Transportation Security Administration

Office of Human Capital

TSA MD 1100.73-5, Handbook

Employee Responsibilities and Code of Conduct

Policy Effective:	May 21, 2009
Handbook Published:	May 21, 2009
Handbook Revised:	September 30, 2013

Signed

Karen Shelton Waters
Assistant Administrator for Human Capital

Transportation Security Administration

Summary of Changes:

Handbook title changed from Employee Responsibilities and Conduct to Employee Responsibilities and Code of Conduct.

Section A, Definitions, added definition of Nexus; modified reference to Executive Order 12958 to 13526.

Section B, Safeguarding and Use of Information, Documents, and Records, added references to TSA MD 2810, *SSI Program*, and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*.

Section D, Use of Federal Equipment, Property, and Personnel, added the use of government-issued electronic communication devices subject to restrictions; changed TSA Information Security Policy Handbook to TSA Information Assurance Handbook; amended to state that separated employees must return their travel card and/or purchase card to their respective Travel Card Organization Program Coordinator; "identification card" changed to "identification media" for consistency.

Section F, Providing Statements and/or Testimony, clarified responsibilities of employees that they must cooperate fully with inquiries initiated by supervisors, Office of Inspection, DHS Office of Inspector General, and that confidentiality does not extend to concerns regarding access to national security information; a note concerning who may issue a Garrity or Kalkines warning added; added additional language regarding the issuance of a Garrity warning.

Section M, Eliminating Discrimination and Creating a Model Work Environment, added references to the Unitary Dispute Resolution System.

Section O, Alcohol and Drugs, specified that the use of marijuana is prohibited by Federal law; added language stating that employees may not leave the testing site without permission prior to completing the testing.

Section T, Canvassing, Soliciting, or Selling, solicitation for a voluntary contribution clarified.

Section U, Gambling and Related Activities, added the prohibition of gambling using government resources and government vehicle.

Section Y, Gifts From Non-Federal Sources, added reference to the TSA Guide to Major Ethics Rules.

Section AA, Advertisements, Endorsements, and Referrals, employees may not use their position for the private gain of other individuals such as friends and relatives.

Section BB, Unauthorized Absences and Tardiness, added reference to the Collective Bargaining Agreement.

This Handbook and all related Attachments and/or Appendices contain stipulations to implement the provisions of TSA MD 1100.73-5, Employee Responsibilities and Code of Conduct. Until TSA MD 1100.73-5 is rescinded, the Management Directive, Handbook, and any Attachments and/or Appendices are considered TSA policy, and must be applied accordingly.

TABLE OF CONTENTS

Section **Page**

A. **Definitions:**

(1) Classified Information: Also known as Classified National Security Information, information that has been determined, pursuant to Executive Order 13526, as amended, or any predecessor or successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(2) For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) Information: FOUO and SBU information is not to be considered classified information. Rather, it is unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the National interest. Information impacting the National Security of the United States and classified as Confidential, Secret, or Top Secret under Executive Order 13526, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered to be FOUO or SBU.

(3) Nexus: For the purposes of an adverse or disciplinary action, it is a connection between a legitimate government interest and the employee's unacceptable performance, conduct, or matter that is the basis for the adverse or disciplinary action. Nexus is presumed when the basis for adverse or disciplinary action is an employee's unsatisfactory job performance or on-duty misconduct, or in the case of criminal activity or other egregious or especially notorious misconduct. However, actions also may be taken against an employee because of off-duty misconduct where there is a nexus between the conduct and the TSA mission and/or effective operation of the agency.

(4) Personally Identifiable Information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S.

(5) Sensitive PII: Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any grouping of information that contains the individual's name or other unique identifier plus one or more of the following elements:

(a) Driver's license number, passport number, or truncated SSN (such as last-4 digits);

(b) Date of birth (month, day, and year);

(c) Citizenship or immigration status;

(d) Financial information such as account numbers or Electronic Funds Transfer information;

(e) Medical information; or

(f) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PINs).

NOTE: Other PII may be "sensitive" depending upon its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number.

(5) Sensitive Security Information (SSI): As defined in 49 C.F.R. Section 1520.5, information obtained or developed in the conduct of security activities, including research and development, the disclosure of which Department of Homeland Security (DHS)/TSA has determined would (1) constitute an unwarranted invasion of privacy (including , but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

B. **Safeguarding and Use of Information, Documents, and Records:**

(1) Employees shall ensure the proper handling of government records and shall not disclose or discuss the content of any classified documents, Sensitive PII, SSI, or FOUO/SBU information unless specifically authorized to do so. Refer to TSA MD 2810.1, *SSI Program*, and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*, for additional information.

(2) Classified information must not be disclosed to anyone without the appropriate security clearance and an official need to know the information.

(3) No employee shall disclose proprietary or source-selection information directly or indirectly to any person other than a person authorized by the Administrator or the contracting officer to receive such information. An employee who does not know whether information is proprietary or source-selection information, or who does not know whether he or she may disclose or receive such information, has an affirmative obligation to inquire of the contracting officer or the Office of Chief Counsel (OCC) as to whether the information is proprietary or source-selection-sensitive.

In addition, employees shall not:

(a) Release any official information in advance of the time prescribed for its authorized issuance;

(b) Use for private purposes, or permit others to use or have access to, any official information not available to the general public;

(c) Remove official documents or records from files for personal or inappropriate reasons. Falsification, concealment, mutilation, destruction, or unauthorized removal of official documents or records, either electronic or hard copy, is prohibited by law and is subject to disciplinary action, arrest, and/or prosecution; and

(d) Disclose information, the release of which would be covered under the provisions of the Privacy Act (5 U.S.C. § 552a), or Freedom of Information Act, (5 U.S.C. § 552, as amended) except as authorized.

C. **Safeguarding Public Funds:**

(1) All employees whose duties involve the expenditure of public funds must have knowledge of and observe all applicable legal requirements and restrictions. In addition, employees are expected to exercise sound judgment in the expenditure of such funds.

(2) Employees must not make unauthorized commitments. An agreement entered into by a TSA employee without authority to enter into agreements on behalf of TSA is an unauthorized commitment; only contracting officers and other designated employees, acting within the scope of their authority, may enter into contracts or other agreements and expend funds on behalf of the Government. Unauthorized commitments are a serious violation of fiscal law and statutes. Persons who enter into unauthorized commitments may be held personally liable. Management officials shall make every effort to prevent unauthorized commitments.

(3) If a legal determination is required on these matters, contact OCC.

D. **Use of Federal Equipment, Property, and Personnel:**

Employees may not use or permit others to use federal equipment, property, time, or personnel; including but not limited to: typing assistance, computer hardware, software, telecommunication capabilities, duplicating services, mail services (internal and external), TSA letterhead or chauffeur services, for other than official business or officially approved or sponsored activities or purposes.

(1) Telephones: Government telephones are for conducting official business. Employees are permitted to make occasional and reasonable personal calls that are of limited duration if they do not interfere with an employee's official duties or result in unreasonable cost to the government, such as brief calls within the local commuting area to locations that can only be reached during working hours (e.g., car repair shop, doctor) or to their residence within the local commuting area (e.g., to arrange

transportation, check on a sick family member). Employees may not make personal long distance calls at government expense except in an emergency. Discussions relating to classified information must be conducted using secure equipment only, e.g., Secure Telephone Unit (STU) or Secure Terminal Equipment (STE), and in accordance with approved procedures.

(2) Email: The government e-mail system is provided for the conduct of official TSA business. However, limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of network services.

(a) Employees are prohibited from sending e-mail or enclosures that are obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable. Under no circumstances shall the government e-mail systems be used to foster commercial interests, individual profit, partisan political endeavors, private fund raising, or passing chain letters. Refer to TSA Information Assurance Handbook for additional information.

(b) Email shall not contain any inappropriate messages that ridicule, or that may be offensive to others based on race, religion (e.g. religious or biblical references), color, sex, age, disability, national origin, sexual orientation, marital or parental status, or genetic information.

(3) Electronic communication devices, including but not limited to cellular phones, pagers, and Blackberry devices: Electronic communication devices are for conducting official TSA business. The use of such devices shall be consistent with assigned duties and responsibilities or consistent with the official business interests of TSA or other authorized purposes. An employee's use of electronic communication device must not adversely reflect on TSA or negatively impact its ability to discharge its mission, cause embarrassment to the agency, or cause the public and/or TSA to question the employee's reliability, judgment or trustworthiness. The use of government-issued electronic communication devices are subject to the restrictions listed in D(2) above.

(a) Texting while driving:

(i) Employees shall not engage in text messaging[1] when using a TSA owned electronic communication device while driving[2].

[1] For the purposes of this directive text messaging refers to reading from or entering data into any handheld or other electronic device, including for the purpose of texting, e-mailing, instant messaging, obtaining navigational information, or engaging in any other form of electronic data retrieval or electronic data communication. The term "text messaging" does not include the use of a cell phone or other electronic device for the limited purpose of entering a telephone number to make an outgoing call or answering an incoming call. The term also does not include glancing at, or listening to, a navigational device that is secured in a commercially designed holder affixed to the vehicle, provided that the destination and route are programmed into the device either before driving or while stopped in a location off the roadway where it is safe and legal to park.

NOTE: Certain employees, devices, or vehicles that are engaged in or used for protective law enforcement, or national security responsibilities, or on the basis of other emergency conditions are exempt from the above requirements. Texting while driving shall only be used as a tool of last resort when all other means of law enforcement communications are unavailable.

(ii) Employees are personally liable for any driving citations or sanctions due to violations relating to texting while driving.

(iii) Employees may also be subject to administrative action resulting in any violation as stated above.

(b) The use of the video camera in these devices shall be in accordance with the performance of the employee's duties. The camera function may not be used to take and disseminate personal photographs.

(c) Employees may not download applications or feature functionalities such as ring tones or games.

(d) Text message notifications for personal use are prohibited.

(e) Employees may be held personally liable or accountable for any unauthorized or unofficial use of electronic communication devices.

(f) Contents contained in electronic communication devices are the property of TSA.

(g) Employees are subject to unannounced periodic monitoring of electronic communication devices to ensure that the employee is not using government time, equipment, property, or personnel in any prohibited activity, including activity that would discredit TSA.

(h) A TSA supervisor or manager may request another TSA employee's call detail records, emails, text messages, IM records, and other data, as appropriate. Requestors must submit TSA Form 1409, *IT Service Request*, with a written statement and two signatures from Approving Authorities (Division Directors and above) to the TSA Office of Information Technology (OIT) Information and Assurance Cyber Security Division (IAD) for processing.

(4) Internet access/use: While on-duty and/or while using government supplied resources

[2] Driving is defined as operating a motor vehicle on an active roadway with the motor running, including while temporarily stationary because of traffic, a traffic light or stop sign, or otherwise.

(including, but not limited to, desk top computers, laptop computers, cell phones, Blackberry devices), internet access/use shall be consistent with assigned duties and responsibilities or consistent with the official business interest of TSA or other authorized purposes. Limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of services. Access of inappropriate sites is prohibited. These locations include sites that are obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable. Under no circumstances shall access to the internet be used to foster commercial interests or individual profit. Refer to TSA Information Assurance Handbook for additional information.

(a) Use/access must not adversely reflect on TSA or negatively impact its ability to discharge its mission, cause embarrassment to the agency, or cause the public and/or TSA to question the employee's reliability, judgment or trustworthiness.

(b) Employees are subject to unannounced periodic monitoring of internet access/use to ensure that government time, equipment, property, or personnel are not used in any prohibited activity, including activity that would discredit TSA. This includes the use of government laptops used to connect to prohibited sites.

(c) Prohibited or non-permissible access/use includes, but is not limited to:

(i) Seeking, transmitting, collecting, storing, or viewing material that is discriminatory, defamatory, or of a sexual and/or harassing nature. This includes accessing internet sites for the purpose of viewing and/or downloading pornographic pictures, videos, and related material. Accessing these sites may result in disciplinary action, up to and including removal, and possible criminal sanctions;

(ii) Accessing internet sites for the purpose of engaging in online gambling, e.g., poker games, sports events, or other related activities;

(iii) Broadcasting or posting inappropriate messages or materials that ridicule, or that may be offensive to others based on race, religion, color, sex, age, disability, national origin, sexual orientation, marital or parental status, or genetic information;

(iv) As defined elsewhere in this handbook, participating in hate groups or organizations that engage in criminal or other notorious activity;

(v) Concealing or misrepresenting user identity or affiliation;

(vi) Pursuing private commercial activities or profit-making ventures, fundraising, or partisan political activities. This restriction applies to

activities that benefit the employee or to activities that benefit another person or group selected by the employee without authority;

(vii) Divulging any unauthorized information related to DHS or TSA on non-government websites;

(viii) Processing classified national security information on computers connected to the agency local area network (LAN) or on electronic communication device; or

(ix) Creating personal web pages or posting content to 'blogs,' or other types of internet communication, the content of which constitutes non-permissible use.

NOTE: An employee's **off-duty** access/use must not adversely reflect on TSA or negatively impact its mission, cause embarrassment to the agency, or cause the public and/or TSA to question the employee's reliability, judgment, or trustworthiness. The above non-permissible or prohibited use/access is applicable while off duty and/or while using non-government supplied resources if an employee's off-duty internet access/use is identified with, or contains references to TSA in a manner that may reasonably imply a connection between TSA and the internet access/use.

(5) Personal Mail: Employees may not have personal mail directed to their place of employment[3].

(6) Government Postage: Personal use of U.S. Government-furnished postage - either metered or stamps - is prohibited. Personal use of other mailing services paid for by TSA is also prohibited. Employees may not use any form of government-supplied postage or mailing service for any personal or other non-approved purpose; this includes submitting job applications or mailing holiday or greeting cards. Employee organizations and/or morale groups and their members are also prohibited from using Government or TSA paid mailing services to distribute organizational information or conduct organizational business.

(7) Fiduciary Cards: Employees are prohibited from using government-provided purchase cards, fleet cards or travel cards for personal use or other non-official or unauthorized purposes. Employees to whom such cards have been issued must become familiar with the provisions of applicable TSA, DHS, and government policies. Employees are subject to TSA MD 1000.5, *Government Travel Cards*.

(a) Employees should seek reimbursement of legitimate official business

[3] An exception to this prohibition is for employees posted or on temporary duty in foreign locations where government mail services have been established for security and safety reasons. See DHS MD 0590, *Mail Management Program*.

expenses within five working days after completion of a trip or period of travel, or every 30 days if the employee is on continuous travel status.

(b) Employees are required to maintain their government credit card accounts in good standing and to make timely payment in full of outstanding balances.

(c) Employees who are separated from TSA are responsible for returning their government-provided purchase card and/or travel card to their respective Travel Card Organization Program Coordinator.

(8) Government Vehicles and Other Passenger Carriers:

(a) Employees who willfully use or authorize the use of a passenger carrier, owned or leased by the Government for other than official purposes shall be suspended without pay for at least one month (30 days), or longer as warranted, or removed from office in accordance with 31 U.S.C. § 1349. Passenger carriers include: motor vehicle, aircraft, boat, ship, or other similar means of transportation owned or leased by the Government. Refer to TSA MD 200.53, *Motor Vehicle Fleet Management*, and TSA MD 200.59, *Home-to-Work Transportation* for additional information.

(b) Employees shall not engage in text messaging when driving a Government vehicle or when driving a personal vehicle while on official TSA business. Certain employees are exempt from this provision as stated above in D(3).

(9) Employee Identification Cards, Uniform Items, Badges, Credentials, Facility Access Cards (including Security Identification Display Area (SIDA) badges), and other Similar Media (for the purposes of this sub-section "identification media"):

(a) Employees will use official (TSA or DHS issued or authorized) identification media only for official or other permissible purposes. Employee use of official identification media must comply with applicable requirements and restrictions, including DHS MD 11010.1, *Issuance and Control of Credentials*, and those issued by the program office responsible for the media in question. Applicable requirements and restrictions include, but are not limited to, a prohibition against allowing another individual to use an employee's identification badge, a requirement to wear, and visibly display an employee identification badge while on duty, and a prohibition from facility access during non-duty hours unless authorized.

(b) Employees are prohibited from using private identification media for purposes other than those for which the media was issued. In this context, private identification media means identification media issued by a non-governmental entity in connection with that entity's legitimate interests. For example, attempting to use an access card issued by a private employer to gain entrance to TSA space, although the user is a TSA employee, is

prohibited.

(c) Employees must not obtain, possess, display, transfer to another, or otherwise use fraudulent identification media.

(d) In the event that identification media is lost or stolen:

(i) Notify the Transportation Security Operations Center (TSOC: 703-563-3240) following awareness of the loss or stolen item;

(ii) Submit a request to the affected employee's local Human Resources Specialist or Business Management Office for reporting the incident in the Performance and Results Information System (PARIS); and

(iii) Make a report of the missing item to the local Police Department in the jurisdiction where the identification media was lost or stolen.

NOTE: A replacement identification media will not be provided by Physical Security Section until the aforementioned steps are fulfilled.

E. **Observing Safety Regulations, Rules, and Instructions:**

Employees must observe all rules, signs and instructions relating to personal safety in the workplace. Employees must report potentially unsafe or unhealthy working conditions and/or practices to their immediate supervisor (or any supervisor or management official in the chain of supervision), or to the appropriate TSA safety and health official, and must cooperate fully with TSA's safety staff. Employees must:

(1) Report accidents involving injury to persons or damage to property or equipment;

(2) Use required protective clothing or equipment;

(3) Take applicable precautions to ensure the safety of personnel, and prevent injury to personnel or damage to property/equipment;

(4) Wear available safety/seat belt while using a motor vehicle for official Government business;

(5) Report any operational error or deviation from safety regulations, rules, or instructions;

(6) Evacuate the premises during a fire alarm/drill or other order to vacate a work site and otherwise abide by the directions of a floor warden, safety, security or management official; and

(7) Perform work-related activities in a safe and prudent manner.

F. **Providing Statements and/or Testimony:**

(1) Employees must cooperate fully with all TSA and DHS investigations and inquiries, including but not limited to inquiries initiated by supervisors and management officials, OOI or DHS OIG, unless a *Garrity* warning is issued to the affected employee. (**NOTE:** This warning may only be issued by authorized OOI or DHS agents). See F(5) below for additional information. This includes providing truthful, accurate, and complete information in response to matters of official interest, and providing a written statement, if requested to do so. Employees must follow established TSA and DHS procedures when responding to such requests for information or testimony.

(2) The requirement to provide information in an inquiry does not, in all cases, take precedence over a promise of confidentiality given under authority of government law, regulation, or policy, such as a promise of confidentiality given by an EEO counselor, an Ombudsman, or a TSA Model Workplace Conflict Management Coach. However, a promise of confidentiality does not extend to information that reveals criminal activity, a threat of harm to a person or persons, a breach of transportation security, concerns regarding access to national security information, or other similarly serious matter (such as an offense listed in the attachment to TSA MD 1100.75-3, *Addressing Unacceptable Performance and Conduct*). Questions concerning confidentiality matters, including promises of confidentiality, should be referred by management to OCC.

(3) TSA's policy is to cooperate fully with Congress and other duly authorized investigative bodies regarding matters under their jurisdiction. All employees must give complete and truthful information in response to requests from such bodies for information or assistance. Prior to responding, employees must advise their supervisor, or their second-level supervisor of any such request.

(4) When directed by the Administrator (or designee), or by another appropriate authority, an employee shall take an oath or make an affirmation about his/her testimony or written statement before an agent authorized by law to administer oaths. If requested, the employee, after reviewing the document, shall sign his/her name to the transcript of testimony, affidavit or written statement that the employee provided. No employee may refuse to testify or refuse to provide a written statement or information pertinent to matters under investigation or inquiry. However, if the employee is being questioned by DHS Office of Inspector General, TSA Office of Inspection (OOI), or other authorized criminal investigator as the subject of an investigation that could result in criminal prosecution, the employee shall be issued a *Garrity* warning.

(5) A *Garrity* warning is appropriate during an investigation when an employee is requested to provide information on a voluntary basis and the possibility exists that the information provided may be used as evidence against the employee in any future

criminal proceeding. In such matters, the employee is advised: (1) that they are not under arrest; (2) the interview is voluntary; (3) they may terminate the interview at any time; (4) any information the employee provides may be used against him or her in a subsequent criminal trial or administrative hearing; and (5) no disciplinary or adverse action may be taken against the employee solely for refusing to provide a statement or answer questions. In these cases, management officials must contact OCC for guidance

(6) A *Kalkines* warning may be issued to the employee in some cases. (**NOTE:** This warning may only be issued by authorized OOI or DHS agents). A *Kalkines* warning is appropriate when the possibility of criminal prosecution has been removed, usually by a declination to prosecute by the U.S. Department of Justice. In these instances, the employee is required to answer questions relating to the performance of his or her official duties or be subject to disciplinary or adverse action, as appropriate.

G. **Letters and Petitions to Congress:**

(1) Employees, in their official capacity, may not engage in "grass roots" lobbying by encouraging persons or entities outside the Government (third parties, special interest groups, or members of the public) to contact members of Congress in support of, or in opposition to, a legislative matter before or after its introduction.

(2) Employees, either individually or collectively, in their personal capacity, may petition Congress or any member thereof, or may furnish information to any committee or member of Congress unless the information furnished is prohibited by law, regulation, or policy from disclosure.

(3) Employees may not use agency facilities (to include facilities, supplies, equipment, personnel and/or duty time) to contact any committee or member of Congress about personal business.

(4) Although TSA desires that employees seek to resolve any workplace problem or grievance within TSA, employees exercising their right to correspond with a member of Congress shall be free from restraint, reprisal or coercion.

H. **Recording or Monitoring of Telephone Calls or Covert Recording or Monitoring of Conversations, Meetings, etc.:**

(1) Recording of telephone conversations in connection with performance of TSA duties without prior approval of the Chief Information Officer (CIO) is prohibited. The use of recording devices, portable or otherwise, on telephones shall be for official purposes and generally limited to areas involving transportation security.

(2) Covert/secret taping of any conversation or meeting occurring at the workplace or off-site that deals with workplace issues and matters of official concern is generally prohibited. This prohibition applies regardless of any state law that may permit

covert/secret tape recording, except that covert recordings may be conducted by OOI agents during their investigations as specified by law.

(3) These prohibitions do not preclude openly using recording equipment in areas involving transportation security, official investigations, or under circumstances wherein the prior willing concurrence of all parties is clearly and specifically indicated and understood.

(4) Electronic communication devices may be used for covert recording involving transportation security. For additional information on electronic communication devices, refer to section D.

I. Defamatory or Irresponsible Statements:

Employees are accountable for the statements they make and the views they express. An employee's public criticism of TSA, its management or employees on matters of public concern (defined as a matter of political, social, or other concern to the community) may be constitutionally protected. However, this protection may be limited if the speech in question disrupts the orderly conduct of official business, concerns protected information, or where such statements adversely affect the efficiency of TSA. For example, defamatory, irresponsible, false or disparaging statements about employees may disrupt the orderly conduct of official business or adversely affect the efficiency of TSA.

J. Relationships in the Workplace:

TSA is committed to avoiding the adverse effects on the morale, operations and mission of the agency that may result from romantic and/or intimate personal relationships in the workplace. A romantic or intimate relationship between individuals who have a direct or indirect supervisory relationship is inappropriate and may violate the Standards of Ethical Conduct for Employees of the Executive Branch. Although TSA has no desire to interfere with the private lives of its workforce, such conduct may affect workplace effectiveness and the best interests of TSA must come first. Therefore, if such a situation develops, the employee in the supervisory position (the more senior position if both employees are supervisors) must inform his/her manager to enable TSA to take appropriate measures to eliminate any potential or actual adverse effects.

K. Sexual Harassment and Misconduct of a Sexual Nature:

TSA is committed to providing a workplace free from sexual harassment or misconduct of a sexual nature. All employees have a right to work in an environment where they are treated with dignity and respect.

(1) Sexual harassment is sex discrimination in violation of Title VII. Sexual harassment is defined as unwelcome sexual advances (actions will be determined as "unwelcome" if the employee did not solicit the action and the employee regarded the conduct as undesirable and/or offensive), requests for sexual favors, and other verbal

or physical conduct of a sexual nature when:

(a) Submission to such conduct is either explicitly or implicitly made as a term of an individual's employment;

(b) Submission to or rejection of such conduct by an individual is used as the basis for employment decisions; or

(c) Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment.

(2) Misconduct of a sexual nature may not rise to the legal definition of sexual harassment, but is nonetheless inappropriate for the workplace and will not be tolerated. For instance, viewing, posting, copying, sharing, distributing and/or printing material of a sexual nature from the internet or other source is prohibited while on duty, while on TSA premises, or when using a TSA computer or server.

(3) All employees have a responsibility to behave in a proper manner and to take appropriate action to eliminate sexual harassment or other misconduct of a sexual nature in the workplace. Additional information may be found in TSA MD 1100.73-3, *Prevention and Elimination of Sexual Harassment in the Workplace*.

L. **Workplace Violence:**

Violent, threatening, intimidating, or confrontational behavior is unacceptable and will not be tolerated. Threatening behavior may include harassment, intimidation, or any oral and/or written remarks or gestures that communicate a direct or indirect threat of physical harm, or which otherwise frighten or cause an individual concern for his or her personal safety. Such irresponsible and inappropriate behavior includes actions, gestures, language or any other intimidating or abusive action that creates a reasonable apprehension of harm. Employees, supervisors, and managers are responsible for enforcing the highest standards of personal safety and welfare at the workplace. Employees must immediately report threats of violence, violent incidents or other inappropriate behavior to their supervisors, Workplace Violence Coordinators, TSA Worksite Managers, or any TSA management official, as appropriate in the situation. Refer to TSA MD 2800.12, *Workplace Violence Program*, for additional information.

M. **Eliminating Discrimination and Creating a Model Work Environment (MWE):**

(1) TSA is committed to providing a work environment free from unlawful discrimination and where the contributions of all employees are supported and encouraged without regard to non-merit factors. All conduct must be appropriate and supportive of a model work environment. For instance, engaging in discriminatory conduct, making disparaging remarks, expressing stereotypical views that reflect negatively on a particular group or individual, or displaying and/or distributing

offensive materials that ridicule or defame a particular group is prohibited in the workplace.

(2) Every level of management, including supervisors, is required to provide positive leadership of and support for TSA's and DHS' Equal Employment Opportunity (EEO) policies and programs by ensuring that all agency programs, practices and activities are developed and administered in accordance with pertinent laws and agency policy prohibiting discrimination. Managers and supervisors must not engage in unlawful discrimination or inappropriate behavior in exercising their authority to take, direct others to take, recommend or approve any personnel action with respect to TSA employees and applicants. Managers and supervisors are responsible for ensuring a hospitable workplace free of discrimination, intimidation, and other offensive behaviors and materials, and may be subject to corrective action for failing to take prompt appropriate action to correct intimidating and/or offensive activity in the workplace.

(3) TSA prohibits reprisal and illegal discrimination against anyone on the basis of race, color, national origin, religion, age, sex, disability, sexual orientation, political affiliation, marital or parental status, or genetic information. Consistent with law, however, TSA may establish physical and mental ability or gender-based employment criteria when necessary to meet TSA's legal and operational mandate to perform security screening functions. In addition, TSA will not tolerate disparate treatment of individuals on the basis of characteristics not bearing on job performance or the statutory qualifications of the job.

(4) It is a violation of TSA policy to coerce, threaten, retaliate against, or interfere with any person in the exercise of his or her right to file a claim of illegal discrimination or his or her right to oppose any discriminatory practices or behavior. No employee shall be subject to retaliation for making a charge of discrimination, giving testimony, assisting, or otherwise participating in the EEO process; nor shall an employee be retaliated against for filing a grievance or participating in any process provided for in the Unitary Dispute Resolution System (UDRS), or raising his or her concerns regarding the workplace through other available means (e.g., Office of the Ombudsman, U.S. Office of Special Counsel, OIG).

NOTE: TSA's Civil Rights Division is responsible for the EEO process at TSA. TSA's National Resolution Center (NRC) is responsible for administering the UDRS.

N. **Possession of Firearms or Other Weapons:**

(1) Unless authorized by TSA, no employee may have in his or her possession any firearm or other dangerous weapon —

(a) While in any Federal facility (as defined in 18 U.S.C. § 930); or

(b) While in any motor vehicle, vessel, aircraft, or other conveyance owned, leased, rented, or controlled by the United States; or

(c) While acting in the course and scope of office or employment, except that an employee is permitted the otherwise lawful storage of a firearm or weapon in a private vehicle or conveyance if not otherwise prohibited by this section N.

NOTE: These rules apply *in addition to* any relevant federal, state, and local or tribal laws, rules, ordinances, and directives.

(2) Employees traveling with firearms must ensure that such items are packed in the employee's checked baggage pursuant to 49 C.F.R. § 1540.111(c), or, with respect to other weapons, ensure that such items are packed in the employee's checked baggage. All employees are required to follow individual airline regulations when traveling with a firearm and/or weapon. Firearms and weapons may only be transported in checked baggage. Employees must declare the firearm or weapon to the ticket agent and present the unloaded weapon in a locked hard-sided case. The hard-sided case does not include a suitcase. No employee may carry a firearm or weapon onto an airplane on their person or in accessible property unless authorized by TSA in accordance with this directive.

(3) The prohibitions outlined in Section N(1) and N(2) above do not apply to any TSA designated law enforcement officers (i.e., TSA Criminal Investigators in 1811 positions, Federal Air Marshals in 1801 positions, AFSDs for Law Enforcement in 1811 positions, and Transportation Security Specialists in 1801 positions in the OLE/FAMS, Security Branch and Physical Security Section, that are designated as law enforcement positions) that comply with all of the requirements of 49 C.F.R. § 1544.219, including the training and notification requirements.

(4) Employees are prohibited from using identification cards, credentials, badges, or other employee identifiers to circumvent these provisions to carry a firearm/weapon in a non-official capacity.

O. **Alcohol and Drugs:**

(1) TSA prohibits the use of illegal substances and the inappropriate use of legal substances. Illegal substances include, but are not limited to, cocaine, marijuana, opiates, amphetamines, and phencyclidine. The use of marijuana is prohibited by Federal law. State and local laws, as well as laws of other countries, do not affect the prohibition of marijuana use by TSA employees. Legal substances include, but are not limited to, alcohol and prescription or over-the-counter medications. These substances can negatively affect the:

(a) Employee's work performance and/or conduct;

(b) Ability of other employees to perform their duties effectively; and

(c) Ability of TSA to accomplish its mission.

(2) As an employer with responsibility for transportation security, TSA is especially concerned when an employee's actions could negatively affect the security of the public or detract from public confidence. Public confidence depends upon trust in the integrity of the nation's transportation systems, and in the employees who maintain the security of the traveling public. Accordingly, employees will be subject to the following requirements:

(a) Employees are prohibited from using illegal drugs;

(b) Employees are prohibited from possessing, distributing or trafficking in controlled and/or illegal substances in violation of federal, state or local law. This prohibition applies to employees both on and off-duty;

(c) Employees who inappropriately use legal substances will not be allowed to perform any safety or security-sensitive duties. TSA shall consider the circumstances of the inappropriate use and determine whether an employee may be returned to duty. An employee shall not be returned to duty unless TSA has determined that such employee is not a risk to public safety or security;

(d) An employee arrested for drug or alcohol-related crimes for which a term of imprisonment could be imposed will not be allowed to perform any safety or security-sensitive duties unless TSA determines that the employee is not a risk to public safety or security. Employees may be subject to an investigation of the circumstances giving rise to the arrest and disciplined in appropriate cases;

(e) Employees occupying Testing Designated Positions (TDPs) other than law enforcement positions are prohibited from consuming or being under the influence of alcohol while on duty or consuming alcohol for a minimum of eight hours preceding performance of security-related functions. Law enforcement positions, including Federal Air Marshals, Criminal Investigators, and any other TSA-designated Law Enforcement Officers are prohibited from consuming or being under the influence of alcohol while on duty or consuming alcohol for a minimum of 10 hours preceding performance of security-related functions. Employees are responsible for ensuring that they are fit for duty and free of any alcohol impairment upon reporting for, and carrying out, their security functions;

(f) Employees in non-TDPs are prohibited from consuming or being under the influence of alcohol while on duty; and

(g) Employees are prohibited from endangering themselves and the public by driving while under the influence of alcohol.

(h) Employees subject to random alcohol and/or drug testing may not leave the testing site without permission from a supervisor prior to completing the alcohol and controlled substance testing. Employees requesting leave due to emergency situations must advise their immediate supervisor and any other management official from whom they are requesting leave that they have been selected for random testing contemporaneous with the leave request, and prior to leaving the testing site.

P. **Membership or Participation in Hate Groups Or Organizations That Engage In Criminal Or Other Notorious Activity:**

(1) Membership or participation in hate groups is inconsistent with TSA's policy that employees not engage in activities that may reflect unfavorably on TSA or the federal government. An employee who knowingly becomes, remains a member of, or participates in a hate group, or who otherwise knowingly associates with the hate-motivated activities of others, proceeds at the risk that his or her membership, participation, or association could reasonably be taken as tacit approval of the prejudice-related aspects of those groups or activities. As used here, "hate group" or "hate-motivated activities" is defined as an organization, association, event, or activity, the sole or primary purpose of which is to advocate or promote hate, violence, or invidious prejudice against individuals or groups based on race, color, religion, national origin, sex, sexual orientation, age, or disability where such association, conduct, or speech adversely affects the efficiency of TSA.

(2) Membership or participation in organizations that condone violence against others or engage in criminal or other notorious activity - whether or not the employee himself or herself engages in such activity - is inconsistent with TSA's and DHS's mission to ensure the safety of our nation's transportation systems and the security of our country. Therefore, employees who associate with such organizations run the risk that their membership, participation, or association could reasonably be taken as approval of the organization's notorious activities. Under certain circumstances, employees may be required to terminate their relationship with such organizations and/or may be subject to administrative action.

(3) Employees will not, except as may be necessary in connection with official assignments or duties, associate with individuals or groups who are believed or known to be connected with criminal activities. This limitation on association covers any social, sexual, financial, or business relationship with a source of information, a suspected or known criminal, or an illegal alien, subject to being removed from the United States of America.

Q. **Subversive Activity:**

In accordance with 5 U.S.C., Chapter 73, no employee shall advocate, or become a member

of any organization that which the employee knows advocates the overthrow of the U.S. Government, or which seeks by force or violence to deny other persons their rights under the Constitution of the United States.

R. **Partisan Political Activity and Holding Partisan Political Office:**

(1) Employees are responsible for complying with the restrictions on partisan political activity contained in the Hatch Act (5 U.S.C. § 7321, et seq, 5 C.F.R. Parts 733-734).

(2) No employee shall run for nomination to or as a candidate for a partisan political office, except as expressly provided in 5 C.F.R Part 733. Employees may not conduct partisan political activities in the Government workplace or while on duty, in a Government vehicle, or while wearing an official uniform. In addition, employees may not solicit, accept, or receive partisan political campaign contributions or host a partisan political fundraiser. Employees are urged to seek the advice of OCC or the U.S. Office of Special Counsel to determine if a particular partisan political activity is permissible under the Hatch Act.

S. **Work Strikes and Slowdowns:**

Employees are prohibited from engaging in, or encouraging another federal employee to engage in, a strike, work stoppage, work slowdown or sickout involving the Federal Government.

T. **Canvassing, Soliciting, or Selling:**

Employees shall not engage in private activities involving the use of government time, the time of a subordinate, or equipment or resources for personal gain or the gain of others or any other unauthorized purpose while on duty or on Government owned or leased property.

(1) This prohibition applies specifically, but is not limited to, such activities as:

(a) Canvassing, soliciting, or selling, particularly for personal or private monetary gain;

(b) Promoting or buying (group or otherwise), when such action could reasonably be interpreted as involving the improper use of Government facilities, equipment, and personnel;

(c) Canvassing or soliciting membership, except in connection with organized, sanctioned employee groups as authorized by law, regulation, or directive; and

(d) Soliciting contributions from other employees for a gift to anyone in a superior official position in contravention of law (5 U.S.C. § 7351) or regulation (5 C.F.R. §§ 2635.301 – 2635.304).

(2) This prohibition does not apply to:

(a) Specifically authorized activities;

(b) Soliciting contributions for authorized charitable, health, welfare and similar organizations (e.g., Combined Federal Campaign) as outlined in 5 C.F.R. Part 950;

(c) Activities of voluntary groups of Federal employees commonly accepted as normal social, welfare or recreational functions of such groups; and

(d) Solicitation for a voluntary contribution for an employee experiencing a significant life event where the collection is conducted by co-workers of approximately equal status to the employee. In this context, a significant life event includes but is not limited to such events as marriage, childbirth, transfer, separation, retirement, illness or death in the family.

U. **Gambling and Related Activities:**

Employees shall not conduct or participate in any gambling activity while on Government-owned or leased property, or at the workplace or in any government office, while in uniform, while using a government vehicle, or using government resources. Gambling activity includes, but is not limited to, operating a gambling device, on-line gambling or internet gambling, conducting or participating in a lottery or pool, conducting or participating in a game for money or property, or selling or purchasing a numbers slip or ticket. However, for the purposes of this directive, the purchasing of state-sponsored lottery tickets is not considered a gambling activity.

V. **Borrowing and Lending Money:**

(1) Managers, supervisors, or supervisory team leads shall not borrow money from subordinates or have a subordinate act as an endorser or co-maker of a note given as security for a personal loan. Employees shall not lend money to any other employee, superior official or peer for monetary profit or other gain. These prohibitions do not apply to the operation of recognized credit unions or to employee welfare plans.

(2) Managers and supervisors should also not engage in any financial agreement or joint business ventures, including, but not limited to, general or limited partnerships, landlord-tenant relationships, or ongoing contractual relationships for providing goods or services, that could affect the financial interests of a subordinate or a supervisor, or otherwise create a conflicting financial interest or create an appearance of lack of impartiality as defined by 5 C.F.R. § 2635.502.

W. **Meeting Financial Obligations**:

Employees shall satisfy in good faith all just financial obligations and shall make and adhere to arrangements for settlement of debts. Financial obligations include, but are not limited to: Federal, state, or local taxes; and other valid debts, including personal commercial debts, Government-provided credit card debts, claims based on court judgments, Federally insured student loans, and tax delinquencies.

X. **Notarial Fees:**

An employee who is a notary public shall not charge or receive fees for performing notarial acts in connection with his or her official duties. The prohibition on acceptance of fees does not apply to notarial acts performed in an unofficial capacity during off-duty hours and off-Government property.

Y. **Gifts From Non-Federal Sources:**

Employees are prohibited from soliciting or accepting, either directly or indirectly, any gift from a prohibited source, or a gift that is offered because of the employee's Government position, unless an exception or exclusion applies to gifts that are offered pursuant to 5 C.F.R. Part 2635, Subpart B. Gifts may not be solicited even if an exclusion or exception would apply if the gift was offered to the employee. Generally, employees may not accept cash. Generally, a prohibited source includes any person or organization seeking official action by doing or seeking to do business with, or whose activities are regulated or substantially affected by TSA or its employees, and includes the traveling public. See 5 C.F.R. § 2635.203(d) for the regulatory definition of a prohibited source. A gift includes any favor, gratuity, discount, entertainment, hospitality, loan, forbearance, or any other thing of monetary value, including free transportation and free attendance. Refer to the TSA Guide to Major Ethics Rules for additional information.

Z. **Outside Employment and Outside Activities:**

(1) Employees may not engage in outside employment or an outside activity that conflicts with their official duties. See 5 C.F.R. § 2635.802 for additional details. Outside employment, or an outside activity, will conflict with an employee's official duties if the employment/activity violates the law or any agency supplemental regulation, or if it will cause the employee to disqualify himself/herself from participating in matters that are so central or critical to the performance of the employee's official duties that the employee's ability to perform the duties of his/her position will be materially impaired. Examples of conflicting outside employment/activities include those matters that will create a financial conflict of interest for an employee, or cause an appearance of lack of impartiality in the performance of his/her official duties.

(2) Employees are urged to seek guidance from their field counsel or OCC in advance to determine whether outside employment/activity will conflict with the employee's

official duties.

(3) Employees who engage in conflicting outside employment/activities may be subject to disciplinary action, may be forced to resign from the conflicting outside employment/activity, or may be subject to civil or criminal prosecution if the outside employment/activity violates the criminal conflict of interest ethics statutes at 18 U.S.C. §§ 201-209, or other laws.

AA. **Advertisements, Endorsements, and Referrals:**

Employees shall not use or permit use of their Government position or title, or any authority associated with their public office, to endorse any product, service, or enterprise, or for the private gain of friends, relatives, or persons with whom the employee is affiliated in a non-governmental capacity , except as permitted by law or regulation, .

BB. **Unauthorized Absences and Tardiness:**

(1) Employees are expected to schedule and use earned leave in accordance with established procedures. Whenever possible, employees must obtain prior approval for all absences including leave without pay (LWOP). Employees are required to contact their supervisor as far in advance of their scheduled tour of duty as possible, or by the time established in the call-in procedures for their organization, to request and explain the need for unscheduled leave. Exceptions to this requirement include when the employee is incapacitated or when there are other exigent circumstances. In such instances, the employee, a family member or other individual should, as soon as is reasonably practical, notify the employee's supervisor of the unplanned leave. Repeated unscheduled absences may negatively reflect on the employee's dependability and reliability, and may adversely affect TSA's mission. Unapproved absences will be charged as absent without leave (AWOL). AWOL may form the basis for administrative action, including discipline, up to and including removal from TSA.

(2) Tardiness includes delay in reporting to work at the employee's scheduled starting time, returning late from lunch or scheduled break periods, or returning late to the employee's work site after leaving the workstation on official business or leave. Unexplained and/or unauthorized tardiness shall be charged as AWOL. Refer to TSA MD 1100.63-1, *Absence and Leave*, for additional information. For Bargaining Unit Employees, refer to Article 3, *Attendance Management Process*, of the Collective Bargaining Agreement between TSA and the American Federation of Government Employees.

CC. **Nepotism:**

TSA officials shall not knowingly appoint, employ, promote, or advance to a position in TSA one of his/her relatives. Among other things, managers and supervisors shall not:

(1) Advocate one of his/her relatives for appointment, employment, promotion, or advancement to a position in his/her agency or in an agency over which he/she exercises jurisdiction or control.

(2) Knowingly appoint, employ, promote, or advance to a position in TSA the relative of a TSA official, or of a public official who exercises jurisdiction or control over TSA, if the TSA official or public official has advocated the appointment, employment, promotion, or advancement of that relative.

(3) Directly or indirectly supervise a relative except in certain limited circumstances. Refer to TSA MD No. 1100.30-2, *Employment of Relatives*, for additional information.