to perform their jobs and respond to requests for information regarding contractor personnel security clearance applications.

d. National Security Information (NSI). Any information that has been determined pursuant to Executive Order 12958, as amended, or any predecessor order to require protection against its disclosure and is so designated. The designations TOP SECRET, SECRET, and CONFIDENTIAL are used to identify such information and are usually referred to as "classified information."

e. Sensitive Duties. Duties in which an assigned military or civilian employee could bring about, by virtue of the nature of their duties, a materially adverse affect on national security. Any duties requiring access to classified information are sensitive duties.

f. Sensitive Information. Any information where the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or conduct of Federal programs, or the privacy which individuals are entitled to under Title 5, U.S.C. §552a (Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine payroll, finance, logistics, inventory, and personnel management systems. Examples include For Official Use Only (FOUO), unclassified technical data, State Sensitive but Unclassified, foreign government information, personally identifiable information, and protected health information.

g. Sensitive Position. Any position so designated, in which the occupant could bring about by virtue of the nature of their duties, a materially adverse affect on national security. All civilian positions within DoD are designated special-sensitive

JUN 03 2015

(SS), critical-sensitive (CS), noncritical-sensitive (NCS), or non-sensitive.

h. Special-Sensitive (SS). Any position which the head of the agency determines to be at a level higher than CS:

(1) Due to the greater degree of damage to the national security that an individual could effect by virtue of his or her position.

(2) Special requirements concerning the position under authority other than Executive Order 10450, such as designations applied under Special Security Officer cognizance pertaining to Director of Central Intelligence Directive 6/4.

(3) Designated Approval Authorities shall be designated as SS, due to the degree of damage an individual could effect by virtue of his or her position, including those information technology (IT) duties in which the incumbent has the responsibility for planning, direction and implementation of a major (Department of the Navy (DON)-wide or DoD-wide) IT security program; has responsibility for direction, planning, and design of a major (DON-wide or DoD-wide) computer system, including the hardware and software; or can access a major (DON-wide or DoD-wide) system during the operation or maintenance in such a way and with relatively high risk for causing inestimable damage or realizing extreme personal gain.

i. CS Position. Any position that includes:

(1) Access to TOP SECRET NSI.

(2) Development or approval of plans, policies, or programs which affect the overall operations of DON (e.g., policy making or policy determining positions).

(3) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(4) Investigative and certain investigative support duties, the issuance of personnel security clearances and access authorizations, or the making of personnel security determinations.

(5) Fiduciary, public contact or other duties demanding the highest degree of public trust.

(6) Any other position so designated by the Secretary of the Navy and/or his or her designee.

JUN 03 2015

j. NCS Position. Any position that includes:

(1) Access to SECRET or CONFIDENTIAL NSI.

(2) Assignment to duties involving the protection and safeguarding of DON personnel and property (e.g., security, police, provost marshal, duties associated with ammunition and explosives).

(3) Duties involving the education and orientation of DoD personnel.

(4) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DON personnel or property.

(5) Responsibility for financial operations subject to routine supervision or approval, but with no funds disbursement or transfer capabilities.

(6) Non-management DON mission support positions with authority for independent or semi-independent action.

(7) Duties involving delivery of service to support the DON mission requiring confidence or trust.

(8) Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems, system security and network defense systems, or the systems resources providing visual access and/or ability to input, delete, or otherwise manipulate sensitive information without controls to identify and deny sensitive information.

(9) Duties associated with or directly involving the accounting, disbursement, or authorizations for disbursement of funds in dollar amounts less than \$10 million per year; and/or duties that involve the development, writing or administration of, and/or awarding, approving, or modifying of contracts with total dollar amounts less than \$10 million dollars per year; or as deemed appropriate by the agency head those commensurate duties with potential for damage or personal gain.

(10) Other positions are designated by the agency head that involve a degree of access to a system that creates a potential for serious damage or personal gain less than that in CS positions.

k. IT Position. Any position in which the incumbent has access to a DON IT system(s) and/or performs IT-related duties with

JUN 03 2015

varying degrees of independence, privilege, and/or ability to access and/or impact sensitive data and information. There are three basic IT levels: Level I (IT-I: Privileged access), Level II (IT-II: Limited privilege, sensitive information access), and Level III (IT-III: No privilege, no sensitive information access).

l. Adjudication. The review and consideration of all available information to ensure an individual's loyalty, reliability, and trustworthiness are such that entrusting an individual with NSI or assigning an individual to sensitive duties is clearly in the best interest of national security. A determination that a person is an acceptable security risk equates to a determination of eligibility for access to classified information and/or sensitive duty assignment.

m. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, document, or communications security programs.

n. Electronic Questionnaires for Investigation Processing (e-QIP). Web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations for Federal security, suitability, fitness, and credentialing purposes. E-QIP allows the user to electronically enter update and transmit their personal investigation data over a secure internet connection to a requesting agency.

o. Defense Office of Hearings and Appeals (DOHA). Administers due process procedures for Industrial Security Program unfavorable personnel security determinations and provides hearings and appeals support to DoD military and civilian unfavorable personnel security determinations.

p. Personnel Security Appeals Board (PSAB). The PSAB is the appellate authority for appeals of unfavorable DODCAF eligibility determinations.

q. National Agency Check with Local Agency and Credit Checks (NACLIC). The NACLIC is the basic Executive Order 12968 standard for determinations of eligibility to access CONFIDENTIAL or SECRET classified NSI. The NACLIC also provides the basis for military suitability determinations for Navy and Marine Corps enlisted members, officers, and contractor staff. The NACLIC includes a National Agency Check (NAC), credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years, and checks of law

JUN 03 2015

enforcement agencies having jurisdiction where the subject has resided, been employed, or attended school within the last five years.

r. Access National Agency Check with Written Inquiries (ANACI). The ANACI is an Office of Personnel Management (OPM) product that meets the investigative requirements for appointment to NCS positions and for access to CONFIDENTIAL or SECRET NSI for Federal civilian employees. The ANACI includes a NAC, a credit check, and written inquiries covering the last five years to law enforcement agencies, to former employers and supervisors, to references, and to schools.

6. PSP. Applies to all regular and reserve military members of the Navy and Marine Corps; Federal civilians; personnel employed by, hired on a contractual basis by, or serving in an advisory/consultant capacity to the DON whether on a permanent, temporary, or part-time basis and whether or not compensated from appropriated or non-appropriated funds; and applicants selected for sensitive positions, or persons accepted for consideration for enlistment or appointment (military), or other persons covered by contract or legal agreement. Key components of the PSP include:

a. Personnel Security Investigations (PSI), access to NCS information, and associated security clearances will be initiated on all military personnel per Exhibit 6A of reference (b). BUMED HQ civilian personnel must submit to background investigations based on position sensitivity and IT requirements. All positions at BUMED HQ are considered, at minimum, to be NCS positions, requiring, at minimum, a final favorable background investigation based upon a NACLIC (military or contractors) or ANACI (civilians) investigation. These investigations are required to be periodically updated according to the level of the employee's position sensitivity. The PSI is initiated using the e-QIP Direct, and the requestor inputs his or her data using the e-QIP Program found on the OPM Web site at: <http://www.opm.gov/e-QIP>. For military, civilian personnel, or contractor personnel not requiring access to classified information, the BUMED HQ Security Manager will submit packages and supporting documentation (to include fingerprints) to OPM. Contractor personnel working at BUMED HQ must submit to background investigations based on contract sensitivity and IT requirements. If the contractor is required by contract to have access to classified information these PSIs are submitted through the BUMED HQ Security Manager with coordination from the Facility Security Officer (FSO) for submission to OPM. Investigations for contractors are adjudicated through DODCAF. The BUMED HQ Security Manager will verify that contractors have favorably adjudicated personnel to BUMED HQ prior to processing the contractor for network access.

JUN 03 2015

b. Access to SCI will only be considered for the established SCI billets at BUMED HQ. Personnel assigned to those billets, to include contractor personnel, must have the required background investigations as well as the eligibility for SCI granted by the Chief of Naval Operations Special Security Officer or DODCAF, as appropriate.

c. Credible questionable, derogatory, or unfavorable information must be reported to the BUMED HQ Security Manager as part of the continuous evaluation program. Any BUMED HQ employee is able to report said information on himself or herself or others within BUMED HQ who have been granted access to classified information or assigned to sensitive duties, to include IT positions.

(1) Credible, derogatory information must be forwarded to the DODCAF via CATS.

(2) The Chief of Staff (COS) may suspend local command access based on the derogatory information. The suspension may only be used as a temporary measure, and the employee must be notified in writing within 10 calendar days of the suspension. The employee must be removed from network access, access lists, and visit certifications; co-workers must be notified of the suspension; and combinations must be changed.

d. Notifications from the DODCAF, Navy Division will be processed by the BUMED HQ Security Manager within three working days. Statement of Reasons from the DODCAF, Navy Division with letters of intent (LOI) to revoke or deny access will be processed immediately per reference (b). The common access card (CAC) will be turned over to the BUMED HQ Security Manager upon final unfavorable determination; if civilian or contractor personnel are working under temporary access (interim network access), the CAC will be turned over to the BUMED HQ Security Manager upon receipt of the LOI. For contractor personnel whose PSI was initiated through the BUMED HQ Security Office the respective company FSO will immediately be notified upon the receipt for handling any LOI, revocation, or denial from DODCAF. For these contractor personnel, the CAC will be turned over to the BUMED HQ Security Manager, and the contractor employee will no longer work on the BUMED HQ compound, use government furnished equipment, or have access to BUMED HQ's network. Follow-up due process guidance must be provided to the military and civilian employees by the BUMED HQ Security Manager for appeals through the DOHA to the PSAB. Once a final revocation or denial decision has been made by the PSAB, the civilian employee, whose position by nature required, at minimum, access to NCS information, will be removed from that position.

e. In the absence of adverse information, temporary access (interim network access) may be granted by the BUMED HQ Security

JUN 03 2015

Manager for military members, civilian employees, and contractors (when appropriate, i.e., mission impact) who meet the requirements set forth in reference (b). If temporary access cannot be granted, civilian employees within their probationary period will be removed; civilian employees beyond their probationary period may be assigned non-sensitive duties (if available).

f. United States citizenship is a basic condition for access to classified information and assignment to a sensitive national security positions. Waiver requests may be initiated through OPM for non-United States citizens.

7. ISP. Applies to the classification, safeguarding, transmission, and destruction of information classified in the interest of national security. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of reference (d). Civilian employees are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of reference (d). Access is to be granted only on a need-to-know basis to the minimum number of individuals necessary to accomplish the mission. No one has a right to have access to classified information solely because of rank, position, or security clearance eligibility. Key components of the ISP include:

a. Reporting Counterintelligence Matters. All personnel are required to report counter-intelligence matters directly to Naval Criminal Investigative Service, 2713 Mitscher RD, SW, BLDG 168, Suite 200, Anacostia Annex, DC 20373. The espionage hotline is 1(800) 543-6289.

b. Staff Assistance Visits and Inspections. Personnel assigned to the BUMED HQ Security Department will conduct periodic staff assistance visits and inspections of work spaces and trash bins in an effort to ensure established procedures are being followed.

c. Marking Classified Documents. All personnel with access to classified information are required to complete the Defense Security Service Academy (DSSA) online course on Marking Classified Documents. All information, whether it is a secured internet protocol router network (SIPRNET) e-mail or actual correspondence, will adhere to marking requirements, to include classification level, paragraph and subparagraph markings, derivative information, and downgrading/declassification guidance. An e-mail created on the SIPRNET is considered to be a final document, not a working document, and must be marked as such. Personnel not adhering to

JUN 03 2015

required markings may have their access suspended for committing practices dangerous to security. Chief, BUMED is not designated as an Original Classification Authority in Exhibit 4A in reference (d); consequently, all classification markings should indicate the sources from which the classification has been derived. Finally, if information does not meet the requirements set forth in Executive Order 12958 to be classified in the interest of national security, personnel shall not mark it as classified information.

d. Storage. Reference (d) indicates specific requirements for storing various levels of classified and controlled unclassified information. Standard Form (SF) 700, Security Container Information and SF 702, Security Container Checklist must be used with the General Services Administration (GSA) approved storage containers. Combinations must be changed per reference (d).

e. Loss/Compromise of Classified Information Procedures. A compromise is the unauthorized disclosure of classified information to a person who does not have a valid clearance, authorized access, or a need-to-know. If a compromise occurs, BUMED HQ personnel must immediately notify the BUMED HQ Security Manager, who will then notify the COS, Naval Criminal Investigative Service (if required), and the Naval Network Warfare Command in the case of electronic spillage, per reference (e). A preliminary inquiry will be initiated if an actual loss or compromise occurs. A person, other than the BUMED HQ Security Manager or anyone involved with the incident, must be appointed in writing to conduct the Personnel Investigation (PI). Reference (d) provides specific guidance for initiating a PI. After completing the PI, if compromise cannot be ruled out or corrective/disciplinary action is required, an individual must be appointed in writing to conduct a Judge Advocate General Manual investigation. Personnel working in office spaces containing safes must inspect them for evidence of attempted entry. Digital safe combinations must be checked each time the safe is opened or closed to ensure numbered sequence has been recorded on the SF 702.

f. Authorization to Escort or Hand-carry Classified Information. The BUMED HQ Security Manager will issue a DD Form 2501, Courier Authorization, to individuals with a recurring need to escort or hand-carry classified information between DoD activities. The DD Form 2501 has an expiration date of no more than two years from date of issue and must be surrendered upon an individual's transfer, termination, or when authorization is no longer needed. Packaging and transporting guidance is provided in reference (d). If overnight travel is anticipated, storage arrangements must be made in advance for the classified material prior to departure.

g. Printing and Reproduction. BUMED HQ does not have a copier machine or scanner approved for reproduction of classified

JUN 03 2015

material. Printers approved at the Secret level are located in Security, 1NW472, BUMED-M1 (Human Resources Manpower Plans and Business Policy) 2NW400, and BUMED-M3 (Vault), 2NW163. All other printing and reproduction equipment at BUMED HQ is only approved for unclassified information.

h. Destruction. BUMED employees may destroy all documents by placing in approved burn bags. A burn bag receipt DD Form 2843 will accompany the material for destruction. The outside of each bag will be annotated with highest classification of the contents, point of contact office code, and telephone number. Burn bags must be sealed at the top and not weigh more than 10 pounds or is more than $\frac{3}{4}$ full. Drop off the burn bags over to the appropriate personnel on the appointed "burn run" day. Classified information cannot be stored in burn bags unless the office is approved for open storage. Classified information must remain in GSA-approved containers until ready for destruction (e.g. the day of the burn run, the classified material can be placed in the burn bags).

i. Dissemination. The BUMED HQ Public Affairs Office must ensure all proposed public releases undergo prepublication security and policy review using guidance provided in Exhibit 8B of reference (d).

j. Corrective Action. Security incidents, violations, and compromises will be evaluated on a case-by-case basis. Nature of incident, damage to national security, and willful intent are the only factors to be considered when determining consequences for incident, violation, and compromise. Consequences range from being removed from work space and undergoing an intense training program, suspension of local command access for classified information, and up to and including termination of employment.

8. Responsibilities

a. No individual will have access to classified information or be assigned to sensitive or NCS duties, to include IT II positions, unless a favorable personnel security determination has been made regarding his or her loyalty, reliability, and trustworthiness by DODCAF or DISCO based upon a NACLIC or ANACI background investigation.

(1) All personnel assigned and employed at BUMED HQ or any Detachment must meet the applicable investigative standards required to perform their duties and comply with security regulations.

(2) All BUMED HQ personnel granted eligibility for access to classified information must sign an SF 312, Classified Information Nondisclosure Agreement.

JUN 03 2015

(3) Prior to access being granted, to include a SIPRNET account, personnel must:

(a) Complete two online courses offered by the DSSA covering Marking Classified Documents and Introduction to Information Security at: <http://www.cdse.edu/catalog/information-security.html>.

(b) Receive a North Atlantic Treaty Organization Security Briefing.

Note: All personnel are expected and encouraged to challenge the classification of information which they believe to be improperly classified using established procedures outlined in reference (d).

b. The COS is responsible for compliance with and implementation of DoD's ISP and PSP within BUMED HQ. The COS must:

- (1) Safeguard classified material.
- (2) Approve an emergency plan for protection and destruction of classified information.
- (3) Designate key sensitive positions in writing.
- (4) Issue a written security plan.
- (5) Ensure command security inspections, program reviews, and assist visits are conducted for effectiveness of the ISP and PSP within BUMED HQ.
- (6) Establish an Industrial Security Program, if applicable.
- (7) Ensure that a robust security education and training program exists, and all personnel receive all mandatory security training.
- (8) Evaluate security personnel (to include critical security element in fitness reports, civil service performance plans, and personnel advancement requirements).
- (9) Serve as the designated decision official for all BUMED HQ civil service personnel where removal may be indicated based upon an unfavorably adjudicated PSI.

c. The BUMED HQ Security Manager must be a military officer or a civilian employee (GS-11 or above) designated in writing with sufficient authority and staff to manage the program for BUMED HQ. The BUMED HQ Security Manager is required to be a United States citizen, have been the subject of a favorably adjudicated Single

JUN 03 2015

Scope Background Investigation within the previous five years, and must also:

(1) Serve as the COS' advisor and direct representative in matters pertaining to security of classified information and personnel security.

(2) Develop written BUMED HQ information and personnel security procedures including an emergency plan which integrates emergency destruction procedures.

(3) Formulate and coordinate the BUMED HQ security education program.

(4) Ensure threats to security and other security violations are reported, recorded, and when necessary, investigated vigorously.

(5) Administer the BUMED HQ program for classification, declassification, and downgrading of classified information.

(6) Ensure BUMED HQ personnel who perform security duties are kept abreast of changes in policy and procedures and are provided assistance in problem-solving.

(7) Develop security measures and procedures regarding visitors who require access to classified information.

(8) Establish procedures for dealing with threats, compromises, and violations.

(9) Ensure compliance with the Industrial Security Program for classified contracts with DoD contractors, as applicable.

(10) Manage the command's JPAS and CATS and coordinate the continuous evaluation program for eligibility for access to classified information and/or assignment to sensitive duties.

d. Deputy Chiefs of BUMED will ensure all security regulations are enforced in their jurisdictions and that all security-related incidents, compromises, and violations are reported to the BUMED HQ Security Manager immediately. If applicable, they must ensure the security of their work spaces by designating a person to:

(1) Inspect daily to ensure classified material storage containers and locked files are secured; classified material is not adrift; windows are closed; and any apparent fire hazards are removed or reported to the Command Duty Officer before securing the space.

JUN 03 2015

(2) Ensure personnel are required to in-process and out-process with the BUMED HQ Security Department prior to performing any duties or permanently leaving BUMED HQ.

(3) Credible questionable, derogatory, or unfavorable information must be reported to the BUMED HQ Security Manager as part of the continuous evaluation program. Any BUMED HQ employee is able to report said information on himself or herself or others within BUMED HQ who have been granted access to classified information or assigned to sensitive duties, to include IT positions.

e. The IT and Communication Services Department will use the System Authorization Access Request-Navy process documentation which has been provided by the BUMED HQ Security Department to ensure all relevant documentation, to include favorable Federal Bureau of Investigation fingerprint checks and required background investigations per reference (e), have been verified and approved by the BUMED HQ Security Department prior to activating any computer or network access, to include establishing SIPRNET accounts.

9. Records. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

10. Forms

a. SF 312 (Rev. 07/2013), Classified Information Nondisclosure Agreement and SF 702 (8/85), Security Container Checksheet, are available electronically from the 'Forms' tab at:
<http://www.gsa.gov/portal/forms/type/>.

b. SF 700 (4/2001), Security Container Information, is available for order from the Federal Supply Service using national stock number (NSN) 7540-01-214-5372.

c. DD Form 2501 (MAR 1988), Courier Authorization, is a controlled form available only from the BUMED HQ Security Manager.


A. M. DIGGS
Chief of Staff
Acting

Distribution is electronic only via the Navy Medicine Web site at:
<http://www.med.navy.mil/directives/Pages/BUMEDHQInstructions.aspx>

JUN 03 2015

ACRONYMS

ANACI	Access National Agency Check with Written Inquiries
BUMED	Bureau of Medicine and Surgery
CAC	Common Access Card
CATS	Case Adjudication Tracking System
COS	Chief of Staff
CS	Critical-Sensitive
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DODCAF	Department of Defense Central Adjudication Facility
DOHA	Defense Office of Hearings and Appeals
DON	Department of the Navy
DSSA	Defense Security Service Academy
E-QIP	Electronic Questionnaire for Investigations Processing
FOUO	For Official Use Only
FSO	Facility Security Officer
GSA	General Services Administration
HQ	Headquarters
ISP	Information Security Program
IT	Information Technology
JPAS	Joint Personnel Adjudication System
LOI	Letter of Intent
NAC	National Agency Check
NACLC	National Agency Check with Local Agency and Credit
Checks	
NCS	Noncritical-Sensitive
NOTAL	Not to All
NSI	National Security Information
OPM	Office of Personnel Management
PI	Personnel Investigation
PSAB	Personnel Security Appeals Board
PSI	Personnel Security Investigations
PSP	Personnel Security Programs
SCI	Sensitive Compartmentalized Information
SF	Standard Form
SIPRNET	Secured Internet Protocol Router Network
SS	Special-Sensitive