

Revised March 2011



Standard Practice Procedures For Security Services

George Mason University
4400 University Drive, MSN 6D4, Fairfax, Virginia 22030

Letter of Promulgation

George Mason University (Mason) has entered into a security agreement with the Department of Defense in order to have access to information that has been classified because of its importance to the national defense. The Mason program and many of our activities are vital parts of the defense and security of the United States of America.

This Standard Practice Procedures (SPP) Manual is the official publication for policy and procedural details relating to the Mason security program. The policy and procedures outlined in the SPP are intended to supplement and clarify certain requirements of the National Industrial Security Program Operating Manual (NISPOM) and to assist employees in applying the provisions of the NISPOM to the Mason business environment. These procedures apply to the handling and safeguarding of classified information transmitted to Mason, of which the U.S. is obligated to protect in the interests of National Defense.

The provisions of this manual are applicable to all Mason sites and personnel operating under the Mason contract in accordance with National Industrial Security Program. This manual is readily available for cleared employee use.

The Mason Facilities Security Officer has the authority to impose and enforce the security procedures promulgated herein.

Keith R. Bushey
Facilities Security Officer

Table of Contents

Chapter 1	Security Functions and Organizational Responsibilities.....	6
1-1	U.S. Government Security Cognizance	
1-2	University Industrial Security Department	
1-3	Facility Security Officer	
1-4	Security Clearance Requirements	
1-5	Security Reviews	
1-6	Safeguarding Classified Material	
1-7	Pre-Publication Review	
1-8	Employee Security Responsibilities	
Chapter 2	Badges, Identification and Escort Procedures.....	12
2-1	General	
2-2	Badges	
2-3	Visit Authorization Request	
2-4	Visitor Control	
2-5	Escort Responsibilities	
Chapter 3	Personnel Security Clearances.....	15
3-1	Employee Clearances	
3-2	Non U.S. Citizens	
3-3	Clearance Notification	
3-4	MASON Security Clearance Records	
3-5	Consultants	
3-6	Clearance Terminations	
Chapter 4	Safeguarding Classified Information.....	18
4-1	General	
4-2	Accountability Procedures	
4-3	Disposition and Retention of Classified Material	

Chapter 5	Area Controls.....	24
5-1	Establishing Controls	
Chapter 6	Classified Meeting Guidelines.....	26
6-1	Security Coordination	
6-2	Attendees	
6-3	Physical Security	
6-4	Classification	
6-5	Note Taking and Electronic Recording	
Chapter 7	Security Awareness.....	28
7-1	Responsibility	
7-2	Briefings Prior to Access	
7-3	Refresher Briefings	
7-4	Debriefing	
Chapter 8	Couriers.....	31
8-1	General	
8-2	Definition	
8-3	Authority	
8-4	Approval Process	
8-5	Courier Appointments and Briefings	
8-6	Personnel Security Clearances	
8-7	Transmittal	
8-8	Courier Instructions	
Chapter 9	Visitor Controls.....	36
9-1	General	
9-2	Types of Visits	
9-3	Representatives of Government Agencies	
9-4	Assistance to Federal Investigators	
9-5	Visitor Records	
9-6	Visits by BAI Personnel to Other Installations	
9-7	International Visits	
Chapter 10	Reports.....	41
10-1	General	
10-2	Types of Reports	

Chapter 11	Investigations.....	44
11-1	General	
11-2	Responsibilities	
11-3	Disposition	
Chapter 12	Security Violations.....	47
12-1	General	
12-2	Policy Guidelines	
12-3	Reporting of Security Violations	
12-4	DOD Hotline	
Chapter 13	Automated Information Systems.....	50
13-1	General	
13-2	Change or Modifications	
Appendix 1	Laptop System Security Plan	52

Revised March 2011

Chapter 1

Security Functions and Organizational Responsibilities

1-1. U.S. Government Security Cognizance

The Secretary of Defense is authorized to act on behalf of certain departments and agencies of the United States Government (hereafter referred to as User Agencies) in rendering industrial security services. The Director, Defense Security Service (DSS) is responsible for the administration of the National Industrial Security Program on behalf of these User Agencies and will perform security oversight with respect to contractor facilities located within the specific geographic regions. In this regard, the cognizant security authority (CSA) is responsible for enforcing policies to safeguard classified information entrusted to that facility. In the event the contractor's facility is located at a User Agency installation, the Commander or Head of the User Agency may perform certain security functions. The provisions of this SPP Manual will apply regardless of location. At periodic intervals, the CSA will review the procedures and safeguards established by a facility. The MASON Facility Security Officer (FSO) will act as the primary liaison for all security relationships and communications between the CSA or Defense Security Service Industrial Representative.

1-2 University Industrial Security Department

- a. The MASON Facility Security Officer (FSO) has sole responsibility and authority for the development, execution, and enforcement of all organization-wide security policies, procedures, and programs. The FSO will also be the final authority for resolving conflicting security issues that concern University employees, their consultants and guests participating in the National Industrial Security Program (NISP).
- b. The overall mission of the MASON FSO is to contribute to the successful operation of the MASON programs and ensure compliance by maintaining the continued integrity of the Security Agreement and ensuring organizational and individual compliance with the security requirements of each classified contract.

1-3 Facility Security Officer (FSO)

- a. The MASON Senior Vice President will appoint a U.S. citizen who is appropriately cleared in connection with the Facility Clearance (FCL) to serve as the Facilities Security Officer (FSO). The FSO will be appointed by the Senior Vice President in writing and the appointment submitted to the DSS Industrial Representative.
- b. The FSO will report directly to the Vice President of Research and will also have unrestricted indirect reporting responsibility. The FSO may appoint an

assistant FSO or other individual entities (alternate FSO) to serve in his/her capacity. All such appointments shall be in writing and submitted to the DSS IR. The FSO may contract certain functions as he/she may determine but retain overall responsibility and authority as FSO under the NISPOM.

- c. Retention in these positions will be dependent upon successful completion of the prescribed training course. Additionally, security support personnel must undergo any other special training as directed by the CSA.
- d. Termination, Transfer or Departure of FSO
 - (1) In the event of a termination, transfer or departure of the FSO, the Senior Vice President shall immediately select a new FSO. The selection should occur as soon as the anticipated departure of the incumbent becomes known. Prior to an anticipated departure, the incumbent FSO and his/her successor will:
 - (a) Conduct a total inventory, physically sighting all classified holdings at the facility.
 - (b) Review past security assistance reports to determine status of the facilities security program.
 - (c) Review all Contract Security Classification Specifications (DD Form 254) for contracts being performed at the facility.
 - (e) Process the personnel security clearance for the successor FSO in connection with the facility clearance.
 - (f) Review all ongoing security actions and programs at the facility.
 - (g) Review all other files, records, and administrative systems and procedures applicable to this function.
 - (h) Process all JPAS accounts for the successor FSO in connection to the facility.
 - (2) The FSO may appoint an Assistant FSO who will act as the FSO in the temporary absence, sudden or unexpected departure of the FSO; except in those situations where the Senior Vice President elects to assign such responsibilities to another individual who is cleared in connection with the facility clearance.

1-4 Security Clearance Requirements

- a. The FSO will ensure that clearances are initiated in a timely manner for all personnel requiring access to classified material. Additionally, the FSO will ensure that only those personnel requiring access are submitted as candidates for a clearance in accordance with Chapter 3 of this SPP. A system will be maintained that ensures that the number of employees submitted for a clearance is kept to a minimum, consistent with operational needs. Upon granting of eligibility, each employee will receive the required security briefings on a recurring basis by the FSO or designate. Employees are advised of the hostile threat, their continuing need to safeguard classified information and the procedures they must utilize in safeguarding classified material.
- b. Reports required to be submitted by the NISPOM and this SPP are considered to be a contractual obligation and will be submitted without interference to proper security officials in a timely manner. No management official will take action that will interfere in the proper discharge of duties required by the NISPOM or customer security regulations.

1-5 Security Reviews

- a. Each cleared MASON area will cooperate in reviews conducted by Defense Security Service (DSS) Industrial Representatives (IR). All necessary actions required will be taken immediately. A copy of each review report will be forwarded to the DSS IR. In order to maintain a constant awareness of the security status of the MASON facility, the FSO shall perform regular security assessments for the purpose of evaluating all security procedures and controls applicable to the facility's operations.
- b. The FSO may conduct random unannounced package checks to ensure that no classified materials are entering or leaving the facility improperly. Additionally, packages will be checked to ensure that prohibited items are not entering the facility. The following materials are considered prohibited items within areas processing or discussing classified information:
 - (1) Firearms and ammunition (except law enforcement and authorized security personnel) (concealed weapons permit is not an exception.)
 - (2) Volatile hazardous substances
 - (3) Alcoholic beverages, controlled substances or contraband

- (4) Unauthorized photographic equipment
- (5) Unauthorized recording equipment
- (6) Unauthorized transmittal of proprietary or government material

Each facility will have notices posted at the entrances to advise personnel of these restrictions.

1-6 Safeguarding Classified Materials

- a. The FSO shall establish an information management system that accomplishes the functions of receipting, accounting, storing, transmitting, and destroying classified holdings and allows for the retrieval of documents in a reasonable period of time. Each employee will ensure that the classified material entrusted to him/her is properly stored and safeguarded in accordance with regulations and procedures herein. Violations will be reported to proper authorities so that corrective actions can be taken.
- b. The FSO shall maintain a copy of the classified inventory as part of his backup plans and procedures in cases of an emergency.
- c. Specific guidance pertaining to the protection and control of classified information is contained in Chapter 4.

1-7 Pre-Publication Release

To preclude the potential for the inadvertent disclosure of classified or sensitive program information, brochures, newspapers or similar type material shall not be published or distributed without the prior review and written authority from the CSA for the DD254 for that specific program, except as authorized by the NISPOM. The FSO and the contract Program Manager are responsible for coordinating these activities.

1-8 Employee Security Responsibilities

- a. Each cleared MASON official is individually responsible for adhering to the regulations established in this manual, as well as the regulations of our customers at their locations, to effect the successful operation of the university security program and to safeguard classified information.
- b. By the acceptance of a personnel security clearance, the employee assumes a great trust that carries with it a most important individual responsibility: the

Revised March 2011

safeguarding of sensitive information vital to the security of the nation. At times, security practices and procedures will cause personal inconvenience. These measures will take time and effort, and on occasion, make it necessary to forego some personal prerogatives. Employees must maintain constant awareness of all of the security requirements associated with their position. Ignorance of a security regulation or requirement will not excuse the individual from disciplinary action in the event of a violation.

Revised March 2011

CHAPTER 2
BADGES, IDENTIFICATION, AND ESCORT PROCEDURES

2.1 General

- a. University employees are responsible for safeguarding classified information in their custody or under their control.
- b. The MASON FSO is required to supervise and direct security measures as necessary.

2-2 Badges

- a. Employee Identification Badges

The university issues a permanent laminated picture identification badge to all employees and students. However information is not placed on the badge to discern clearance level. Therefore, the FSO shall introduce or verify individual clearances to other MASON employees using the third party introduction method. Employees are encouraged to check with the FSO if knowledge of an individual's clearance is unknown.

- b. Visitor Badges

Visitors to MASON at the classified level must have their clearances sent to the FSO via fax or through the JPAS process. Laminated badges will not be issued to visitors indicating clearances. In instances where the visitor either has no visit request or clearance on file, or has no contractual association with MASON, (i.e., salesmen, vendors, applicants, etc.), a temporary badge denoting the requirement for an escort may be issued. It is the responsibility of the host to escort all visitors whose clearances are on file while visiting the MASON campus.

2-3 Visit Authorization Requests

- a. Visitors are responsible for submitting a Visit Authorization Request (VAR) prior to arriving for a visit. MASON employees who are hosting a visitor will provide the name, phone number and fax number for the FSO to the prospective visitor. This must be done a minimum of five work days in advance of the planned visit. Hand-carried VAR's on the day of the visit will not be accepted.
- b. Once the FSO has received the VAR, he/she will ensure the data is updated in the Visitor Database and notify the host that the clearance(s) have been received. It is the responsibility of the host or FSO to verify the visitors' identification before releasing classified information in their

possession. All visitors must present valid identification upon entering the secure area before classified information is transferred to the visitor.

2-4 Visitor Control

- a. When a visitor arrives, the FSO or designee, will verify the visitor's clearances. All visitors must sign a MASON Visitor's Sign In Sheet. If the FSO, or designee, has no record of a VAR, then access may be granted provided the host complies with his/her escorting responsibilities outlined in section 2-5. Only the FSO, or Alternate FSO, may authorize a guest to begin a visit without a VAR on file.
- b. When a visit is completed, the visitor will return his/her badge to the FSO or AFSO and log out of the Visitor's Log.
- c. Any questions regarding visit procedures will be referred directly to the FSO. In the event that the FSO is not available, the Alternate FSO or designee will be contacted.

2-5 Escort Responsibilities

A designated escort is responsible for ensuring visitors under his/her supervision only access authorized areas. Escorts will be briefed by the FSO or AFSO on their responsibilities prior to assuming responsibility as an escort.

Revised March 2011

CHAPTER 3
PERSONNEL SECURITY CLEARANCES

3-1 Employee Clearances

- a. MASON personnel designated for access to classified material within the scope of their employment or contract will be processed for a security clearance. The FSO and supervisor or departmental manager will make the determination for the requirement of a security clearance based on contractual obligation or direct Government sponsorship. The contractual stipulations and the Contract Security Classification Specification associated with each classified contract is a major consideration in determining the need for personnel security clearances (PCL). Government sponsorship is generally done via specific determination made by name for the individual to be processed for a PCL. The FSO shall contact the sponsor and together they will determine the appropriate contract vehicle to initiate the clearance access process.
- b. Those personnel requiring an initial investigation or periodic reinvestigation will be submitted through the e-QIP process. The FSO or designate will contact the individual and acquire the data needed to initiate the clearance application in accordance with NISPOM directives. Employees already cleared and determined eligible are granted access according to the Joint Personnel Access System (JPAS).

3-2 Non-U.S. Citizens

Non-U.S. citizens will only be processed or issued a clearance in those cases where the individual possesses some exceptional skill or talent which is critical to the performance of a contract and where special authorization is obtained from a Contracting Officer and the CSO. Such individuals may be granted a Limited Access Authorization (LAA).

3-3 Clearance Notification

- a. All PCL are granted via JPAS. When an eligibility determination is granted, the FSO or AFSSO shall notify the individual that he or she is approved and will brief the individual on security procedures. If the person does not have a current Non-Disclosure Agreement or SF-312 indicated in JPAS, the FSO or AFSSO shall prepare the form and get the person to sign it prior to the briefing. Once eligibility determination is confirmed, the FSO/AFSSO shall perform the following tasks:
 - (1) Brief the individual,

- (2) Notify the employee's department/project supervisor. The supervisor will verbally advise the employee of his/her clearance status.
 - (3) The FSO or designee will perform the security indoctrination with the employee. The FSO will witness the signature of the employee and will forward the SF 312 to the CSA. The FSO will also both send a copy to DSS and file a copy inside the employee's security file.
- b. The termination of an employee: (1) whose clearance is in process at the time of termination; (2) who has an active clearance; or (3) who has an administratively terminated clearance; will be reported to the FSO who will in turn notify DSS via JPAS that the individual no longer works at MASON and will be separated from MASON within JPAS.

3-4 MASON Security Clearance Records

The FSO or designee is responsible for maintaining a current database of the security clearance information of all employees who possess security clearances or who are in the process of obtaining a security clearance. At a minimum, the information in the record will reflect the level and date of clearance, as well as the clearing agency. In addition, the record may contain a complete clearance action history, overseas eligibility determination, and visit request information.

3-5 MASON Consultants

Consultants who require access to classified material are cleared in the same manner as MASON employees except that a Consultant Agreement must be executed in addition to regular processing forms. The FSO shall monitor Consultant clearances to ensure that clearances are terminated upon expiration of the consultant agreement or when inactivity has occurred over the past 12 months.

3-6 Clearance Terminations

Upon notification of termination of employee (discharge, resignation, retirement or the beginning of a layoff or leave of absence of indefinite duration or excess of one year), the employee, consultant or individual's supervisor will advise the FSO. The FSO will in turn notify the DSS via JPAS. The employee or consultant shall ensure upon departure that all classified material within his or her possession has been accounted for and transferred to another appropriately cleared and authorized individual.

Revised March 2011

CHAPTER 4

SAFEGUARDING CLASSIFIED INFORMATION

4-1 General

This section contains the basic regulations that govern the handling of all classified information. It is essential that these rules are understood and obeyed by all personnel whose duties require contact with classified material.

4-2 Accountability Procedures

a. General Policy

The FSO is responsible for establishing and coordinating information management for the control of classified information in its possession in accordance with the NISPOM. Personnel working under contract will ensure that all classified information in their custody is used or retained only in the furtherance of a lawful and authorized U.S. Government purpose.

b. Document Control

Any classified material regardless of classification must be processed through an accountability system. The FSO will administer any accountability system that is required by the NISPOM and will be available to assist in any reviews conducted by the cognizant DSS office. The term "accountability system" defines the procedure for the transmission of classified material to and/or from, or within MASON possession is recorded.

c. Records

(1) MASON shall maintain a record that reflects:

- (a) The date of the material
- (b) The date of receipt or dispatch (via a receipt)
- (c) The classification
- (d) An unclassified description of the material
- (e) The identity of the activity from which the material was received or to which the material was dispatched.

- (2) Receipt and dispatch records shall be retained for 2 years.
- (3) The FSO shall maintain a copy of the inventory and retain the data for five years following dispatch of the material.

d. Receipt of Incoming Classified Material

All Registered, U.S. Postal Service Express, and Certified Mail shall be mailed to George Mason University, Attn: Facility Security Officer, Post Office Box 319, Fairfax Station, Virginia 22039. The mailbox will be checked no less frequently than every two weeks by an appropriately cleared, designated individual or the FSO. All classified material being hand-carried, and all incoming registered, express, and certified mail will be given immediately to a specifically designated individual or to the FSO.

e. Identification Markings

All classified material, regardless of the form in which it appears, will be marked with the appropriate information to ensure that it is afforded the necessary safeguards. Markings must be uniformly and conspicuously applied to documents to leave no doubt as to the classification level, the reason for classification, the duration of classification, and the authority or source for classification. Material will be marked in accordance with the NISPOM and Executive Order 12958.

f. Generation of Classified Material

SECRET or CONFIDENTIAL: marked with the overall classification and with the annotation. "WORKING PAPERS" will be dated when created and destroyed when no longer needed or within 6 months.

g. Transmittal of Classified Material Outside of Facility

- (1) Classified material transmitted/sent by MASON within the U.S., Puerto Rico, or a U.S. Trust Territory will be accomplished by the following means:
 - (a) SECRET: By the methods established for TOP SECRET, or U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, cleared "Commercial carrier", cleared commercial messenger service, a commercial delivery company approved by the CSA, or other methods as directed, in writing, by the CSA. (Refer to the NISPOM for explicit directions).

- (b) CONFIDENTIAL: By the methods established for SECRET material or by U.S. Postal Service Certified Mail.
 - (2) All classified material, regardless of classification, being transmitted from the facility will be packaged and appropriately dispatched by the FSO.
- h. Storage of Classified Material
- (1) Storage containers for classified material will conform to the specifications for safes and locked filing cabinets. The FSO shall maintain all storage devices in accordance with DCID 6/9 Physical Security and NISPOM.
 - (2) A minimum number of authorized persons shall have knowledge of combinations. The FSO shall maintain a listing of all combinations in a sealed envelope with clear instructions at an offsite location/facility at the same or higher facility clearance level.
 - (a) Security containers, closed areas, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.
 - (b) The combination shall be safeguarded in accordance with the highest level of classified material retained in the container.
 - (c) Superseded combinations will be destroyed.
 - (3) Combinations shall be changed by the FSO whenever an employee who has the combination is debriefed or terminated. In addition, combinations are changed when a security compromise occurs or as instructed within DCID 6/9.
- i. When in use, classified information must be under the continuous supervision of an authorized user who is in a physical position to exercise constant control over the material.
- j. The FSO shall encourage users and/or authorized MASON personnel to keep reproduction of classified material to a minimum that is consistent with contractual and operational requirements.

4-3 Disposition and Retention of Classified Material

- a. Classified information no longer needed shall be processed for appropriate disposition. The FSO or designee will perform all destruction of classified material required at MASON in accordance with the instructions outlined in the NISPOM. No classified information will be retained beyond contractual requirements without retention authority from the official source as identified within the DD254 or Government Contracting Authority (GCA). The FSO shall establish procedures for review of all classified holdings on an annual basis to reduce classified inventories to a minimum necessary for effective and efficient operations.
- b. MASON personnel desiring to retain classified material received or generated under a contract may do so for a period of 2 years after completion of the contract, provided the GCA does not advise otherwise. If retention is required beyond the 2-year period, written authorization must be received by the GCA.
- c. MASON shall return or destroy classified material in accordance with the following schedule:
 - (1) If the classified material was not received under a specific contract, such as material obtained at classified meetings or from a secondary distribution center, within 1 year after receipt.
 - (2) MASON will destroy classified material in their possession as soon as possible after it has served the purpose for which it was intended. Approved methods for destruction are listed in the NISPOM.
 - (3) The destruction of classified information will be accomplished by appropriately cleared employees.
 - (4) All classified waste will be destroyed as soon as practicable in accordance with the destruction methods prescribed herein. Pending destruction, classified waste will be properly safeguarded and receptacles used to accumulate such waste will be clearly identified.

4-4 Classified Computing

For the purpose of this document, Automated Information Systems (AIS) will include any electronic equipment capable of recording, transmitting, storing and/or processing classified data such as computers, typewriters, calculators, test bed equipment, copiers, facsimile machines, or any other equipment or device which employs any nature of memory components and is utilized to such a degree to manipulate classified data. Automated Information Systems (AIS),

used to capture, create, store, process or distribute classified information must be operated so that the information is protected against unauthorized disclosure or modification.

Protection requires a balanced approach that includes AIS features, as well as administrative, operational, physical, and personnel controls. Protection is commensurate with the classification level and category of the information, the threat, and the operational requirements associated with the environment of the AIS.

Physical security safeguards shall be established that prevent or detect unauthorized access to accredited system entry points and unauthorized modification of the AIS hardware and software. Hardware integrity of the AIS, including remote equipment, shall be maintained at all times, even when the AIS is not processing or storing classified information.

Attended classified processing shall take place in an area, normally a Restricted Area, where authorized persons can exercise constant surveillance and control of the AIS. All unescorted personnel to the area must have a government granted PCL and controls must be in place to restrict visual and aural access to classified information.

When the AIS is processing classified information unattended, or when classified information remains on an unattended AIS, a Closed Area is required.

When the AIS is not in use, all classified information has been removed and properly secured, and the AIS has been downgraded, continuous physical protection, to prevent or detect unauthorized modification of the AIS hardware and software, shall be implemented through one or more of the following methods:

- (1) Continuous supervision by authorized personnel.
- (2) Use of approved cabinets, enclosures, seals, locks or Closed Areas.
- (3) Use of area controls that prevent or detect tampering or theft of the hardware and software. These controls will vary depending on the overall physical security controls in effect in the immediate secure area.

Currently at Mason, the only classified computing is to be done on a dedicated laptop computer. When not in use by an appropriately cleared individual, the entire laptop computer will be stored in the approved safe as described above in the section entitled "Storage." Specific guidance on the use and storage of the laptop computer is provided in **APPENDIX I: Laptop System Security Plan**.

Revised March 2011

CHAPTER 5

AREA CONTROLS

5-1 Establishing Controls

- a. The FSO is responsible for establishing control areas that may be required to provide additional protection to adequately safeguard classified documents and material. Controlled areas may be of two types: Restricted Areas and Closed Areas.
 - (1) Restricted areas: when it is necessary to control access to classified material in an open area during working hours, a restricted area may be established. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. For example, a room or lab with a lock and intrusion detection system or alarm is acceptable. Access to the area is controlled by a guard or access control device, i.e., combination lock, badge access card, etc.
 - (2) Closed areas: closed areas may be required due to the size and nature of classified material or to operational necessity. They must be approved by the CSA and constructed in accordance with the NISPOM.
- b. Employees will challenge unauthorized personnel found in either a Closed Area or a Restricted Area and should report such violations to the FSO immediately.

Revised March 2011

CHAPTER 6
CLASSIFIED MEETING GUIDELINES

6-1 Security Coordination

Any employee anticipating sponsoring or conducting a classified meeting must coordinate those plans with the FSO responsible for the area where the meeting is to be held.

6-2 Attendees

Attendees at the classified meeting will be limited to only those authorized individuals who are properly cleared and certified as having a need-to-know. The FSO is responsible for verifying the clearance level of each attendee. Any person whose clearance is not verified must be excused from the meeting.

6-3 Physical Security

The physical security measures for the classified sessions shall provide for control of, access to and dissemination of the classified information to be presented and shall provide for secure storage capability, if necessary.

6-4 Classification

The classification of a meeting is determined by the highest classification of the subject matter being discussed. All attendees of the meeting must possess at a minimum the same level or higher clearance level as the material. The individual holding the meeting shall orally advise all attendees of the classification of the information being divulged to them and remind them of their responsibilities to safeguard that information.

6-5 Note Taking and Electronic Recording

Generally, the taking of notes and the recording of a classified meeting is discouraged. However, when note taking is necessary to fulfill an official need, all classified notes should be collected at the end of the meeting and mailed to the attendees in the same manner as any other classified material. Electronic recording devices are prohibited in classified meetings.

Revised March 2011

CHAPTER 7

SECURITY AWARENESS

7-1 Responsibility

- a. The FSO or designee will be responsible for the implementation, administration, and coordination of security briefings. The FSO will be responsible for ensuring all appropriate MASON employees participate in the MASON Security Education/Awareness Program.
- b. When access to classified information is essential in the performance of a contract, employees will be cleared to the highest level authorized under the contract, and debriefed upon termination of employment or as otherwise specified.

7-2 Briefing Prior to Access

- a. The employee must execute Standard Form 312, Classified Information Non-Disclosure Agreement prior to accessing classified information. The Standard Form 312 will be forwarded to DSS if one is not already indicated in JPAS and a copy kept in the employee's security file. In addition, he/she will be briefed on his/her obligation to safeguard classified information. The FSO will advise the employee of the importance of the classified material and inform him/her of their responsibilities.
- b. Employees who refuse to execute SF 312 will forfeit their approval to access classified information. The FSO shall inform DSS and notify their supervisor of the employee's refusal.

7-3 Refresher Briefings

At least annually, each employee will be briefed concerning responsibilities to safeguard classified information, the hostile intelligence threat and methods of operations, and the local security procedures. This briefing will be prepared by the FSO and provided to each employee. The FSO shall determine the best possible means to distribute and/or conduct the annual refresher briefing. The FSO may use one or several means to distribute the material and ensure that each employee is given an opportunity to refresh themselves on their obligations and responsibilities to protect classified material under their control. The FSO shall retain a record of each briefing, identifying each employee who has completed the annual requirement.

7-4 Debriefing

- a. When a cleared employee, who has been granted a security clearance, either terminates employment (including discharge, resignation, or retirement), or departs on a leave of absence (for an indefinite period or longer than one year) he/she shall be debriefed by the FSO or designee. The FSO shall separate the employee within JPAS and place their security file in retention for 2 years.
- b. Employees who are placed on long-term disability may be debriefed administratively, and will be re-briefed upon their return to work. The FSO shall inform the supervisor of which action is being taken prior to taking such action. In addition, if the FSO determines to debrief the employee, the FSO or supervisor shall advise the employee that he/she is no longer in access under Mason's authority.

Revised March 2011

CHAPTER 8

COURIERS

8-1 General

These guidelines are intended to amplify procedures described in the NISPOM regarding the hand-carrying of classified information by MASON personnel.

8-2 Definition

A courier is defined as an appropriately cleared employee of MASON who has been authorized by the MASON FSO to transport or accompany classified material outside a facility, and one who has been properly briefed in their responsibility to protect such material while in-transit.

8-3 Authority

Transmission of classified material via courier is authorized only at the Secret level within the continental limits of the United States. Employees must receive written authorization from the FSO prior to transporting classified material. Employees who have a repetitive need to transport classified materials will be issued a "Courier Card" signed by the FSO, see section 8-5 for specific guidance.

8-4 Approval Process

Requests for Courier authorization and approval shall be made to the FSO at least 2 days prior. The FSO will perform the required briefings, authorize the issuance of a Courier Authorization Letter on MASON letterhead or a Courier Card and provide the courier with other special guidance or instructions as may be required. The FSO shall retain a copy of the appointment letter in their security file until the individual is no longer required to transport classified materials.

8-5 Courier Appointments and Briefings

- a. Certain employees may be designated as regular couriers who perform this function on a daily or frequently scheduled basis as part of their normal job activity. These individuals will be briefed on their responsibility to safeguard classified information.
- b. Occasionally, it is necessary to designate other appropriately cleared employees as couriers to hand-carry classified material on an infrequent or emergency basis.
- c. In these instances, the employee will receive an initial courier briefing and will be provided with a Courier Authorization Card not to exceed one full year or

12 months. These cards will also be provided to regularly appointed couriers when utilizing a mode of travel other than automobile or when required to satisfy contractual or security requirements.

- d. In some instances, the User Agency may stipulate a requirement to administer special courier briefings and indoctrinations to be administered by a U.S. Government official in addition to those given by MASON or to reserve the authority for courier appointments. In these cases, the User Agency directives will govern.

8-6 Personnel Security Clearances

Couriers must possess a final personnel security clearance at least at the highest classification level of the material being transported.

8-7 Transmittal Procedures

- a. The servicing FSO shall ensure that the proper marking, accountability, and packaging requirements are accomplished prior to shipment.
- b. Prior to accepting a classified shipment, the FSO or designee will ensure that the shipment is wrapped in accordance with prescribed procedures. Under no circumstances should an improperly prepared shipment be transported from the facility.

8-8 Courier Instructions

- a. Pickup and delivery must be scheduled to occur within normal working hours of the same day. If, in any rare and unusual situation where the pickup and delivery cannot be accomplished in the same day, the FSO or designee must be advised so that emergency safeguarding arrangements can be made for approved overnight storage.
- b. Couriers will not make any unauthorized stops while transporting classified material that would leave the material unprotected or susceptible to compromise.
- c. The material must remain in the continuous possession and control of the courier until delivery is made, or in the event of an emergency, approved alternate storage arrangements are confirmed.
- d. Prior to departure on trips exceeding 50 miles one way or the Washington, DC metropolitan area, the courier will contact the receiving facility and ensure

that arrangements are made to receive the material. If, for any reason, the receiving facility cannot accept the material on the day of intended delivery, the courier will not transport the material and alter their plans accordingly.

e. Via Automobile

- (1) While en route, the courier will not allow the classified material to be left unattended in a vehicle, nor will it be taken into a lunchroom, restaurant, restroom, or any other location where the potential for loss or compromise exists.
- (2) The courier will operate the vehicle in a safe, lawful manner and insofar as possible, avoid any situation, which could possibly result in arrest, detention, or possible physical separation from the shipment. Intoxicants or drugs that may impair the individual's judgment may not be used while assigned to courier duties.
- (3) The courier will also maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the shipment and take such action as may be necessary to avoid interference with the safe passage of the vehicle. If it is necessary to detour from a prescheduled route of travel, the courier should be familiar with the side roads and where they lead.

f. Via Commercial Aircraft

- (1) Hand carrying of classified material on commercial aircraft must be authorized in writing only by the FSO after coordination with the GCA. Only classified documents may be transported. Bulky packages or classified hardware may not be carried aboard aircraft.
 - (a) The courier must possess the prescribed courier identification and a Courier Authorization Letter bearing the original signature of the FSO.
 - (b) Packages must be double-wrapped and sealed. The package must be of a thickness, which will allow physical inspection at an airport screening station by flexing, feeling, etc., without the envelope being opened.
 - (c) The envelope will contain no binders, paper clips, or other metal, which would inhibit processing by detection devices at the airport.

- (d) In the event the inspection official requires the classified envelope to be opened, the courier will present the Courier Authorization Letter and his/her credentials and request that the package be examined by a detection device. If no alarm results, the courier will be allowed to proceed.
- (e) In all instances, the courier will not authorize the opening of the classified envelope. If the above measures do not permit boarding without opening the envelope, the courier will not board the aircraft but will return to his/her facility for alternate means of transmitting the material. Any instances in which the envelope has been opened will be reported promptly to the FSO who will in turn report the incident to the GCA.
- (f) In the event a courier is aboard an aircraft which is hijacked and lands in a foreign country, he/she will conduct themselves as follows:
 - (1) If identification is required, the courier will present civilian personal identification.
 - (2) He/she will not, under any circumstances, volunteer that he/she has classified information in their possession.

Revised March 2011

CHAPTER 9

VISITOR CONTROLS

9-1 General

- a. The MASON FSO or designee is responsible for the organization and supervision of the MASON visitor control program, which is concerned with both classified and unclassified visits to areas where access to classified material or classified research is possible, and for the maintenance of visitor control records required IAW the NISPOM.
- b. The objectives of the visitor control program are:
 - (1) To ensure that visitors of the MASON facility do not gain unauthorized access to classified material and/or proprietary information, and
 - (2) To limit all visits, particularly those requiring access to classified material, to the minimum number consistent with the efficient transaction to fulfill contract obligations.

9-2 Types of Visits

- a. In general terms, all visits to MASON are defined as classified or unclassified, depending on the nature of the visitor's business and/or clearance status. Unclassified visits are permitted and are not controlled by provisions of the NISPOM. However, proper identification of all visitors must be obtained, and the standard visitor control procedures outlined herein will be followed. Security procedures for controlling classified visits (also defined as authorized visits) must be in accordance with stipulations of the NISPOM.
- b. Unclassified Visits

General admission of visitors who are not cleared will typically fall into one or more of the categories listed herein. Those persons permitted to enter the facility on unclassified business are applicants for employment, technical and administrative personnel, vendor representatives, service personnel, etc. After admission to the facility is authorized, the visitor will be escorted if the visit is near where classified information is discussed or processed. Those personnel requiring an escort will be accompanied by a designated employee and escorted from the time of admission until the time of departure. An entry will be made in the Visitor Log recording the name and activity / home organization of the visitor as well as the time of entrance and exit.

c. Classified Visits

- (1) A person desiring to visit MASON on classified business must ensure his/her clearances are on file with the MASON FSO.
- (2) All visitors requiring access to classified information must possess security clearances commensurate with the classification of the information sought. The FSO is responsible for verifying that each authorized visitor has an adequate security clearance and has need-to-know at the time of his visit.
- (3) Approval of a classified visit constitutes authority to disclose classified information only to the extent cited in the authorization and in accordance with the limitations imposed herein. Approval of the visit does not imply authorization for the visitor to remove classified material.

9-3 Representatives of Government Agencies

Representatives of the following Government agencies, when acting in their official capacities and upon presentation of proper credentials, are not considered visitors. However, please ensure that each and every visitor signs the visitor log upon entering your facility.

- a. Industrial Security Representatives of DoD and other User Agencies
- b. Defense Security Service
- c. Federal Bureau of Investigation

9-4 Assistance to Federal Investigations

- a. Each facility will cooperate fully with representatives of Federal investigative agencies and of cognizant security offices conducting official investigations pertaining to the unauthorized disclosure of classified information or concerning the eligibility of personnel requiring access to classified information. This will include providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours and making employment and security records available for review upon request of such representatives and otherwise rendering assistance as necessary.

- b. Similarly, the same assistance and cooperation will be made available to representatives of the MASON Security Office during any investigation or inspection being conducted by that office.

9-5 Visitor Records

- a. Records of authorized visitors to MASON whose purpose is to have access to classified material will be maintained by the FSO. At a minimum, the records will reflect the name of the visitor and the activity represented as well as the date and time of arrival and departure.
- b. The Classified Visit Request will be maintained for a minimum of six months after completion of the visit but no longer than one year from the day of visit.

9-6 Visits by MASON Personnel to Other Installations

- a. When a MASON employee wishes to make a classified visit to another facility or User Agency activity, he/she will notify the MASON FSO to seek such a request.
- b. The request shall be submitted to the FSO as soon as possible but no later than 24 working hours (i.e. three full work days) before the day of travel when traveling within the continental U.S., and no later than 30 days in advance of foreign country visits. The FSO or designee will certify, prepare and forward the request to the proper authority.
- c. Classified visits will be authorized only for the transaction of business involving:
 - (1) An existing contract between MASON and the organization being visited
 - (2) Pre-contract negotiations
 - (3) Mutual exchange of information
 - (4) Contacts with Government agencies, or
 - (5) Travel to overseas locations.

9-6 International Visits

Because of U.S. export laws, we are often required to restrict the access of foreign persons to our technical information. As a result, the visit of any foreign person to a U.S. facility must be reviewed for export licensing requirements. A U.S.

Revised March 2011

Government export license may be required prior to disclosing any technical data (other than sales & marketing data), or materials to foreign persons, including foreign persons who are employees of MASON.

Revised March 2011

CHAPTER 10

REPORTS

10-1 General

The FSO is responsible for reporting to the appropriate U.S. Government agencies certain facts and information regarding the security status of contracts, facilities, and/or employees. **Such reporting is mandatory and is exempt from any privacy acts or other Federal statutes.** Reports will be marked with the caveat: "Government: For Official Use Only" and/or "Industry: Company Proprietary."

10-2 Types of Reports

a. MASON Facility Reports

(1) Changes or Establishment of Controlled Areas

The FSO will report to the CSA via MASON letterhead change(s) in the extent or location of closed areas, restricted areas, and vaults created under the provisions of Chapter 5, Section 3, (NISPOM). The FSO will also inform the CSA of the establishment of such areas.

(2) Change(s) to the Key Management Personnel (KMP) listing

The FSO shall report changes in the KMP listing to their DSS Industrial Representative.

(3) Change(s) in Mason's Facility Clearance

The FSO shall report any changes that would have an impact on Mason's facility clearance to the CSA via MASON letterhead. Reports are filed with the FCL Management notebook and retain until reviewed by the DSS Industrial Representative.

b. Individual Employee Reports

(1) It is the individual responsibility of each cleared MASON employee to advise his or her FSO or designee of any known or suspected threat to the security of MASON or to the national interest of the United States of America.

(2) It is critically important that employees report the following specific situations immediately:

- (a) Adverse information concerning any employee possessing, or in the process of obtaining, a security clearance, including any such situation in which the employee may be personally involved.
 - (b) Any change of an employee's status (e.g., death, change of name).
 - (c) Loss, compromise, or suspected compromise of classified material.
 - (d) Any existing, suspected, or threatened espionage, sabotage, or subversive activities, or any suspicious contact or association with employees by individuals seeking information regarding classified contracts or other unusual elements of information concerning the employee's duties, knowledge, responsibilities, or relationships gained through employment with MASON.
 - (e) Foreign interest representation.
 - (f) Any security violation.
 - (g) Evidence of tampering with a shipment containing classified information.
 - (h) Change in citizenship status.
 - (i) The unwillingness of any employee to perform classified work or accept security responsibilities.
 - (j) The request by any employee to terminate a clearance or clearance action, or reject a clearance.
- (3) Foreign Travel

All employees should notify the FSO immediately of anticipated foreign travel or attendance at conferences and symposiums where foreign nationals may be present. Following such notification, the FSO will provide the traveler with a foreign travel orientation if necessary as provided by the CSA.

Revised March 2011

CHAPTER 11

INVESTIGATIONS

11-1 General

- a. Occasionally, it is necessary to conduct certain levels of inquiry into a security violation to obtain sufficient evidence and information regarding what has occurred, how it occurred, who is responsible or involved, and to make an assessment and determination of the degree of damage or potential for damage caused by the incident. While almost any person with good judgment and an awareness of people and things can often logically follow an inquiry to a useful conclusion, that effort cannot always be applied in the matter of security investigations. These investigations require in-depth knowledge of the National Industrial Security Program Operating Manual (NISPOM), the legal and judicial considerations, rules of evidence, the environmental security conditions, and myriad other factors to be considered in planning, executing, and reporting a security investigation.
- b. The value of a well-executed investigation cannot be overestimated. The security integrity of an entire facility, its employees, and its business may depend on the outcome of such an investigation. In this regard, the FSO will provide onsite guidance, assistance, and professional resources in the conduct of a field investigation.

11-2 Responsibilities

- a. The FSO will be responsible for conducting initial administrative inquiries and other preliminary investigations as required. All information will be reported to the CSA by the most expeditious means possible. Major incidents must be reported within 1 hour of discovery. As a general rule, major incidents are defined as those, which might have a substantial adverse impact on the security or business operation of the facility or upon the employees, the university, a program, or contract. The following examples include, but are not limited to, those situations that would be considered as being of a major nature:
 - (1) Suspension/termination of a facility clearance because of unsatisfactory security conditions.
 - (2) Loss, compromise, or suspected compromise of SECRET or TOP SECRET classified information.
 - (3) Espionage, sabotage, and acts of terrorism against the University.
 - (4) Arson, bombings, and major crimes involving violence.

- (5) Theft, fraud, embezzlement, or larceny of money or property, the value of which exceeds \$5,000.

- b. At foreign locations, acts of terrorism, kidnapping, etc., must be reported immediately to the nearest U.S. embassy and ultimately the CSA and MASON FSO.

11-3 Disposition

No final disposition of a major investigative matter will be made to the CSA prior to a review of the substance of the investigation by the responsible Key Management Person for MASON; and, if required, a representative of the legal staff, and presentation of the facts to the George Mason University Board of Visitors.

Revised March 2011

CHAPTER 12

SECURITY VIOLATIONS

12-1 General

A violation of any of the regulations prescribed within this manual or other recognized security practice established by MASON is defined as a security incident. Such an infraction places both the concerned individual and the contract in jeopardy. To emphasize the importance of compliance with all security measures, MASON has established certain internal discipline standards.

12-2 Policy Guidelines

- a. The following are among those actions that may prompt MASON to take immediate action, up to and including termination, if the incident occurs in such a manner as to involve MASON or its government customer:
 - (1) Being under the influence or in possession of alcoholic beverages or narcotics.
 - (2) Theft, willful destruction, defacing or misuse of the university's or a fellow employee's property, and/or removing such property from the premises without proper authorization.
 - (3) Criminal behavior.
 - (4) Unauthorized possession of a dangerous weapon on MASON property.
 - (5) Willful violation or neglect of security regulations or procedures.
- b. The following are among the actions that may result in termination after a written warning, if the incident occurs in such a manner as to involve MASON or its government customer:
 - (1) Failure to meet established security standards.
 - (2) Intentional violation or neglect of security regulations or procedures contained in the Standard Practice Procedure manual of the company.

12-3 Reporting of Security Violations

It is the responsibility of each individual to report suspected or actual violations of any of the security regulations outlined in this procedure. An appropriate investigation will be accomplished by the FSO or designated representative, to identify an individual culpable for the violation. This report

Revised March 2011

shall include date, time, place, type and description of incident. The report will be sent to the culpable person's supervisor who will identify the corrective action taken in accordance with management policy. A complete report of the incident will be forwarded to the CSA by the FSO.

12-4 DOD HOTLINE

Federal Agencies maintain hotlines to provide an avenue for personnel participating in the National Industrial Security Program to report, without fear of reprisal, any known or suspected instances of security irregularities or infractions. The address and telephone number of the Hotline are:

Defense Hotline - The Pentagon Washington, DC 20301-1900
Toll Free: 1-800-424-9098
Washington Metro area: 1-202-693-5080

Revised March 2011

CHAPTER 13
AUTOMATED INFORMATION SYSTEMS

13-1 General

For the purpose of this section, Automated Information Systems (AIS) include any electronic equipment capable of recording, transmitting, storing and/or processing classified data such as computers, typewriters, calculators, test bed equipment, copiers, facsimile machines, or any other equipment or device which employs any nature of memory components and is utilized to such a degree to manipulate classified data. Specific guidelines for the use of AIS is contained in Appendix I to this SPP. MASON personnel are reminded of their obligations and responsibility to refrain from processing classified information on unclassified systems.

13-2 Conflict

In the event of a conflict between this SPP, to include Appendix I and procedures set forth in NISPOM Chapter 8, the later will be followed.

Appendix I

Laptop System Security Plan

Introduction

This document is intended to detail the security requirements and controls to comply with National Industrial Security Program Operating Manual Chapter 8 requirements for a System Security Plan (SPP). It is intended to supplement the University's Standard Practice Procedures for Security Services (MASON SPP).

1. System Identification

1.1 Security Personnel

Facility Security Officer (or designee): Keith Bushey, kbushey@Mason.edu, x3088

Information Systems Security Officer: Nicholas Clark, nclark1@Mason.edu, x1743

Principal Investigator (or designee): the system will be under the supervision of the Principal Investigator or Program Manager.

1.2 System Description

The system will consist of a laptop used as a standalone computer with multiple users, an external storage device for transporting data, and an additional external storage device for backing up data. The system will store electronic data from multiple sources to support research on the specific project. Stored data will be comprised of databases, data sets, reports, and documents. The research performed will not be classified, however the input and derivative data will be classified.

2. System Requirements Specification

2.1 Sensitivity and Classification Levels

The laptop will store data inputs and outputs with SECRET and lower classifications. All users of the system will have a minimum of SECRET level clearance. All users of the system will have a need-to-know for all of the stored data. This meets the requirements for NISPOM protection level 1, PL-1 (NISPOM 8-403) [1].

2.1.1 Formal Access Approval

a. Access to the system will be permitted only for individuals with the required clearance and authorization from the Principal Investigator.

b. The Principal Investigator will provide the Information Systems Security Officer (ISSO) with a list of authorized users and immediate notice of any changes to the list. This list will be kept in the secured storage facility with the system components.

c. The ISSO will create and update system accounts for users.

d. Physical access to the system will be coordinated with individuals with access to the secured storage facility. These individuals will be permitted to check out the system to users on the system access list. The system must be checked back in to the secured storage facility every evening.

2.2 Levels of Concern for Confidentiality, Integrity, and Availability:

	Level of Concern	Description
Confidentiality	Medium / SECRET	All users have access to all data. All users have need-to-know for all data
Integrity	Basic	Reasonable degree of accuracy required for mission accomplishment.
Availability	Basic	Information must be available with flexible tolerance for delay.

2.3 Protection Requirements and Measures

2.3.1 Audit Capability - Audit 1 (NISPOM 8-602)

a. An automated audit trail will be maintained using the native Windows operating system event logs. Logged events will include:

- i. Successful and unsuccessful logons and logouts.
- ii. Successful and unsuccessful requests to modify security related components.
- iii. Creation, deletion, and modification of user accounts.

b. Logs of user accounts and their creation/deletion will be maintained as a hard copy

c. Access to Windows event logs will be restricted to users in the Administrators group. System users will be restricted from accessing and manipulating the event logs by group policy.

d. Event logs will be reviewed regularly.

2.3.2 Data Transmission – Trans 1 (8-605)

- a. The system will be used only in approved, closed areas.
- b. The system will utilize NSA approved AES 128bit full disk encryption for stored data [2].
- c. No network access will be permitted.
- d. The wireless network interface will be physically removed.
- e. The wired network interface will be disabled.
- f. Users will not copy or move data off of the system using any means. This excludes copying data for backup purposes to marked external storage drive.

2.3.2 Access Controls – Access 1 (8-605)

- a. Physical access to the system will be restricted to authorized individuals whom hold SECRET or higher clearance.
- b. See 2.1.1 for Formal Access Approval procedures.

2.3.4 Identification & Authentication – I&A1 (8-607)

- a. All system users will be assigned a shared disk encryption password required to boot the system.
- b. All users will be assigned unique login names used for authentication. Authentication will require a combination of password and fingerprint biometric identification [3].

2.3.5 Resource Control

- a. The system and all storage devices will be used exclusively for this project. They will not be reallocated for other uses without sponsor approval.

2.3.6 Session Controls – SessCtrl 1 (8-609)

- a. User Notification:
 - i. All users will be notified prior to gaining access to the system that system usage will be monitored, recorded, and subject to audit. Users will also be notified that by

using the system, they consent to this monitoring. Notification will include warnings that the system contains SECRET classified material.

- ii. Notification will be provided through a text message window displayed prior to Windows logon. This message must be acknowledged by positive user action prior to logon.
 - iii. A notice will be displayed as the desktop background image indicating that the laptop contains SECRET classified material.
 - iv. The system and all external storage devices will contain physical markings or labels indicating that it contains SECRET classified material.
- b. Successive Logon Attempts: Since the system will operate as a standalone computer, with no remote login, no protections will be applied to disable accounts after successive failed interactive logon attempts.
- c. System Entry: The system will not be connected to a network and no remote access will be permitted. Access to the system will be restricted to interactive console logins.

2.3.7 Security Documentation – Doc 1 (8-609)

- a. This document will serve as the system security plan.

2.3.8 Separation of Function Requirements (8-611)

- a. The system does not require separation of functions at NISPOM Protect Level 1; however, the system will differentiate between permissions for administrators and regular system users.

2.3.9 System Recovery – SR 1 (8-612)

- a. In the event of a security or operational failure of the system, users shall notify the project manager or the systems administrator as soon as possible.

2.3.10 System Assurance – SysAssur 1 (8-613)

- a. The system will differentiate between administrative users and system users. Access to administrative functions, which includes account creation/modification/deletion, system policy modifications, and modification of any security components, will be restricted to administrative users.

- b. The system will use a supervisor password to protect modification of BIOS functions. BIOS authentication will utilize the internal Trusted Platform Module (TPM) chip embedded in the system. The systems administrator will keep a hard copy of the password in a sealed envelope in a secured area.
- c. The system BIOS will be configured to boot from the internal hard drive only. All other boot devices will be disabled.
- d. The physical system will never be left unattended or unsecured.

2.3.11 Security Testing – Test 1 (8-614)

- a. The systems administrator will confirm that the system operates according to this SSP.

2.3.12 Backup and Restoration of Data - Backup 1 (8-603)

- a. The system will be backed up manually, at least monthly, to an external hard drive. The external drive will be kept in the classified storage area at all times, except during backup or restores.

2.4 System-Specific Risks and Vulnerabilities

This system consists of a laptop computer and external storage devices. The portable nature of these devices makes them especially vulnerable to theft. This vulnerability will be mitigated by:

- a. Restricting use of the system to secured, closed areas.
- b. System users will be required to maintain constant supervision of all devices at all times. No component of the system should ever be left unattended.
- c. The system will employ full disk encryption using AES 128bit encryption and require a password at boot to access data on the internal hard drive [2].

2.5 System Configuration (example)

Hardware Type	Laptop Computer
Make/Model	Lenovo Thinkpad T61
Processor	Intel Core 2 Duo 2.0Ghz
Memory	2G PC2-5300 667Mhz (2DIMMs)
Display	15.4 WSXGA+ TFT
Hard Drive	Seagate Momentus FDE.2 160GB 5400RPM HDD with DriveTrust
Wireless	Removed
SmartCard	PC Cardslot/Smartcard available
Operating System	Windows XP + Service Pack 2

[1] 5220.22-M, “National Industrial Security Program Operating Manual”, 2/28/2006. Chapter 8, Information System Security

[2] The Seagate Momentus FDE.2 hard disk uses a technology called DriveTrust to encrypt the entire hard drive independent of the operating system. DriveTrust uses AES 128 bit encryption. AES is an approved cryptographic system for government systems, Federal Information Processing Standard (FIPS) 197. Seagate’s implementation using DriveTrust is certified compliant with AES according to National Institute of Standards AES Validation List <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>, certificate 587 7/2/2007. AES 128bit encryption is approved for the storage of SECRET classified materials according to The Committee on National Security Systems Policy No. 15, Fact Sheet 1.

[3] Biometric authentication using the embedded fingerprint scanner does not meet any government security requirements and is implemented only as an additional security layer.