Security Program
Standard Practice Procedures

George Mason University
4400 University Drive, MSN 6D5, Fairfax, Virginia 22030

Table of Contents

Acronyms **3**

CHAPTER 1: **4**

GENERAL SECURITY INFORMATION

CHAPTER 2: **6**

PERSONNEL SECURITY CLEARANCES

CHAPTER 3: **8**

SECURITY AWARENESS

CHAPTER 4: **9**

SAFEGUARDING CLASSIFIED INFORMATION

CHAPTER 5: **13**

REPORTING REQUIREMENTS

CHAPTER 6: **15**

CLASSIFIED VISITS

CHAPTER 7: **16**

COURIERS

CHAPTER 8: **18**

SECURITY VIOLATIONS AND INVESTIGATIONS

CHAPTER 9: **19**

AUTOMATED INFORMATION SYSTEMS

CHAPTER 10: **20**

INSIDER THREAT PROGRAM

Acronyms

AIS	Automated Information Systems
ATO	Approval to Operate
DSS	Defense Security Services
e-QIP	Electronic Questionnaires for Investigations Processing
FSO	Facility Security Officer
ISSM	Information Systems Security Manager
ITPSO	Insider Threat Program Senior Official
JPAS	Joint Personnel Adjudication System
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
ODAA	Office of the Designated Approving Authority
SPP	Standard Practice Procedures
SSP	System Security Plan
VAR	Visitor Authorization Request

Chapter 1

GENERAL SECURITY INFORMATION

I. Background

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.

Mason has a Top Secret facility clearance. A facility clearance is an administrative determination that a facility is eligible for access to classified information or award of a classified contract.

This Standard Practice Procedures (SPP) manual contains the policies and procedures 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 Mason. These procedures apply to the handling and safeguarding of classified information transmitted to or generated by Mason.

II. Facility Security Officer

Having a facility clearance means that Mason must adhere to the rules of the National Industrial Security Program (NISP). As part of the NISP, contractors such as Mason are responsible for appointing a Facility Security Officer (FSO). The FSO must be a U.S. citizen, an employee of Mason, and cleared to the level of the facility clearance. The FSO must complete the required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM and related Federal requirements for classified information.

Mason's FSO is Melissa Perez (mperez21@gmu.edu or 703-993-5522).

The FSO may appoint an Alternate FSO who has the same responsibilities under this SPP as the FSO. Mason's Alternate FSO is Nick Clark (nclark1@gmu.edu or 703-993-1743).

The FSO will be appointed by the Vice President of Research in writing, and the appointment letter will be submitted to the DSS Industrial Representative.

The FSO reports directly to the Associate Vice President of Research, Development, Integrity and Assurance and will also have unrestricted indirect reporting responsibility.

In the event the FSO is terminated, transferred, or departs Mason, the Vice President

of Research will appoint a new FSO. Prior to an anticipated departure, the incumbent FSO and their successor will:

- Review all ongoing security actions and programs at the facility, including Contract Security Classification Specifications (DD Form 254).
- Review all relevant files, records, and administrative security systems and procedures.
- Process the personnel security clearance for the successor FSO in connection with the facility clearance, if applicable.
- Establish JPAS accounts for the successor FSO.
- Take other appropriate steps to ensure a smooth transition to the successor FSO.

III. Assessments and Self-Inspections

Mason will be assessed by DSS on a yearly (or less frequent) basis. During that time, DSS Industrial Security Representatives will review our security processes and procedures to ensure compliance with the NISPOM, and interview Mason employees to assess the effectiveness of the security program. Your cooperation with DSS during the assessment is required.

The FSO will also perform a self-inspection, similar to the DSS assessment. The purpose is to self-assess the security procedures to determine the effectiveness of the security program and identify any deficiencies/weaknesses. As part of this self-inspection, Mason employees may receive a questionnaire or be interviewed. The results of the self-inspection will be briefed to Mason senior leadership and provided to DSS.

CHAPTER 2

PERSONNEL SECURITY CLEARANCES

I. Clearance Procedures

Mason employees will be processed for a personnel security clearance only when a determination has been made that access is necessary for performance on a classified contract held by Mason.

Mason will use the Joint Personnel Adjudication System (JPAS) to initiate the clearance request process. Each applicant for a security clearance must produce evidence of U.S. citizenship such as an original birth certificate or passport. Applicants must complete the Questionnaire for National Security Positions (SF-86) through OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system.

Prior to initiating the process, the FSO will notify the applicant that the SF-86 is subject to review by the FSO only to determine the information is adequate and complete, will be used for no other purpose, and is protected in accordance with the Privacy Act of 1975.

II. Clearance Notification and SF-312 NonDisclosure Agreement

When an eligibility determination is granted, the FSO shall notify the individual. If the person does not have a current Non-Disclosure Agreement or SF 312 indicated in JPAS, the FSO will witness the signature of the employee and forward the SF 312 to DSS. The FSO will file a copy inside the employee's security file.

Employees who refuse to execute SF 312 will forfeit their approval to access classified information. The FSO must inform DSS and notify the employee's supervisor of the employee's refusal.

III. Reinvestigations

Depending upon the level of access required, individuals holding security clearances are subject to a periodic reinvestigation at a minimum of every five years for Top Secret, 10 years for Secret, and 15 years for Confidential. The FSO is responsible for reviewing all access records to ensure employees are submitted for reinvestigations as required.

IV. Consultants

If consultants are supporting a classified program, Mason will hold their clearances. Consultants must comply with this SPP and the NISPOM and will be required to execute a Consultant Certificate which provides security requirements specific to their status as a consultant.

V. Non-U.S. Citizens

Non-U.S. citizens will be processed for a clearance only in those cases where the FSO and Principal Investigator determine that the individual possesses some exceptional skill or talent which is critical to the performance of a contract and where special authorization is obtained from the U.S. Government. Such individuals may be granted a Limited Access Authorization by the U.S. Government.

VI. Clearance Terminations

Upon notification of termination of a cleared employee (for any reason), the FSO will change the employee's status in JPAS. Prior to departure, the employee must ensure that all classified material within their possession has been accounted for and transferred to another appropriately cleared and authorized individual.

CHAPTER 3

SECURITY AWARENESS

I. General

The FSO is responsible for the implementation, administration, and coordination of security briefings. The FSO is responsible for ensuring all appropriate Mason employees participate in the Mason security awareness program and must retain records of all security briefings.

II. Initial Security Briefings

All cleared employees must receive an initial security briefing prior to being granted access to classified material for the first time. At a minimum, the initial briefing will include the following:

- Threat Awareness Briefing
- Defensive Security Briefing
- Overview of Security Classification System
- Employee reporting requirements
- Other material required by the NISPOM

III. Refresher Briefings

Annually, each employee will be briefed concerning responsibilities to safeguard classified information, the hostile intelligence threat and methods of operations, and insider threat. This briefing will be prepared by the FSO and provided to each employee.

IV. Debriefing

Cleared employees who are terminating (for any reason) or who will no longer hold an active clearance will be debriefed by the FSO and will sign the termination briefing. The termination briefing reiterates the individual's continuing responsibility to protect classified information.

CHAPTER 4

SAFEGUARDING CLASSIFIED INFORMATION

I. Accountability Procedures

The FSO is responsible for establishing a management system for controlling classified information in its possession in accordance with the NISPOM. Cleared personnel 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.

A. Document Control

Any classified material, regardless of classification, must be processed through an accountability system. The accountability system will record the transmission of classified material to and from Mason. Receipt and dispatch records shall be retained by the FSO for 2 years. The FSO shall maintain a copy of the inventory for five years following dispatch of the material.

The accountability system will include:

- The date of the material
- The date of receipt and return
- The classification
- An unclassified description of the material
- The identity of the person from whom the material was received or to whom the material was dispatched

All classified material, regardless of classification, being transmitted from the facility will be packaged and appropriately dispatched by the FSO.

B. Receipt of Incoming Classified Material

All incoming classified material that is not hand couriered shall be mailed to George Mason University, Attn: Facility Security Officer, Post Office Box 319, Fairfax Station, Virginia 22039. The mailbox will be checked periodically by an appropriately cleared, designated individual or the FSO. All incoming classified material will be given immediately to a specifically designated individual or to the FSO.

C. Identification Markings

All classified material, regardless of the form in which it appears, must 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.

II. Safeguarding Classified Materials

The FSO has established control areas to adequately safeguard classified material. There is a sign conspicuously posted at the front and rear entrances of control areas stating that all persons who enter or exit the area are subject to an inspection of their personal effects. Employees must challenge unauthorized personnel found in an area containing classified information and must report such incidents to the FSO immediately.

Employees must choose private office space or other approved areas to perform classified work, where access by unauthorized personnel can easily be prevented. Should an unauthorized person enter your work area while classified work is in progress, the classified material should be covered or turned over. Never place classified material inside a desk or other unapproved container for any length of time.

Cleared employees must ensure that classified discussions do not take place over unsecure telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons. If you need to have a classified discussion, contact the FSO to determine which areas have been designated for classified discussions.

Do not provide classified information to another individual unless that person has the proper level security clearance, and the need-to-know for the information involved. Physically check the person's identity by personally reviewing an official form of photo identification such as a driver's license, passport, or credentials. Compare the photo against the individual's appearance. Confirm the person's clearance level with the FSO. Before releasing classified information to anyone or before allowing unescorted access to a closed or restricted area, identify the most restrictive classification involved and compare it to the person's clearance level.

Do not remove classified material from Mason without prior approval from the FSO.

A. Storage of Classified Material

Storage containers for classified material must conform to the specifications for safes and locked filing cabinets. The FSO must maintain all storage devices in accordance with the NISPOM.

Security containers, closed areas, cabinets, and other authorized storage containers must be kept locked when not under the direct supervision of an authorized person.

When in use, classified information must be under the continuous supervision of an authorized user.

All classified material must be secured in the appropriate security container at the end of each working day. Security personnel will check classified storage containers at the end of each business day to ensure that the contents are properly secured.

The FSO maintains a secure listing of all combinations. The written record of the combination must be safeguarded in a classified container in accordance with the highest level of classified material retained in the container. A minimum number of authorized persons will be permitted to know the combinations for the security containers.

Combinations must be changed by the FSO whenever an employee who has the combination is debriefed or terminated. In addition, combinations will be changed if a security compromise occurs or as instructed within the NISPOM.

B. Pre-Publication Release

Classified material must not be published or distributed without the prior review and written approval set forth in the DD254 for that specific program. The FSO and the Principal Investigator are responsible for coordinating these activities.

C. Copying Classified Material

Before any classified material, regardless of format, is copied, the FSO must be informed of the intent to copy the material. Classified copies can only be made on equipment that has been designated and authorized for classified reproduction.

Mason personnel must keep reproduction of classified material to a minimum; should only make copies in response to a contractual requirement such as in the performance of a deliverable; and must treat reproduced copies of classified material with the same protections as the originals.

D. Safeguarding Classified Information in Emergency Situations

In emergency situations, it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency situation is the safety of personnel. Do not risk your life or the lives of others in order to secure classified information. For example, in case of fire, you may need to immediately exit the facility with the classified materials in your possession. Seek out the FSO for further instructions once in a safe environment.

III. Disposition and Retention of Classified Material

Classified information no longer needed must be returned to the U.S. Government for appropriate disposition. No classified information will be retained beyond contractual requirements without retention authority from the official source as identified within the DD254. The FSO establishes procedures for annual review of all classified holdings to reduce classified inventories to a minimum necessary for effective and efficient operations.

Mason personnel who wish 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 U.S. Government does not advise otherwise. If retention is required beyond the 2-year period, written authorization must be received by the U.S. Government.

CHAPTER 5

REPORTING REQUIREMENTS

I. General

All cleared employees must report any of the following information to the FSO. The FSO will notify DSS and, as required in the NISPOM, the FBI as well.

A. Espionage/Sabotage

Cleared personnel must report any information concerning existing or threatened espionage, sabotage, terrorism, or subversive activities to the FSO.

B. Suspicious Contacts

Cleared personnel must report all suspicious contacts to the FSO. Suspicious contacts are efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, cleared employees must report any contacts with known or suspected intelligence officers from any country, or any contact which suggests the employee may be the target of an attempted exploitation by a foreign intelligence service.

C. Adverse Information

Cleared personnel must report adverse information regarding themselves or another cleared individual to the FSO. Adverse information is any information regarding a cleared employee or employee in process for a clearance which suggests that their ability to safeguard classified information may be impaired or that their access to classified information may not be in the interest of national security. Reports should not be based on rumor or innuendo. Reportable adverse information includes:

- Relationships with any known saboteur, spy, or secret agent of a foreign nation
- Serious mental instability or treatment at any mental institution
- Use of illegal substances or excessive use of alcohol or prescription drugs
- Excessive debt, including garnishments on employee's wages
- Unexplained affluence
- Unexplained absence from work for periods of time that is unwarranted or peculiar
- Criminal convictions involving a gross misdemeanor, felony, or court martial
- Violations or deliberate disregard for security regulations or procedures
- Unauthorized disclosure of classified information

D. Loss, Compromise, or Suspected Compromise of Classified Information

Cleared personnel must immediately report the loss, compromise, or suspected compromise of classified information to the FSO.

E. Security Violations

Cleared personnel must report any failure to comply with a requirement of this SPP or of the NISPOM to the FSO.

F. Personal Changes

Cleared personnel must report personal changes including:

- Change in name
- Termination of employment
- Change in citizenship
- No longer need access to classified information
- No longer wish to be processed for a personnel clearance or continue an existing clearance

G. Foreign Travel

All employees must notify the FSO in advance of anticipated foreign travel. The notification must include the travel dates, destination(s) and purpose of travel.

The FSO periodically will remind cleared employees of the risks involved in foreign travel. If an employee wishes to receive a classified or unclassified briefing prior to travel, the FSO will arrange this briefing.

Cleared personnel must contact the FSO upon their return if they had any suspicious foreign contacts while traveling.

All cleared employees must provide the FSO with copies of any business cards received from foreign parties (received either while on international travel or otherwise). The business cards must be provided to the FSO even if the employee does not intend to have future contacts with the foreign person.

II. DOD HOTLINE

Federal Agencies maintain hotlines to provide an avenue for personnel participating in the NISP 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

CHAPTER 6

CLASSIFIED VISITS

The FSO is responsible for approving classified visits to Mason.

I. Incoming Visits

All incoming classified visits must be approved in advance by the FSO. Visitors are responsible for ensuring that a Visit Authorization Request (VAR) is submitted in JPAS prior to the visit. The FSO will verify each visitor's security status in JPAS prior to allowing classified access. All visitors requiring access to classified information must possess security clearances commensurate with the classification of the information sought.

The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Approval of the visit does not imply authorization for the visitor to remove or copy classified material.

II. Outgoing Visits

When it becomes necessary for cleared Mason employees to visit other cleared contractors or Government agencies and access to classified information is anticipated, employees must notify the FSO in advance and provide information concerning the contractor or agency to be visited, including the SMO, the date(s) of the visit, the reason for the visit, and the person to be contacted (including phone number). Ample time must be allowed to permit the visit authorization request to be submitted via JPAS to the contractor/agency and processed by the host's visitor control.

III. Visitor Records

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, the date(s) of their visit, and who they visited at Mason.

CHAPTER 7

COURIERS

I. Courier Appointments, Briefings and Responsibilities

A courier is a cleared employee of Mason who has been authorized by the FSO to transmit classified material to its destination.

Certain employees who have a repetitive need to transport classified materials may be designated as couriers. Couriers must possess a final personnel security clearance at least at the highest classification level of the material they will transport.

Couriers will be briefed on their responsibility to safeguard classified information and will sign a Courier Briefing.

Couriers will be provided with a Courier Authorization Card not to exceed 12 months. When employees are transporting classified materials, they must have their Courier Authorization Card and their Mason ID with them.

Couriers must retain personal possession of the classified materials at all times and are not permitted to make any unauthorized stops that would leave the material unprotected or susceptible to compromise. Couriers may make arrangements for overnight storage at a U.S. Government installation or other cleared facility that has appropriate storage capability.

Couriers will contact the receiving facility in advance and ensure that arrangements are made to receive the material.

Intoxicants or drugs that may impair the individual's judgment may not be used while an individual is performing courier duties.

II. Transmittal Procedures

The FSO and courier must ensure that the proper marking, accountability, and packaging requirements are accomplished prior to hand carry.

The FSO and courier will create an inventory of the items to be hand carried, in accordance with the NISPOM, and the courier will keep a copy of the inventory during transport. The courier will not accept custody or release of classified material without the exchange of receipts.

III. Transport Via Commercial Aircraft

If an employee needs to transport classified material on commercial aircraft, they must receive approval from the FSO.

The courier must possess the prescribed courier identification and a courier authorization letter, as described in the NISPOM.

Couriers undergo normal airline screening procedures.

- In order to allow for screening, packages should contain no metal (including paper clips or binders) which might inhibit processing by detection devices at the airport.

- Couriers may need to make special arrangements with the air carrier for items that cannot undergo routine screening due to size, weight or other characteristics.

- If airport security personnel are unable to screen the classified material and request that the courier open the package, the courier must notify security personnel that the carry-on items contain U.S. Government classified information and cannot be opened.

- Under no circumstances may the classified material be opened by either the courier or airport personnel.

CHAPTER 8

SECURITY VIOLATIONS AND INVESTIGATIONS

I. Security Violations

A security violation is the failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information. Failing to comply with the NISPOM or any procedures contained in this Standard Practice Procedure may result in disciplinary action, up to and including termination. Any person who has knowledge of a potential security violation must immediately report it to the FSO.

II. Investigations

The FSO is responsible for conducting initial administrative inquiries and other preliminary investigations when a violation is suspected.

The FSO will conduct an appropriate investigation to identify what has occurred, how it occurred, and who is responsible or involved and will make a determination of whether a violation occurred.

If the preliminary inquiry confirms a violation, the FSO will prepare an initial report for DSS and continue the investigation.

A final report will be submitted to DSS in accordance with the NISPOM.

CHAPTER 9

AUTOMATED INFORMATION SYSTEMS

I. Requirements for Use of Classified AIS

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 used to manipulate classified data. Use of any AIS for classified processing is permitted only under a System Security Plan (SSP) that has been approved by DSS. Mason personnel are prohibited from processing classified information on unclassified systems.

The operation of AIS for processing classified information is possible only under specific circumstances:

- The sponsoring agency has authorized classified research activity and included a DD-254 in the contract provided to the Office of Sponsored Programs.
- There is a clear need to use classified computing on campus for completion of the work.
- Hardware and software or funding to procure hardware/software for the AIS is provided in the contract.

If these requirements are met, then the Principal Investigator of the project must work with the FSO and the appointed Information Systems Security Manager (ISSM) to complete the process of procuring, configuring, and obtaining approval to use an AIS for classified computing from the DSS Office of the Designated Approving Authority (ODAA).

There is a specific and detailed process for obtaining an Approval to Operate (ATO) for classified AIS. The process is described in the "DSS ODAA Process Manual" available from the DSS Website http://www.dss.mil/isp/odaa/request.html. **No AIS can be used to process classified information until an ATO/IATO has been provided by DSS**. The ISSM will handle interaction with DSS ODAA to initiate and complete the approval process.

II. NISPOM Chapter 8 Compliance

As a result of the DSS approval process, a detailed SSP and Profile will be present for each AIS. The SSP will describe all of the controls necessary to comply with the NISPOM Chapter 8 requirements. The ISSM will be responsible for managing and overseeing compliance with the SSP. The ISSM will brief each project member designated as an authorized user of the system. Authorized users are responsible for complying with all of the security requirements of the system and the SPP.

CHAPTER 10

INSIDER THREAT PROGRAM

I. General

NISPOM Change 2 requires contractors such as Mason to establish and maintain an insider threat program to detect, deter and mitigate insider threats. Insider threat is defined as "the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information."

Specifically, the program must gather, integrate, and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines that indicate of a potential or actual insider threat to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risk of an insider threat.

Mason is required to self-certify to DSS that a written Insider Threat Program has been implemented and is current.

II. Insider Threat Program Personnel

a. Insider Threat Program Senior Official (ITPSO)

(1) Mason's President, or the President's designee, will appoint a senior official who is a U.S. citizen and appropriately cleared in connection with the Facility Clearance to serve as the Insider Threat Program Senior Official (ITPSO). The ITPSO is responsible for establishing and executing the insider threat program and serves in a position within Mason that has the authority to provide management, accountability and oversight of the program. The ITPSO will be designated as Key Management Personnel.

(2) Termination, Transfer or Departure of ITPSO

(i) In the event of a termination, transfer or departure of the ITPSO, the President or the President's delegate must immediately select a new ITPSO. The selection should occur as soon as the anticipated departure of the incumbent becomes known. Prior to an anticipated departure, the incumbent ITPSO and his/her successor will conduct a review of the insider threat program and resolve any open action items.

(ii) In the temporary absence, sudden or unexpected departure of the ITPSO, or if the new ITPSO's clearance is pending, the FSO will act as ITPSO unless the President or the President's delegate elects to assign such responsibilities to another individual who is cleared in connection with the facility clearance.

b. Insider Threat Program Working Group

(1) Members of the insider threat program working group ("Working Group") will be responsible for gathering, integrating and reporting relevant and credible information regarding potential insider threats to the ITPSO and FSO. This Working Group will include the ITPSO, FSO, and representatives from Human Resources, IT Security, Compliance, Ethics & Diversity, and the Mason Police Department. The Working Group will meet on a regular basis, as needed.

III. Reporting

Employees are required to report to the FSO or ITPSO relevant and credible information regarding a cleared employee who exhibits any of the indicators listed in the personnel security adjudicative guidelines found in §32 CFR Part 147 (https://www.gpo.gov/fdsys/pkg/CFR-2012-title32-vol1/xml/CFR-2012-title32-vol1-part147.xml). The indicators are:

Guideline A—Allegiance to the United States. This includes involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means; or association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts

Guideline B—Foreign influence. This includes when an immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country.

Guideline C—Foreign preference. This includes performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States. Examples include the exercise of dual citizenship, possession and/or use of a foreign passport, military service for a foreign country, seeking or holding political office in the foreign country, or voting in foreign elections.

Guideline D—Sexual behavior. This includes sexual behavior of a criminal nature; compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior; sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; or sexual behavior of a public nature and/or that which reflects lack of discretion or judgment

Guideline E—Personal conduct. This includes conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Examples include refusal to undergo or cooperate with required security processing or to complete required security forms; the deliberate omission, concealment, or falsification of relevant and material facts on any personnel security questionnaire; or deliberately providing false or misleading information concerning relevant and material matters to an investigator in connection with a personnel security or trustworthiness determination.

Guideline F—Financial considerations. This includes deceptive or illegal financial practices (for example, embezzlement, employee theft, check fraud, income tax evasion); unexplained affluence; or financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Guideline G—Alcohol consumption. This includes alcohol-related incidents away from work, such as driving while under the influence; alcohol-related incidents at work, such as reporting for work in an intoxicated or impaired condition, or drinking on the job; medical diagnosis of alcohol abuse or alcohol dependence; or habitual or binge consumption of alcohol to the point of impaired judgment.

Guideline H—Drug involvement. This includes illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or medical diagnosis of drug abuse or drug dependence.

Guideline I—Emotional, mental, and personality disorders. This includes a medical opinion that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability; a pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior; or information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Guideline J—Criminal conduct. This includes a single serious crime or multiple lesser offenses.

Guideline K—Security violations. This includes unauthorized disclosure of classified information that is deliberate or multiple or due to negligence.

Guideline L—Outside activities. This includes *any service, whether compensated, volunteer, or employment with a* foreign country, any foreign national, or a representative of any foreign interest.

Guideline M—Misuse of information technology systems. This includes illegal or unauthorized entry into any information technology system; illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system; removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations; or introduction of

hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Upon receipt of such information, the FSO and ITPSO will review to determine if it must be reported to the Government and will report as required by the NISPOM. The FSO and ITPSO will notify campus police when a report is made to the Government if it involves an employee who presents a danger to the university community. They will also determine what actions, if any, need to be taken to prevent any immediate security violations and will implement those actions with assistance from other units on campus, as needed (such as Human Resources, etc.).

The FSO and ITPSO will also initiate any mitigation steps required to reduce the risk, such as providing refresher training to the employee or enlisting other departments, such as HR, to determine if any university programs or resources might be available to assist the employee.

IV. Training

a. Insider Threat Program Personnel: The ITPSO, FSO and members of the Working Group are required to complete insider threat training that describes counterintelligence and security fundamentals, including applicable legal issues; procedures for conducting insider threat response actions; applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information; and applicable legal, civil liberties, and privacy policies.

   Any employees assigned to the Working Group after November 30, 2016 must complete the insider threat program training within 30 days of being assigned those duties.

   All members of the Working Group must complete insider threat program training annually.

b. Cleared Employees: Each cleared Mason employee or consultant is required to complete insider threat awareness training that describes the importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee; methodologies of adversaries to recruit trusted insiders and collect classified information; indicators of insider threat behavior, and procedures to report such behavior; and counterintelligence and security reporting requirements, as applicable.

   Cleared employees must complete the insider threat program training prior to being granted access to classified information. Cleared employees already in access at the time of the issuance of NISPOM Change 2 must complete the training prior to May 31, 2017.

All cleared employees must complete insider threat program training annually.

c. Training Records: The FSO will create and maintain training records of all employees who are required to take insider threat program training, including initial and annual refresher training. The FSO will also include insider threat information in the annual security refresher briefing.

V. Self-Inspections of the Insider Threat Program

The FSO and ITPSO will conduct self-inspections of the insider threat program on an annual basis. The FSO will prepare a formal report for the ITPSO to review which will include any findings and the resolution of any issues discovered. A copy of the self-inspection report will be made available to the DSS Representative upon request.

The FSO and ITPSO will notify Mason's President of the findings of the self-inspection. The President will certify in writing to the DSS Representative that the self-inspection occurred, that he or she was briefed on the self-inspection, and that appropriate corrective actions (if applicable) were taken.

VI. Classified Information Systems

In accordance with Chapter 9, any Automated Information Systems used to process classified information will be configured for and operated under an approved System Security Plan approved by Defense Security Services (DSS) Office of the Designated Approval Authority (ODAA). The DSS ODAA Process Manual describes three key initiatives to support insider threat programs related to the use of information systems.

a. User Training: All classified information system users will be trained on their responsibilities including information related to this Insider Threat Program. This training will be conducted at least annually with regular information system security briefings.

b. Use of System Logon Banners: Classified information system users will be notified at logon that their activity is subject to monitoring as required in the approved SSP notification banner.

c. User Activity Monitoring/Auditing: The Information System Security Manager (ISSM) or designated Information System Security Officer (ISSO) will monitor and review user activity for the detection of insider threat activity and protect the methods used and information obtained. The audit trails will be analyzed at least once per calendar week. The auditing configurations and controls will be configured as described in the approved SSP.