GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

ADM 5400.1A
July 1, 2020

GSA ORDER

SUBJECT: Meetings with Representatives of Foreign Governments or Foreign Industry, Foreign Travel, and Foreign Contacts

1. Purpose. This U.S. General Services Administration (GSA) Order establishes procedures and reporting requirements for all GSA personnel regarding:

a. Meetings and visits with representatives from foreign governments and/or foreign industry for all employees;

b. Official or unofficial foreign travel for covered individuals; and

c. Maintaining foreign contacts for covered individuals.

2. Applicability. This Order applies to:

a. All GSA employees (except as noted under paragraphs 2.c. and 2.d. below), and includes additional responsibilities for covered individuals (see Appendix C for definition).

b. Covered individuals are not limited to Government employees but include all persons defined in Security Executive Agency Directive (SEAD) 3.

c. The Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG's independent authority under the Inspector General Act and it does not conflict with other OIG policies or the OIG mission.

d. The Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines it is consistent with its independent authority under the Contract Disputes Act and other authorities and it does not conflict with the CBCA's policies or mission.

3. Cancellation. This Order cancels and supersedes ADM P 5400.1, Meetings with Representatives of Foreign Governments or Foreign Industry, Foreign Travel, and Foreign Contacts.

4. Background.

a. GSA operates in an environment where foreign governments and others continue to invest considerable time and resources to assessing and targeting U.S. Government employees for both recruitment and the transfer of vital Government information. Transfer attempts are devised both knowingly and unknowingly through a targeted individual, often seeking information that is unclassified yet sensitive in nature when compiled from multiple sources or over a sustained time period.

b. Presidential Decision Directive PDD/NSC-12 indicates that a mainstay of foreign intelligence services is the recruitment of well-placed assets, such as U.S. Government employees, who can provide insightful intelligence on a particular issue. The U.S. is, and will continue to be, the prime focus of foreign intelligence services. Therefore, those in the Federal workforce, especially those in sensitive positions, are of special interest to Foreign Intelligence Services.

c. This Order is not intended to limit or impair professional or personal contacts. Rather, its purpose is to protect the security of the U.S. and its employees while ensuring privacy of employees and their freedom of association. This policy ensures that security risks to individuals or to the U.S. Government are identified at the earliest opportunity and deterred.

d. This Order is designed to protect GSA and its employees against foreign government and foreign industry exploitation, while also preventing unauthorized access to classified, sensitive, proprietary information, Sensitive But Unclassified (SBU) information or Controlled Unclassified Information (CUI).

e. GSA will maintain a comprehensive foreign travel, foreign meetings and visits, and foreign contacts program in accordance with national level directives (to include the specific notification, briefing, and debriefing requirements in SEAD 3). The program will reduce or mitigate risk to GSA and employees. It will protect GSA’s sensitive and classified information and its critical infrastructure from the threats posed by foreign intelligence entities.

5. Covered Individual Responsibilities.

a. All covered individuals incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad.

b. SEAD 3 establishes reporting requirements for all covered individuals. Covered individuals also have a responsibility to recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility. They must also report incidents of adverse personal behaviors and activities (e.g., arrests, financial difficulties, etc.). SEAD 6 establishes policy and requirements for the continuous evaluation (CE) of covered individuals who require continued eligibility for access to classified

information or eligibility to hold a sensitive position.

c. Covered individuals shall report to the Office of Mission Assurance (OMA), Threat Management Office (TMO), any planned or actual involvement in any of the following activities: meetings/visits with representatives of foreign governments or foreign industry, foreign contacts, and foreign travel. OMA shall conduct an analysis of such reported activities to determine whether they pose a potential threat to national security and take appropriate action.

d. Reporting shall be automated to the extent practical and provide required data elements as identified in Appendices A and B.

e. Failure to comply with GSA reporting requirements may result in administrative action that includes, but is not limited to, revocations of national security eligibility.

6. Meetings/Visits with Representatives of Foreign Governments or Foreign Industry.

a. For purposes of this Order, the following individuals are not considered foreign visitors requiring reporting:

(1) Lawful Permanent Residents or other Protected Individuals as defined in 8 U.S.C. 1324b (both must be able to present evidence of their status to OMA if requested);

(2) GSA employees (if employed in accordance with statutes and regulations) or GSA contractor employees who are Foreign Nationals;

(3) Foreign Nationals who visit GSA facilities during public events or activities, or in areas that are open to the general public (i.e., in circumstances that do not require visitors to pass through an access control point manned by security personnel, receptionists, or electronic screening devices).

b. Representatives of a foreign government, foreign industry or foreign visitors who participate in meetings/visits at GSA facilities or with GSA employees in non-GSA facilities could pose a security risk. It is an opportunity for visitors to solicit and collect information that is not readily available and an opportunity for them to identify points of contact and recruit personnel to provide information in the future.

c. Any GSA employee who receives a request for a meeting/tour from a foreign government or foreign industry must notify the Office of Congressional and Intergovernmental Affairs (OCIA). OCIA will coordinate with the Department of State and other Federal agencies as applicable, and for approved visits, become the lead point of contact with the foreign government or foreign industry officials.

d. Any GSA office that plans to host a meeting/tour both on and off of GSA property

that includes one or more representatives from a foreign government or foreign industry will coordinate the foreign visit with the TMO. The hosting office must submit a meeting request in coordination with OCIA to the TMO. The meeting request must be submitted **at least 10 business days prior** to the visit, and the information listed in Appendix A must be included.

e. In the case of repeat or recurring visits by the same representative(s) of a foreign government or foreign industry, the TMO may issue Extended Period Memorandums for Record (EPMFR) that covers a project/program for a one year period; for example, the Land Port of Entry location employees have daily recurring contact with foreign nationals as part of their daily responsibilities. The TMO will look at these situations on a case-by-case basis. If your project or program has daily recurring foreign contact in the course of official duties, you may contact the TMO and request an EPMFR. The TMO will provide you with requirements at that time.

f. Prior to initiating virtual Meetings with foreign government or foreign industry, the planned meetings must also be reported to the TMO for guidance.

g. The TMO will review the meeting/visit request and make a recommendation for or against the meeting to OCIA and the hosting office.

h. Prior to the visit, the hosting office will contact the foreign visitor(s) and request they bring proper identification to the building. They will also advise that electronic devices—including, but not limited to, flash drives, cameras, cellular telephones, and personal communication and media devices—are prohibited from being brought to the meeting/visit/facility unless an exception is granted. It is not the TMO's intent to limit collaboration with foreign visitors. While visitors are normally instructed to not bring electronic devices to GSA due to validated security concerns, on occasion there may be business exceptions that make it necessary to allow visitor access with electronic equipment. Based on requirements for the meeting, the decision to grant an exception concerning electronic devices is ultimately the responsibility of the hosting office with coordination through GSA IT Security and concurrence from the TMO.

i. If no exception is requested, the hosting office is responsible for ensuring that electronic devices are not brought into GSA facilities by foreign visitors.

j. On the day of the meeting/visit, the identity of the representative(s) of the foreign government or foreign industry will be verified by a representative of the hosting office at the facility entrance after clearing screening and before access is permitted to the GSA facility.

k. The hosting office must:

(1) Comply with all requirements for access approval and conduct, including providing timely, complete, and accurate information regarding the visit to the TMO. The TMO may deny access to a foreign visitor if the hosting office fails to provide complete and accurate information in advance of a visit;

(2) Take all reasonable steps to ensure the foreign visitor is given access only to information necessary for the successful completion of the visit;

(3) Prevent physical, visual, and virtual access to classified, SBU or CUI, or otherwise proprietary or not-for-public release data, information, or technology;

(4) Take all reasonable steps to ensure that a foreign visitor does not use electronic devices that have been granted an exception for entry in those areas in GSA facilities where classified, SBU or CUI or otherwise proprietary, or not-for-public release data, information, or technology is present;

(5) Immediately report suspicious activities or anomalies involving foreign visitors to the TMO; and

(6) Promptly notify the TMO if there is a change to the arrival or departure date of any foreign visit.

l. Additionally, all electronic devices from a representative of a foreign government or foreign industry must never be used in Government computers, devices or systems. (Note: Per this Order, Paragraph 6, Subparagraphs h., i., and k. (4), electronic devices are not to be brought to the meeting/visit unless an exception is approved.)

m. The hosting office must ensure that the foreign visitors are escorted and closely monitored at all times while they are visiting GSA facilities. The TMO recommends the hosting office have one escort for every 5 to 7 foreign visitors and ensure that representative(s) of foreign governments or foreign industry are not allowed access to any GSA information technology system(s). A foreign visitor must be escorted by a U.S. citizen, Government employee of the hosting office, at all times on GSA property, except in areas that are open to the general public.

n. Any gift from a representative of a foreign government or foreign industry that is an electronic device must be submitted to the Director, Personnel Security for inspection and inventory as soon as possible after receipt. Additionally any gift must be reported in compliance with GSA Order OAS 7880.1B, Acceptance of Gifts and Decorations from Foreign Governments and the Giving of Gifts to Foreign Individuals by GSA Employees. A debriefing of the hosting employee and other GSA employees who were meeting/visit participants may be conducted by the Director of Personnel Security if necessary.

o. The TMO may revoke any approved foreign visit and deny any hosting office foreign visitor request.

p. Based upon the information required concerning each foreign visitor, the TMO will conduct applicable agency checks and will make a risk assessment determination and notify the hosting office and OCIA of approval or denial of access. In the event of denial of access, a senior level employee of the affected office may appeal to the Director of Personnel Security, who will consider whether the benefits of a proposed visit justify the

risks.

7. Foreign Travel.

a. All covered individuals may be required to submit an itinerary (see Appendix B) for all foreign travel conducted for either official or personal purposes. The Foreign Travel Notification Form should be submitted to the TMO at least 14 calendar days in advance of travel. Except as noted in the subparagraphs below, covered individuals must provide advance notice of foreign travel.

(1) Travel to U.S. Territories is not considered foreign travel and need not be reported.

(2) Unplanned day trips to Canada or Mexico shall be reported within five business days of return.

(3) When required by the TMO, covered individuals must prior to travel, receive a travel threat briefing and in some special circumstances, a counterintelligence (CI) briefing.

(4) While emergency circumstances may preclude full compliance with pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics. If possible, inform the TMO, prior to departure. In any event full reporting shall be accomplished within five business days of return.

b. All covered individuals may be required to receive a travel briefing prior to foreign travel. Travel may require approval for the trip based upon active threat streams and will be subject to a security debriefing upon completion of foreign travel. This process may include face to face, electronic, or automated briefings as deemed appropriate for the situation.

c. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary, regardless of duration, are discouraged. If the covered individual decides to conduct an unscheduled border crossing they must disclose it to the TMO during the post travel debriefing.

d. All deviations from approved travel itineraries shall be reported to the TMO during the post travel debriefing. The post travel debriefing must be completed within five business days of return.

e. In accordance with SEAD 3, the GSA Administrator may disapprove unofficial foreign travel of GSA employees who are covered individuals when it is determined that such travel presents an unacceptable quantifiable risk to the employee (e.g., to countries with active threat streams or ongoing infectious disease outbreaks). Travel

risk is currently assessed by the TMO and disapprovals should be used only if there is an imminent threat to Federal employees or U.S. citizens within the requested travel destination. For active war zones, the Chief of Station, U.S. State Department, has the final say and provides country clearances as necessary for those areas. Failure to comply with such disapproval may result in administrative action that includes, but is not limited to, revocation of national security eligibility.

f. All GSA employees without a security clearance or who do not occupy a sensitive position as defined in Appendix C are encouraged to notify the TMO of all foreign travel, conducted for either official or personal purposes. Such employees may receive travel briefings at their request prior to foreign travel and may be asked to participate in a security debriefing upon completion of foreign travel.

g. All GSA employees and contractor employees wishing to take Government-furnished electronic (GFE) devices (e.g., laptops, tablets, phones) on foreign travel must submit a request through the GSA IT Service Desk.

8. Foreign Contacts.

a. All covered individuals are required to report official and unofficial contacts with foreign nationals to the TMO as part of their official duties and responsibilities. All covered individuals will report:

(1) Continuing association with foreign nationals, or any contact with a foreign national that involves the exchange of personal information. This reporting requirement is based on the nature of the relationship regardless of how or where the contact with the foreign national was made or how the relationship is maintained (e.g., via personal contact, telephonic, postal system, or Internet).

(2) Following initial reporting, updates regarding continuing unofficial association with known foreign nationals shall occur only if and when there is a significant change in the nature of the contact.

b. All employees must report when:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information including Personally Identifiable Information (PII), even if the employee does not have access to classified information or otherwise sensitive information;

(2) The employee is concerned that he/she may be a target of actual or attempted exploitation by a foreign entity; and/or

(3) Contact occurs with a known or suspected foreign intelligence entity.

c. Content for reportable foreign contacts should include the following information:

(1) Name of the employee who had foreign contact;

(2) Date and location of the contact;

(3) General circumstances of the contact;

(4) If the contact involved a request to receive information that the individual is not authorized to receive, the specific content of the conversation and a description of the requested information and/or documents must be reported; and

(5) If known, the name and description of the individual(s) that made the request.

d. Reporting limited or casual contact with foreign nationals is not required, e.g., a GSA employee attends a festival while on foreign travel, where they meet random foreign nationals and have no intention of keeping in contact with the contacts. If unsure, GSA employees may reach out to the TMO for clarification/determination on whether to report the contact or not.

9. GSA Employees with Overseas Duty Stations.

a. Covered individuals with Overseas Duty Stations are still required to report foreign travel and foreign contacts. The TMO understands that overseas employees may be reporting this information via the local supporting command per established Memoranda of Understanding or other relevant agreement, but the TMO must still be notified of foreign travel and contacts as outlined below.

b. The TMO recognizes that various Status of Forces Agreements (SOFA) and Chief of Mission agreements cover different overseas areas where GSA employees are based. As outlined below, overseas employees must still report certain foreign travel and foreign contacts to the TMO. This can be accomplished in several ways and might include an agreement with the supporting command to provide the TMO with that information.

(1) To the greatest extent possible, the TMO has automated the foreign travel reporting process, so overseas employees can easily report their travel via GSA InSite and review travel warnings online at any time. Overseas employees on official travel within a SOFA area are exempt from reporting this travel to the TMO. The TMO considers the entire SOFA area the employee's official duty station for the purpose of foreign travel reporting.

(2) However, overseas employees on official travel must still report any plans to travel outside of their SOFA area in accordance with local sponsoring command policies. In some cases employees may be required to request country clearance from the associated embassy or consulate.

(3) Covered individuals with overseas duty stations must still report all leisure travel if they plan to, or inadvertently, cross a sovereign country border. Even if assigned in a Schengen Agreement area of the European Union, covered individuals must report leisure

travel plans to cross international borders. Travelers may contact the TMO for travel-related guidance at any time.

c. Covered individuals with overseas duty stations must report foreign contacts if they involve establishment of a material personal relationship or the attempt to exploit information from the employee. The following examples may help clarify reportable versus non-reportable contacts:

(1) Reportable Contact Examples:

- Contact/Meeting in a foreign embassy is reportable and will also be processed by the TMO as foreign travel.
- Talking randomly with foreign citizens where a relationship is established with the intention to pursue further contact is reportable.
- Having dinner, socializing or attending events with a foreign citizen on a regular basis is a reportable contact.
- If a foreign citizen seems overly interested in your official duties, this contact must be reported.

(2) Non-Reportable Contact Examples:

- Incidental contact, like friendly conversation with local citizens or neighbors in local areas or places of business is not reportable.
- Contact in the course of official duties is generally not reportable.
- If you are not sure if an incident is reportable, contact the TMO for guidance.
- Exceptions, clarifications or questions, contact the TMO for guidance.

(3) A GSA employee with an overseas duty station must report interactions with foreign industry in accordance with the above types of examples. An employee requiring guidance related to a specific interaction should contact the TMO. GSA business operations overseas focus on close collaboration with local vendors. In most cases these interactions are not reportable. Even if the GSA work unit occasionally participates in partnership style gatherings such as a barbeque, it is not reportable. However, if any relationship moves from the professional realm to a more personal nature it must be reported to the TMO.

d. Exceptions. All overseas employees must report attempts to obtain sensitive or classified information. Report must be made to the TMO, as soon as possible.

e. Government furnished electronic (GFE) devices.

(1) All GSA employees with an overseas duty station wishing to take GFE devices (including laptops, smartphones, and tablets) on leisure foreign travel must submit a request through the GSA IT Service Desk and receive approval from GSA IT and their supervisor, with a recommendation for approval or disapproval from the TMO related to country specific threat assessment.

(2) GSA IT may issue blanket waivers at its discretion for official travelers' use of GFE based on SOFA status and area of operations on a case-by-case basis for up to one year in duration. Blanket waivers must be reassessed on an annual basis. Any specific issues, questions or requests for waivers, must be coordinated through the GSA Chief Information Officer or GSA IT Service Desk.

(3) GSA IT will request that the TMO provide a recommendation related to travel with GFE based on active threat streams and country specific foreign intelligence modus operandi. However, the TMO only plays an advisory role in this process and does not approve or disapprove transport of GFE. The TMO may concur or non-concur with the decision, but the sole responsibility for approving travel with GFE remains with GSA IT.

10. Nature of Revisions.

a. Security Executive Agent Directive 3 (SEAD 3), released June 12, 2017, is added. SEAD 3 outlines reporting requirements for personnel with access to classified information or who hold a sensitive position.

b. Security Executive Agent Directive 6 (SEAD 6), released January 12, 2018, is added. SEAD 6 outlines requirements for the continuous evaluation (CE) of covered individuals who require continued eligibility for access to classified information or eligibility to hold a sensitive position.

c. GSA Order OAS 7880.1B, Acceptance of Gifts and Decorations from Foreign Governments and the Giving of Gifts to Foreign Individuals by GSA Employees, August 22, 2016, is added. GSA Order OAS 7880.1B provides guidance governing the receipt of gifts and decorations from foreign governments.

d. Section 5. "Covered Individual Responsibilities" is added.

e. Section 6. "Meetings/Visits with Representatives of Foreign Governments or Foreign Industry" adds the requirement to report meetings conducted both on and off of GSA property.

f. Section 6. "Meetings/Visits with Representatives of Foreign Governments or Foreign Industry" outlines the use of Extended Period Memorandums for Record (EPMFR).

g. Section 6. "Meetings/Visits with Representatives of Foreign Governments or Foreign Industry" modifies electronic device element of the policy prohibiting such devices in a GSA facility unless an exception is granted for business purposes by the TMO.

h. Section 7. "Foreign Travel" adds that the Administrator may disapprove unofficial foreign travel of covered individuals, when it is determined that such travel presents an unacceptable quantifiable risk to the employee.

i. Section 9. "GSA Employees With Overseas Duty Stations" is added.

11. Additional Information. Questions regarding this Order should be addressed to the Director, Personnel Security at threat-management-office@gsa.gov or OMA at eoc@gsa.gov.

12. Signature.

/S/_____
EMILY W. MURPHY
Administrator

Appendix A
Appendix B
Appendix C
Appendix D

APPENDIX A. FOREIGN VISITORS

Requests for hosting meetings and visits with representatives of foreign governments or foreign industry must contain the following information:

Foreign Visitor Identifying Data
(TMO will provide an Excel Spreadsheet template)

- Visitor's Full Name (First, Middle, Last)
- Gender
- Country(ies) of Origin/Citizenship (Identify if dual citizenship)
- Country of Current Residence
- Date of Birth (MM/DD/YYYY)
- Place of Birth (City and Country)
- Passport or Visa Number:
    - Country That Issued Passport
    - Issuance Date
    - Expiration Date
- Visitor Organization/Employer
- Purpose of Meeting:
    - Meeting Start Date and Time
    - Meeting End Date and Time
    - Building(s) and Room Number(s) to be Visited
- Hosting Office/Hosting Official (Name, Title, Building, Room Number, and Phone Number)
- Escort Information (If different from hosting office)
- Proposed Discussion Topics

APPENDIX B. FOREIGN TRAVEL FORMS

Requests for Foreign Travel; Official and Unofficial (Leisure) by all GSA employees will be coordinated via the Threat Management Office.

Employees can access the following forms. They must be filled-out and submitted to the Threat Management Office:

FOREIGN TRAVEL NOTIFICATION FORM

FOREIGN TRAVEL DEBRIEFING FORM

APPENDIX C. TERMS AND DEFINITIONS

Agency Check: A procedure whereby a request is made to a U.S. Government agency to determine whether information exists on a particular Foreign National.

Classified National Security Information or Classified Information: Information that has been determined pursuant to EO 13526 or any predecessor or successor order, EO 12951, or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, et seq., as amended, to require protection against unauthorized disclosure.

Counterintelligence (CI): Information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Covered Individuals:

a. A person who performs work for or on behalf of the Executive Branch who has been granted access to classified information or holds a sensitive position, but does not include the President or (except to the extent otherwise directed by the President), employees of the President under 3 USC 105 or 107, the Vice President, or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. 106 or annual legislative Branch appropriations acts.

b. A person who performs work for or on behalf of a State, local, tribal, or private sector entity, as defined in EO 13549, who has been granted access to classified information, but does not include duly elected or appointed governors of a State or territory, or an official who has succeeded to that office under applicable law.

c. A person working in or for the legislative or judicial branches who has been granted access to classified information and the investigation or determination was conducted by the Executive Branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President.

d. Covered individuals are not limited to Government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who have access to classified information or who hold sensitive positions in GSA.

Escort(s): An individual or team of GSA employees from the hosting office, assigned the responsibility of accompanying a foreign national or a group of foreign visitors who lacks authorized access within a GSA facility in order to ensure adherence to security measures protecting classified, SBU, CUI or otherwise proprietary, or not-for-public-release data, information, or technology from unauthorized physical, visual, or virtual access.

Foreign Industry/Corporation: A business or company that is incorporated and headquartered in a foreign country and conducts its primary business operations overseas.

Foreign Intelligence Entity: Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services, international terrorists, and transnational criminal organizations.

Foreign National: Any person who is not a U.S. citizen or a U.S. national.

Foreign Travel: Travel outside the U.S. and its Territories.

Foreign Visit: Any access by a Foreign National to a GSA facility, regardless of the length of time involved.

Foreign Visitor: Any person who is not a U.S. citizen or a U.S. national accessing a GSA facility.

Hosting Office: The organization responsible for managing the foreign visit and for taking all reasonable steps to protect classified, SBU, CUI, or otherwise proprietary, or not-for-public-release data, information, or technology from unauthorized physical, visual, and virtual access by a foreign visitor or guest.

Insider Threat: The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Lawful Permanent Resident or Other Protected Individual: Any person not a citizen of the U.S. who is living in the U.S. under legally recognized and lawfully recorded permanent residence as an immigrant. Also known as “permanent resident alien,” “resident alien permit holder,” and “Green Card holder.”

National Security: Those activities which are directly concerned with the foreign relations of the U.S., or protection of the Nation from internal subversion, foreign aggression, or terrorism.

Sensitive But Unclassified (SBU): Specific information that while not classified, requires protection from disclosure.

Sensitive Position: Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.

Status of Forces Agreement (SOFA): An agreement between a host country and a foreign nation stationing military forces in that country. SOFAs are often included, along with other types of military agreements, as part of a comprehensive security arrangement.

Unauthorized Disclosure: A communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

APPENDIX D. REFERENCES

(a) The National Security Act of 1947, as amended.

(b) Counterintelligence Enhancement Act of 2002, as amended.

(c) Intelligence Reform and Terrorism Prevention Act of 2004, as amended.

(d) Title 5, Code of Federal Regulations (CFR), Part 732 “National Security Positions.”

(e) Title 32, CFR, Parts 2001 and 2003 “Classified National Security Information.”

(f) Intelligence Community Directive (ICD) 700, “Protection of National Intelligence,” dated June 7, 2012.

(g) ICD 701, “Security Policy Directive for Unauthorized Disclosures of Classified Information,” dated December 22, 2017.

(h) EO 12968, Access to Classified information, as amended, dated August 2, 1995.

(i) EO 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, dated June 30, 2008 (Amended by EO 13869, April 24, 2019).

(j) EO 13526, as amended, Classified National Security Information, dated December 29, 2009.

(k) EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated October 7, 2011.

(l) EO 12333, as amended, United States Intelligence Activities, dated December 4, 1981.

(m) Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 21, 2012.

(n) Presidential Decision Directive/NSC-12, Security Awareness and Reporting of Foreign Contacts, dated August 5, 1993.

(o) Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, dated June 12, 2017.

(p) Security Executive Agent Directive 6, Continuous Evaluation, dated January 12, 2018.

(q) Performance Accountability Council Memorandum, Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards, dated December 6, 2012.

(r) GSA Order OAS 5775.1 CHGE 2, Foreign Travel Policy, August 2, 2017.

(s) GSA Order OAS 7880.1B, Acceptance of Gifts and Decorations from Foreign Governments and the Giving of Gifts to Foreign Individuals by GSA Employees, August 22, 2016.