

United States of America DEPARTMENT OF COMMERCE	DEPARTMENT ADMINISTRATIVE ORDER <u>207-12</u>	
DEPARTMENT ADMINISTRATIVE ORDER SERIES	DATE OF ISSUANCE April 12, 2006	EFFECTIVE DATE April 12, 2006
	SUBJECT  FOREIGN NATIONAL VISITOR AND GUEST ACCESS PROGRAM	
<p><u>SECTION 1. PURPOSE.</u></p> <p>This Order sets forth Department of Commerce (the Department) policies and procedures for Foreign National Visitor and Guest access to DOC facilities.</p> <p><u>SECTION 2. SCOPE.</u></p> <p>.01 This Order applies to all DOC operating units, bureaus, and Departmental offices and to all Foreign Nationals who visit or are assigned to DOC facilities or activities. This Order also provides guidance for DOC organizations regarding information to be provided to the Office of Security (OSY) concerning Foreign National Visitors and Guests; the steps that must be taken to protect sensitive DOC information from unauthorized disclosure; and the requirement to report suspicious activities by any Foreign National that places a DOC facility, operation, or program at risk.</p> <p><u>SECTION 3. DEFINITIONS.</u></p> <p>.01 <u>Agency Check(s)</u> - A procedure whereby a request is made to one or more U.S Government agencies to determine whether information exists on a particular Foreign National. Examples may include the FBI (Federal Bureau of Investigations), BICE (Bureau of Immigration and Customs Enforcement), Department of State and other appropriate agencies that maintain such information.</p> <p>.02 <u>Commerce Control List</u> - The list of items (i.e., commodities, software, and technology) subject to the export licensing authority of the Bureau of Industry and Security.</p> <p>.03 <u>Controlled Technology</u> - Technology that is required for the development, production, or use of items on the Commerce Control List.</p> <p>.04 <u>Countries of Proliferation Concern</u> - Countries so designated by the Department of State for seeking advanced weapons capabilities that would present a threat to international security.</p> <p>.05 <u>Deemed Export</u> - Any release of technology or source code subject to the Export Administration Regulations to a Foreign National within the United States. Such a release is deemed to be an export to the home country or countries of the Foreign National. This deemed export rule does not apply to persons lawfully admitted for permanent residence in the United States or to persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).</p>		

- .06 Departmental Sponsor (DS) - A U.S. Citizen employee of the Department responsible for the day-to-day activities associated with the successful accomplishment of a foreign visit and for taking all reasonable steps to protect classified, Sensitive But Unclassified (SBU), or otherwise controlled, proprietary, or not-for-public release data, information, or technology from unauthorized physical, visual, and virtual access by a Foreign National Visitor or Guest.
- .07 Escort – A U.S. citizen employee of the Department assigned the responsibility of accompanying a Foreign National Visitor or Guest who lacks authorized access within a facility in order to ensure adherence to security measures protecting classified, SBU, or otherwise controlled, proprietary, or not-for-public release data, information, or technology from physical, visual, or virtual access.
- .08 Facility - An educational institution, manufacturing plant, laboratory, vessel, office building or complex of buildings located on a site that is operated and protected as one unit by the Department or its contractor.
- .09 Foreign National – Any person who is not a citizen or national of the United States.
- .10 Foreign Visit - Any access by a Foreign National to a DOC facility, regardless of the length of time involved. Foreign Nationals are, however, categorized as Visitors or Guests depending upon the length of their visit (See Section 4 .02).
- .11 Lawful Permanent Resident - A non-U.S. Citizen living in the United States who has been granted the right to permanently reside and work in the United States; previously referred to as a Permanent Resident Alien or “green card holder.”
- .12 National Security - The national defense and foreign relations of the United States.
- .13 Protected Person - A non-U.S. Citizen granted asylum under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).
- .14 Sensitive But Unclassified - Specific information that, while not classified, requires protection from disclosure.
- .15 Servicing Security Office - A field office of the Office of Security that provides security services, support, and guidance to DOC organizations. A servicing security office may provide services and support to a single bureau or may provide services and support to all DOC organizations in a given geographical area.
- .16 State Sponsors of Terrorism - Countries so designated by the Department of State as sponsors of groups and/or activities that support terrorism or terrorist activities and are on the List of State Sponsors of Terrorism.
- .17 Technology - Specific information necessary for the development, production or use of a product; the information may take the form of technical data or technical assistance.

.18 Visa - A permit to enter the United States that establishes a particular status (immigrant/non-immigrant, student, exchange visitor, diplomat, etc.) evidenced by a stamp in the Foreign National's passport or his/her status as noted on Form I-94 or I-95. A Form I-94 (Arrival-Departure Record) or Form I-95 (Crewman's Landing Permit) shows the date a Foreign National arrived in the United States and the "Admitted Until" date – the date the authorized period of stay expires. A Foreign National receives a Form I-94 or I-95 upon arrival at a U.S. port-of-entry. Of note, a visa is not a guarantee that the Foreign National will be permitted to enter the United States. Final approval for a Foreign National to enter the United States rests with Bureau of Immigration and Customs Enforcement officials at the port-of-entry.

#### SECTION 4. CATEGORIES OF VISITS BY FOREIGN NATIONALS.

.01 Foreign Nationals are any persons who are not citizens or nationals of the United States.

.02 For the purpose of this Order, Foreign Nationals are categorized based on the length of their visit. The length of a visit is delineated by the date of initial arrival at and final departure from any and all facilities of a particular Departmental bureau or operating unit; e.g. a visit to a headquarters office one day and a field site on a subsequent day is single visit.

a. Visitors are those who are accessing Departmental facilities for three or fewer days or attending a conference of five or fewer days.

1. A conference is defined as a colloquium, seminar, or symposium sponsored by any Departmental bureau or operating unit for the specific purpose of exchanging information, knowledge, or views, no matter whether it is held in a Departmental facility.

2. A Foreign National attending a conference that requests a follow-on visit for three or fewer additional days will remain categorized as a Visitor.

b. Guests are those who are accessing Departmental facilities for more than three days. Guests are subject to a security check at the discretion of the Director for Security. Guests remaining beyond two years must undergo a security check conducted by the servicing security office. The servicing security office will notify Departmental Sponsors that those Guests are required to complete and sign the paperwork (SF-85; credit release, etc.) necessary to conduct the check. A Guest's failure to complete and sign the necessary paperwork will result in termination of the Guest's access to DOC facilities.

.03 This DAO does not apply to:

a. Lawful Permanent Residents or Protected Persons (both must present evidence of their status).

b. Foreign Nationals who are employees of DOC residing and working at DOC facilities outside of the United States.

c. Foreign National diplomats and senior government officials at the ambassadorial or vice-ministerial level or above who visit DOC officials for the purpose of high-level policy dialogue. The Departmental Sponsor (DS) will coordinate with the servicing security office to determine if a Foreign National meets the aforementioned criteria. Accompanying staff members or advance teams shall be treated as Visitors or Guests pursuant to this Order.

d. Foreign Nationals who visit DOC 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). Facility managers must coordinate with the servicing security office to designate as public access any areas that require Foreign National Visitors or Guests to pass through an access control point, and must maintain written documentation of such designation.

## SECTION 5. GENERAL PROVISIONS.

.01 Balance between openness and security. Because the Department recognizes the value of their contributions to U.S. scientific and technological efforts and other Departmental functions, it offers Foreign National Visitors and Guests access to its facilities, staff and information while engaged in a broad range of collaborative activities. This access, however, must be balanced with the need to protect classified, Sensitive But Unclassified (SBU), or otherwise controlled, proprietary, or not-for-public release data, information, or technology.

.02 Departmental Sponsor. The Departmental Sponsor (DS) is a U.S. Citizen employee of the Department who is charged with responsibility for the successful completion of a foreign visit and for taking all reasonable steps to protect classified, SBU, or otherwise controlled, proprietary, or not-for-public release data, information, or technology from unauthorized physical, visual, and virtual access by a Foreign National Visitor or Guest

.03 Departmental Sponsor Responsibilities. The DS is responsible for taking all reasonable steps to ensure that the conduct of, and activities for, their Foreign National Visitor or Guest are appropriate for the Federal workplace and comply with this Order. Prior to the arrival of a Foreign National Guest, the DS shall coordinate with the servicing security office to obtain a counterintelligence briefing that includes the contents of the Espionage Indicator Guide (Attachment 1) for employees of the sponsoring bureau within the work area encompassed by the foreign visit. Because of the frequency of foreign visits, these employees need only be briefed on an annual basis rather than each time a foreign visit occurs. The DS must read and sign a Certification of Conditions and Responsibilities for the Departmental Sponsor of Foreign National Guests (Attachment 2) and forward the certification to the chief administrative official or other appropriate senior bureau official responsible for administrative matters in the sponsoring bureau for review and endorsement. The DS must also:

a. Comply with all requirements for access approval and conduct, including providing timely, complete, and accurate information regarding the visit to the servicing security office. The servicing security office will deny access to a Foreign National if the DS fails to provide complete and accurate information in advance of a visit.

- b. Take all reasonable steps to ensure his/her Foreign National Visitor or Guest is given access only to information necessary for the successful completion of their visit.
- c. Prevent physical, visual, and virtual access to classified, Sensitive But Unclassified (SBU), or otherwise controlled, proprietary, or not-for-public release data, information, or technology. Exceptions may occur when there is explicit written authorization for access to non-classified information, and when necessary, a license has been issued to the sponsoring bureau by the Bureau of Industry and Security pursuant to the Export Administration Regulations or by any other U.S. Government agency with appropriate jurisdiction.
- d. Take all reasonable steps to ensure that a Foreign National Visitor or Guest does not use personal communication, photographic, recording, or other electronic devices in those areas of Departmental facilities where classified, SBU, or otherwise controlled, proprietary, or not-for-public release data, information, or technology is present without explicit authorization. (See Section 5 .09.)
- e. Immediately report suspicious activities or anomalies involving Foreign National Visitors or Guests to the servicing security office.
- f. Promptly notify the servicing security office if there is a change to the arrival or departure date of any Foreign National.
- g. Ensure that all Foreign National Guests meet with the servicing security office to complete the Certification of Conditions and Responsibilities for the Foreign National Guest Program (Attachment 3) within three days of arrival if the servicing security office is collocated. If the servicing security office is not collocated, the DS will brief the Foreign National Guest on the contents of the document, and ensure the certification is signed, dated, and forwarded to the servicing security office within three days of arrival.
- h. The appropriate senior administrative official in the sponsoring bureau or office will review the request from the Departmental Sponsor and will ensure that the value of collaborative efforts gained with access to Departmental facilities, staff and information is balanced with the need to protect classified, Sensitive But Unclassified (SBU), or otherwise controlled, proprietary, or not-for-public release data, information, or technology. The senior administrative official's endorsement and Departmental Sponsor's certificate (Attachment 2) will be forwarded to the servicing security Office.

.04 Revocation of DS approval. The Director for Security may revoke DS approval for any employee who violates the provisions of this Order. The servicing security office will review alleged violations of this directive to determine if any corrective action is required. Violations may also form the basis for other administrative or disciplinary actions (e.g., knowingly facilitating access for a Foreign National who has previously been denied access). Violations may result in administrative action or disciplinary action under the provisions of DAO 202-751, "Discipline."

.05 Major Considerations. Servicing security offices will use a risk-based methodology to approve access by Foreign Nationals. Major considerations include:

- a. The Foreign National’s country of citizenship, dual citizenship, residence, and birth.
- b. The critical nature of technology, information, or other material to which the Foreign National may have physical, visual, or virtual access.
- c. The Departmental Sponsor’s history of compliance with this Order.
- d. The security status of the DOC facility as indicated by existing physical and cyber controls established in compliance with DOC and Federal regulations and standards.
- e. The length of visit.

.06 Advance Notice and Information Required by Category of Foreign National.

<b>Category</b>	<b>Visitor</b> 3 or fewer days or attending a conference of 5 or fewer days	<b>Guest</b> More than 3 days
<b>Advanced Notice Required</b>	As soon as the information is received but no later than one full business day prior to the visit	30 calendar days prior to arrival
<b>Information Required (same for both categories)</b>	Full name Gender Date of birth Place of birth Passport Number and Issuing Country Citizenship and Country(ies) of Dual Citizenship (if applicable) Country of Current Residence Sponsoring Bureau Purpose of Visit Facility number and location Arrival date Departure date DS name DS telephone number DS email address	Full name Gender Date of birth Place of birth Passport Number and Issuing Country Citizenship and Country(ies) of Dual citizenship (if applicable) Country of Current Residence Sponsoring Bureau Purpose of Visit Facility number and location Arrival date Departure date DS name DS telephone number DS email address

.07 Approvals. Based upon the information required concerning each Foreign National, OSY Headquarters will conduct applicable agency checks and forward the results to the servicing security office. The servicing security office will make a risk assessment determination and notify the Departmental Sponsor of approval or denial of access. In the event of denial of access, a senior executive of the affected bureau, operating unit, or office may appeal to the Director for Security who will consider whether the benefits of a proposed visit justify the risks.

.08 Escort Requirements. Foreign National Visitors must be escorted by a U.S. Citizen employee of the Department at all times while on Departmental property, except in areas that are open to the general public. Foreign National Guests may be granted unescorted access to designated areas of a facility upon approval by the servicing security office. Approval rests upon the favorable completion of applicable agency checks and a determination that no unauthorized physical, visual, or virtual access to classified, Sensitive But Unclassified (SBU), or otherwise controlled, proprietary, or not-for-public release data, information, or technology is likely to occur.

.09 Use of Personal Electronic Devices. Foreign Nationals may not use personal communication, photographic, recording, or other electronic devices in those areas of Departmental facilities where classified, SBU, or otherwise controlled, proprietary, or not-for-public release data, information, or technology is present without the explicit authorization of their Departmental Sponsor. These devices include but are not limited to 'blackberries,' cell phones/camera phones, still or video cameras, laptops, pagers, Personal Data Assistants, etc. Departmental Sponsors must take all reasonable steps to ensure that adequate measures are in place to protect against collection of said data, information, or technology before authorizing use of such devices. If adequate measures are not in place to do so, Departmental Sponsors must ensure that Foreign Nationals turn-off all such devices upon entry to an area where said data, information, or technology is present. Departmental Sponsors must remain aware of all use of such devices throughout the length of a visit. Guidance concerning adequate protective measures may be obtained from the servicing security office.

.10 Export Licenses. Approval of a visit by a Foreign National Visitor or Guest under this Order does not substitute for a license issued by the Bureau of Industry and Security pursuant to the Export Administration Regulations or any other U.S. Government agency with appropriate jurisdiction.

.11 On-site Reviews. OSY will conduct announced and unannounced on-site reviews to ensure compliance with this Order.

.12 Debriefing. During the course of a visit by, or upon the departure of, select Visitors and Guests, particularly those from countries designated as State Sponsors of Terrorism and Countries of Proliferation Concern, the servicing security office or OSY Headquarters will conduct a debriefing of the Departmental Sponsor and other employees of the Department who have had contact with the Foreign National.

SECTION 6. RECORDS.

Office of Security Headquarters and the servicing security office will maintain a database containing identifying data for all Foreign National Visitors and Guests to which this Order applies.

---

Director for Security

---

Chief Financial Officer and  
Assistant Secretary for Administration

## **Espionage Indicators Guide**

Espionage indicators are signs that an individual, either a DOC employee or a Foreign National Visitor or Guest may be involved in illegal collection of information on behalf of a foreign intelligence organization. The purpose of this guide is to provide you with common indicators of questionable behavior that may place sensitive U.S. Government information at risk. If you become aware of any attempts by Foreign National Visitors or Guests or Departmental employees to exploit their working relationship within the Department with the intent to commit espionage, you must report this information to your servicing security office. Continuing studies of past espionage cases show that employees often overlooked or failed to report espionage indicators which, had they been reported, would have permitted earlier detection of espionage.

If your reporting helps stop a case of espionage, you may be eligible for a reward of up to \$500,000. The reward is authorized by an amendment to Title 18, U.S.C., Section 3071, which authorizes the Attorney General to make payment for information on espionage activity in any country, which leads to the arrest and conviction of any person(s):

- For commission of an act of espionage against the United States; or
- For conspiring or attempting to commit an act of espionage against the United States.

Also, you may be eligible for a reward for information which leads to the prevention or hindrance of an act of espionage against the United States. Some of the following indicators are clear evidence of improper behavior. Others probably have an innocent explanation but are sufficiently noteworthy that your servicing security office should be informed so the activity can be assessed and evaluated.

### **Potential Indicators of Espionage**

- Disgruntlement with the U.S. Government strong enough to cause an individual to seek or wish for revenge.
- Any statement that suggests conflicting loyalties may affect the proper handling and protection of sensitive information.
- Active attempts to encourage others to violate laws or disobey security policies and procedures.
- Membership in, or attempt to conceal membership in, any group which: 1) advocates the use of force or violence to cause political change within the United States, 2) has been identified as a front group for foreign interests, or 3) advocates loyalty to a foreign interest.
- Repeated statements or actions indicating an abnormal fascination with and strong desire to engage in "spy" work.

### **Potential Indicators of Information Collection**

- Asking others to obtain or facilitate access to classified material or unclassified but sensitive information to which one does not have authorized access.
- Obtaining or attempting to obtain a witness signature on a classified document destruction record when the witness did not observe the destruction.
- Offering money to a person with a sensitive job in what appears to be an attempt to entice that person into some unspecified illegal activity.

- Undue curiosity or requests for information about matters not within the scope of the individual's job or need-to-know.
- Unauthorized removal or attempts to remove unclassified, classified, export-controlled, proprietary or other protected material from the work area.
- Retention of classified, export-controlled, proprietary, or other sensitive information obtained through previous employment without the authorization or the knowledge of that employer.
- Extensive, unexplained use of copier, facsimile, or computer equipment to reproduce or transmit unclassified, sensitive, classified, proprietary or export-controlled material.
- Taking classified or sensitive materials home purportedly for work reasons, without proper authorization.
- Working odd hours when others are not in the office or visiting other work areas after normal hours for no logical reason.
- Bringing cameras or recording devices, without approval, into areas storing classified, sensitive or export-controlled material.

#### **Potential Indicators of Unauthorized Information Transmittal**

- Storing classified material at home or any other unauthorized place.
- Short trips that are inconsistent with one's apparent interests and financial means, to foreign countries or to U.S. cities (e.g., New York City.) with foreign diplomatic facilities.
- Excessive use of email or fax.
- Failure to comply with regulations for reporting foreign contacts or foreign travel.
- Attempts to conceal foreign travel or close and continuing contact with a foreign national.
- Foreign travel not reflected in the individual's passport to countries where entries would normally be stamped.
- Maintaining ongoing personal contact with diplomatic or other representatives from countries with which one has ethnic, religious, cultural or other emotional ties or obligations, or with employees of competing companies in those countries.

#### **Potential Indicators of Illegal Income**

- Unexplained affluence, or life-style inconsistent with known income. Notably, sudden purchase of high-value items or unusually frequent personal travel, which appears to be beyond known income. Sudden repayment of large debts or loans, indicating sudden reversal of financial difficulties.
- Joking or bragging about working for a foreign intelligence service, or having a mysterious source of income.

#### **Other Potential Indicators of Concern**

- Behavior indicating concern that one is being investigated or watched, such as actions to detect physical surveillance, searching for listening devices or cameras, and leaving "traps" to detect search of the individual's work area or home.
- Any part-time employment or other outside activity that may create a conflict of interest with one's obligation to protect classified or sensitive but unclassified information.

It is important to emphasize that the existence of one or two of the aforementioned factors does not necessarily mean that a person is engaged in espionage activity. However, the risk

that someone may be involved in espionage against the DOC increases when these elements are present. When in doubt report it!

If you believe that someone may be contemplating espionage or other criminal activity, or has taken steps to initiate it, you are obligated to immediately report this information to the Office of Security Headquarters through your servicing security office.

**Certification of Conditions and Responsibilities for  
Departmental Sponsors of Foreign National Guests**

I understand and acknowledge that I have been designated as the Departmental Sponsor (DS) for \_\_\_\_\_, a Foreign National Guest. I understand that I am responsible for taking all reasonable steps for ensuring that the conduct and activities of this Foreign National Guest are appropriate for the Federal workplace and comply with this Order and other applicable security directives. I further understand, acknowledge, and certify that I shall comply with the following conditions and responsibilities including providing timely, complete and accurate information to the Office of Security.

1. I will promptly notify the servicing security office if there is any change to the arrival or departure date of my Foreign National Guest.
2. I will ensure my Foreign National Guest meets with the servicing security office within three days of arrival to receive and sign the Certificate of Conditions and Responsibilities for the Foreign National Guest program. In the event the servicing security office is not located within my facility, I will provide the required briefing and ensure the certification is signed and forwarded to the servicing security office within three days of the Guest's arrival.
3. My Foreign National Guest's normal work area will be \_\_\_\_\_. I will take all reasonable steps to ensure that my Guest will not have unauthorized physical, visual, or virtual access to classified, Sensitive But Unclassified (SBU), and otherwise controlled, proprietary, or not-for-public release data, information, or technology. This specifically includes but is not limited to access to technology on the Commerce Control List, sensitive economic data, and trade policies or practices not approved for public release unless properly authorized by appropriate Departmental officials and, when necessary, licensed by the Bureau of Industry and Security or any other U.S. Government agency with appropriate jurisdiction.
4. I will only provide my Foreign National Guest with access to information or technology necessary to the successful completion of the visit in accordance with the Guest Researcher Agreement/Memorandum of Understanding, Intergovernmental Personnel Act, or other applicable document governing the terms of the visit.
5. I will take all reasonable steps to ensure that my Foreign National Guest does not use personal communication, photographic, recording, or other electronic devices in those areas of Departmental facilities where classified, SBU, or otherwise controlled, proprietary, or not-for-public release data, information, or technology is present without explicit authorization and unless adequate protective measures are in place to protect against collection of the same.

6. I will inform my Foreign National Guest that he/she shall not use his/her tenure with DOC or his/her DOC photo identification badge to arrange or sponsor visits by other individuals to DOC or other U.S. Government and /or privately owned facilities. Any requests for visits must be approved and arranged by me.

7. I will inform my Foreign National Guest that he/she must, upon request, consent to a security check and complete and sign the paperwork necessary to conduct the check. I will further inform my Guest that his/her failure to consent to a security check or to complete and sign the necessary paperwork will result in termination of his/her access to DOC facilities.

8. I will report any suspicious activities or anomalies involving my Foreign National Guest to the servicing security office.

9. I have read, understand, and shall comply with all applicable security regulations of the Foreign National Guest Program.

\_\_\_\_\_  
(Typed Name)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Title)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Bureau and Telephone Number)

\_\_\_\_\_  
(Address)

**Endorsement by the Senior Administrative Official**

Concur/Nonconcur with the request of the Departmental Sponsor.

\_\_\_\_\_  
Name/Title

\_\_\_\_\_  
Date

**Certification of Conditions and Responsibilities  
for a Foreign National Guest**

I understand and acknowledge that I have been approved for access as a Guest of the Department of Commerce's \_\_\_\_\_

(insert bureau, operating unit or office)

to engage in collaborative activity concerning \_\_\_\_\_

(insert specific program description or name)

at \_\_\_\_\_.

(insert facility name and location).

I further understand, acknowledge, and certify that I shall comply with the following conditions and responsibilities:

1. The overall purpose of my visit is to participate in a collaborative activity with Departmental staff or to provide expertise to the Department of Commerce. I shall have no access to information or technology except as required to successfully complete my visit in accordance with my Guest Researcher Agreement/Memorandum of Understanding, Intergovernmental Personnel Act, or other applicable document governing the terms of my visit as determined by my Departmental Sponsor, \_\_\_\_\_.  

(insert name)
2. I understand I will not be afforded unauthorized physical, visual, or virtual access to classified, Sensitive But Unclassified (SBU), and otherwise controlled, proprietary, or not-for-public release data, information, or technology. I understand that explicit written authorization and, when necessary, licensing by the Bureau of Industry and Security or other U.S. Government agencies is required for such access. This certification does not relieve me of obligations to comply with any and all requirements of any license that the Bureau of Industry and Security, or any other U.S. Government agency, may issue to authorize my access to certain items, information, or technology.
3. I shall perform only functions directly related to my Guest Researcher Agreement/Memorandum of Understanding, Intergovernmental Personnel Act, or other applicable document governing the terms of my visit and shall not act in any other capacity on behalf of my government or any other entity during the period of my visit.
4. I will not use personal communication, photographic, recording, or other electronic devices in Departmental facilities, except in areas open to the general public, without explicit authorization from my Departmental Sponsor. I understand that such devices include but are not limited to 'blackberries,' cell phones/camera phones, still or video cameras, laptops, pagers, Personal Data Assistants, etc.
5. All unpublished information or controlled technology or source code to which I may have access pursuant to a license or other written authorization during this assignment is the property of the U.S. Government and shall not be further released or disclosed by me to any other person, firm, organization or government without proper U.S. Government authorization.
6. I will immediately report to my Departmental Sponsor and the Office of Security all attempts from individuals without a need to know to obtain classified, SBU, and otherwise controlled, proprietary, or not-for-public release data, information, or technology.

7. I understand I am not authorized to approve visits by other individuals to DOC facilities and will not use my assignment with DOC or my DOC photo-identification badge to arrange any visits. If my duties make it necessary for me to make visits to other U.S. Government and/or privately owned facilities, the visits will be arranged and coordinated by my Departmental Sponsor.

8. I understand that I will have unescorted access to \_\_\_\_\_  
(insert designated areas)  
of \_\_\_\_\_ during normal working hours as determined by my  
(insert building name(s) and number(s))  
Departmental Sponsor Access during other hours or to other parts of Departmental facilities must be approved by my Departmental Sponsor and shall be in compliance with DOC escort requirements.

9. Upon request, I will consent to a security check and complete and sign the paperwork necessary to conduct the check. I understand that my failure to consent to a security check or to complete and sign the necessary paperwork will result in termination of my access to DOC facilities.

10. I have been briefed on, understand, and shall comply with all applicable security regulations of the Foreign National Guest Program.

\_\_\_\_\_  
(Typed Name)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Title)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Bureau and Telephone Number)

\_\_\_\_\_  
(Address)