NAO 207-12
Eff: 5/11/06; Iss: 5/19/06

TECHNOLOGY CONTROLS AND FOREIGN NATIONAL ACCESS

SECTION 1. PURPOSE.

This Order sets forth National Oceanic and Atmospheric Administration (NOAA) procedures for foreign national visitors and guests' access to NOAA facilities. This Order implements Department Administrative Order (DAO) 207-12, Foreign National Visitor and Guest Access Program. This Order also sets forth responsibilities and requirements to safeguard technology subject to Export Administration Regulations (EAR) controls to prevent inappropriate release or transfer of controlled technology (actual or deemed) to foreign nationals. The EAR is administered and regulated by the Department of Commerce (DOC) Bureau of Industry and Security (BIS).

SECTION 2. SCOPE.

.01 The Export Administration Regulations (EAR), 15 CFR Parts 730-774**,** place certain requirements on NOAA and its employees; and on NOAA contractors, grantees, and other recipients of NOAA funds. This Order applies to all NOAA entities, employees, contractors, grantees, and recipients of NOAA funds, and to all foreign national visitors and guests in NOAA facilities or participating in NOAA activities. However, the Order does not apply to foreign nationals in a NOAA facility for law enforcement purposes.

.02 This Order provides guidance for NOAA organizations regarding their responsibilities in identifying and safeguarding sensitive technology subject to EAR controls prohibiting unauthorized access by, or transfer to, foreign nationals. The Order also establishes requirements for obtaining appropriate clearances on foreign national visitors and guests seeking access to NOAA facilities; requirements for reporting information to the DOC Office of Security (OSY) regarding such foreign nationals; and requirements to report suspicious activities by a foreign national that may place a NOAA facility, activity, or program at risk.

SECTION 3. DEFINITIONS.

.01 Agency Checks - A procedure whereby a request is made by DOC/OSY to appropriate U.S. Government agencies to determine whether information exists on a particular foreign national. The list of agencies includes the Federal Bureau of Investigation (FBI), Bureau of Immigration and Customs Enforcement (BICE), Department of State, and other agencies that maintain such information.

.02 Agreed upon international program or project - A program or project that has been established pursuant to an appropriately signed agreement between NOAA or a NOAA Line Office (LO) or Staff Office (SO) and a foreign agency or organization, an international organization, or a U.S.-based organization with international membership.

.03 Commerce Control List (CCL) - The list of items (i.e., commodities, software, and technology) subject to the export licensing authority of BIS (15 CFR 774).

.04 Controlled technology - Items and technology that are required for the development, production, or use of the items on the CCL and that are subject to EAR controls. Controlled technology includes dual use items which are items that have both commercial and military or proliferation applications. Whether a deemed export license is required in any particular situation is determined by the home country designation of the foreign national and the type of access that foreign national has to the technology.

.05 Controlled Technology Coordinator (CTC) - The NOAA employee, designated by each NOAA Assistant Administrator (AA), Corporate Office (CO), and SO Director, responsible for managing and coordinating foreign national access and deemed export compliance activities. The CTC shall be responsible for planning and implementation of foreign national and deemed export compliance activities within his/her organization. The CTC shall assist the Departmental Sponsors/NOAA (DSNs) in performing their roles in an appropriate manner and in accordance with this Order and other related DOC and NOAA policies and procedures. The CTC may also be the individual who serves as the LO Deemed Export Steering Committee member.

.06 Deemed Export - Any release of technology or source code subject to the EAR 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)).

.07 Departmental Sponsor/NOAA (DSN) - The NOAA employee responsible for the day-to-day activities associated with the successful accomplishment of a foreign visit at the DSN's location. The DSN must take all reasonable steps to protect classified, Sensitive But Unclassified (SBU), export controlled, 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. A foreign national cannot host another foreign national. The DSN must be a U.S. citizen.

.08 EAR 99 Items - Items subject to the EAR that are not elsewhere controlled by the CCL category or in any other category in the CCL; they are designated by the number EAR 99.

.09 Escort - A U.S. citizen employee of NOAA assigned the responsibility of accompanying a foreign national visitor or guest who lacks authorized access within a facility in order to ensure adherence to (1) security measures and (2) technology controls as required by the EAR.

.10 Exports - Any item transported from the United States to a foreign destination is an export. How an item is transported (shipped, hand-carried, regular mail, e-mail, fax, telephone conversations, software uploads/downloads) outside of the United States does not matter in determining export license requirements. An item may be considered an export even if it is leaving the United States temporarily, if it is leaving the United States but is not for sale (e.g., a gift), or if it is going to a wholly-owned U.S. subsidiary in a foreign country. Even a foreign-origin item exported from the United States, transmitted or transshipped through the United States, or being returned from the United States to its foreign country of origin may be considered an export. Finally, release of technology or source code subject to the EAR to a foreign national in the United States is "deemed" to be an export to the home country of the foreign national under the EAR (15 CFR 734.2(b)).

.11 Facility - An office building; a laboratory; ship, aircraft, or other vessel; or a complex of buildings located on a site that is operated and protected as one unit by DOC/NOAA or its contractors.

.12 Foreign National - A person who was born outside the jurisdiction of the United States, who is subject to a foreign government, and who has not been naturalized under U.S. law. This includes foreign national contractors and vendors. As used in this Order, and for the purposes of EAR controls, a “foreign national” subject to the deemed export rule is an individual who is not a citizen of the United States, not a legal permanent resident (meaning not a "permanent resident alien" or "Green Card" holder), and not a "protected individual" under 8 U.S.C. 1324b(a)(3). As a practical matter, foreign nationals present in NOAA facilities may likely include employees, contractors, vendors, tourists, students, business persons, scholars, researchers, technical experts, military personnel, and diplomats but may include other categories of visitors or guests. One exception to this general statement is for a "protected person," which includes political refugees and political asylum holders.

.13 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 definitions below and Section 5.08 of this Order).

.14 Guests - Guests are those foreign nationals accessing NOAA facilities for more than three days, including foreign nationals conducting work at a NOAA facility under a grant, contract, or cooperative arrangement or agreement, where such work requires access to NOAA facilities. 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 DSNs when those guests are required to

complete and sign the necessary paperwork (SF-85, credit release, etc.) 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.

.15 Lawful Permanent Resident (LPR) - 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. Unlike a U.S. citizen, however, an LPR does not have the right to vote and can be deported if, for example, convicted of certain crimes. An LPR is also known as a permanent resident alien or Green Card holder.

.16 National Security - The national defense and foreign relations of the United States.

.17 Protected Person - A non-U.S. citizen granted asylum under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)). "Protected person" includes political refugees and political asylum holders.

.18 Sensitive But Unclassified (SBU) - Specific information that, while not classified, requires protection from disclosure. SBU is one of several security classifications applied to sensitive information or documents. Information or documents designated as SBU will be marked accordingly.

.19 Servicing Security Office - A field office of DOC/OSY 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.

.20 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 (see www.state.gov).

.21 Technology - As defined in 15 CFR 772.1, "The specific information necessary for the development, production, or use of a product. The information takes the form of 'technical data' or 'technical assistance.'"

.22 Visa - A permit to enter the Unites 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 BICE officials at the port-of-entry.

.23 Visitor - Visitors are foreign nationals who access NOAA facilities for three days or less, or foreign nationals attending NOAA-sponsored conferences for five or fewer business days. A foreign national attending a conference who requests a follow-on visit for three or fewer additional days will remain categorized as a Visitor.

SECTION 4. GENERAL PROVISIONS.

Balance between openness and security. NOAA values the contributions of international collaborations to the scientific and technological strength of the United States and to NOAA mission success, and offers foreign national visitors and guests access to NOAA's facilities, staff, and information to participate in a broad range of activities. Meetings with and visits by foreign nationals and foreign representatives are a common means to facilitate interchange with NOAA's foreign scientific and technical counterparts in support of broad agency objectives and program goals. However, NOAA must balance this openness with the need to protect classified, SBU, export controlled, or otherwise controlled, proprietary, or not-for-public release data, information, or technology subject to EAR controls.

SECTION 5. FOREIGN NATIONAL ACCESS CONTROLS.

.01 Categorization. For the purpose of this Order, foreign nationals are categorized based on the length of their visit to a NOAA-controlled facility or platform (such as a ship or airplane). The length of a visit is delineated by the date of initial arrival at and final departure from any and all NOAA facilities (e.g., a visit to a headquarters office one day and to a field site on a subsequent day is a single visit).

a. Visitors are those foreign nationals who access NOAA facilities for three days or less, and foreign nationals attending NOAA-sponsored conferences for five or fewer business days. A conference is defined in DAO 207-12 as a colloquium, seminar, or symposium sponsored [by NOAA] for the specific purpose of exchanging information, knowledge, or views, no matter whether it is held in a Departmental facility. A foreign national attending a conference who conducts a follow-on visit for three or fewer additional days will remain categorized as a visitor.

b. Guests are those foreign nationals who are accessing NOAA 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 DSNs when 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.

.02 Exceptions. This Order does not apply to the following foreign nationals.

a. Foreign nationals who are employees of NOAA residing and working at NOAA facilities outside of the United States.

b. Foreign national diplomats and other foreign national senior government officials at the ambassadorial or vice-ministerial level who visit designated NOAA officials for the purpose of high-level policy dialogue. Accompanying staff members or advance teams shall be treated as visitors or guests pursuant to this Order. The DSN shall coordinate with the servicing security office to determine if a foreign national meets the aforementioned criteria.

c. Foreign nationals who visit NOAA facilities during public events or activities, or in locations that are open to the general public (e.g., 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 designations. Guards or NOAA employees (DSNs/designated others) shall be present to preclude access to restricted areas beyond those authorized for temporary public access.

.03 Responsibilities of the Departmental Sponsor/NOAA (DSN). The key to maintaining the optimal balance between openness and security is the DSN. The DSN is responsible for ensuring the accomplishment of the mission requirements during the time the foreign national is in the facility, and for protecting controlled information and technology from unauthorized physical, visual, or virtual access by the foreign national visitor or guest. The DSN shall take all reasonable steps to ensure that the conduct of, and activities for, his/her 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 at a NOAA facility, the DSN shall coordinate with the servicing security office to obtain a counterintelligence briefing that includes the contents of the Espionage Indicators Guide (see Appendix A to this Order) for the NOAA staff within the work area accessible to the foreign national. Because of the transient nature of foreign guests, the affected staff members will be briefed only on an annual basis rather than each time a foreign guest arrives at their work location. The guest's DSN must read and sign the Certification of Conditions and Responsibilities for the Departmental Sponsors of Foreign National Guests (see Appendix B to this Order). The DSN must also prepare any required supplemental materials and forward these documents to the CTC or other designated official for review. The DSN shall request DOC/OSY coordinate the administration of Espionage Indicators briefings as set forth in DAO 207-12. The DSN shall perform the following.

a. Comply with all requirements for access approval and conduct, including providing timely, complete, and accurate information regarding the visit or assignment to the servicing security office. The DSN shall contact the servicing security office regarding the requirements for reporting the visit or assignment and shall provide the required information prior to the visit or assignment. The servicing security office will take appropriate action (i.e., deny access to a foreign national visitor or guest) for failure by the DSN to provide complete and accurate information related to the specific foreign national in advance of the visit or assignment.

b. Take all reasonable steps to ensure that his/her foreign national visitor or guest is given access only to information necessary for the accomplishment of the mission requirements.

c. Take all reasonable steps to prevent physical, visual, and virtual access to classified, SBU, export controlled, 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, in circumstances involving export controlled technology, a license has been issued to NOAA by BIS pursuant to the EAR or by any other U.S. Government agency with appropriate jurisdiction. The DSN shall work with DOC/OSY to designate secure areas for NOAA sites in order to establish specific access controls to prevent unlicensed foreign nationals from physically, virtually, and/or visually accessing export controlled equipment, commodities, services, and/or technology. It is the responsibility of the DSN to work with the CTC and others in NOAA to apply for an export license in advance, if needed, requesting access for the foreign national to export controlled technology. When an export license is required, it must be approved before access is allowed. It is critical to check the foreign national visitor or guest against the most recent Denied Persons List, Unverified List, Entity List, Specially Designated Nationals List, and the Debarred List, which are maintained at http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm. Additional information on export licenses for dual-use items is available by contacting BIS or by visiting http://www.bis.doc.gov. Information on export licenses for munitions can be obtained by contacting the Department of State Directorate of Defense Trade Controls or by visiting www.pmdtc.org.

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, export controlled, or otherwise controlled, proprietary, or not-for-public release data, information, or technology is present without explicit authorization (see Section 5.11 of this Order).

e. Prohibit the connection of unauthorized electronic devices to Departmental networks and systems, and seek authorization from Information Technology staff, when necessary.

f. Report immediately any suspicious activities or anomalies involving foreign national visitors or guests to the servicing security office. Additionally, the DSN shall instruct NOAA staff and employees to report suspicious activities involving the foreign national to the DSN who, in turn, shall report them to the servicing security office immediately. For guidance on "suspicious activities," refer to the Espionage Indicators Guide (see Appendix A to this Order).

g. Notify the servicing security office immediately if there is a change to the arrival or departure date of any foreign national visitor or guest or any change in assignment.

h. Ensure the foreign national guest who will be accessing NOAA facilities meets with the servicing security office to complete the Certification of Conditions and Responsibilities for a Foreign National Guest (see Appendix C to this Order) within three days of arrival if the servicing security office is collocated. If the servicing security office is not collocated, the DSN 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.

.04 Responsibilities of the Controlled Technology Coordinator (CTC) or Other Designated Official. The CTC or other designated official will make a determination whether to support the DSN assessment that the value of collaborative efforts gained with access to Departmental facilities, staff, and information is balanced with the need to protect classified, SBU, export controlled, or otherwise controlled, proprietary, or not-for-public release data, information, or technology. This official shall forward Appendix B and supplemental materials to the senior administrative official for final review and endorsement.

.05 Responsibilities of the Senior Administrative Official. The senior administrative official will review the information provided by the CTC or other designated official and the DSN to ensure it adequately demonstrates that the value of collaborative efforts gained with access to Departmental facilities, staff, and information is balanced with the need to protect classified, SBU, export controlled, or otherwise controlled, proprietary, or not-for-public release data, information, or technology. The senior administrative official shall signify his/her endorsement in the appropriate location on the Certification of Conditions and Responsibilities for the Departmental Sponsors of Foreign National Guests (see Appendix B to this Order) and shall ensure this completed Certification is forwarded to the servicing security office.

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

.07 Major Considerations. A risk-based approach will be used by the servicing security office to approve access by foreign nationals. Major considerations include:

a. country of residence, country of citizenship, dual citizenship, and country of birth of the foreign national;

b. criticality of technology or information, or other material to which the foreign national may have physical, visual, or virtual access;

c. sponsor compliance history with this Order;

d. security status of the NOAA facility as indicated by existing physical and cyber controls established in compliance with DOC and federal regulations and standards;

e. length of visit or assignment; and

f. applicability of export control laws and regulations to the equipment and/or technology to be accessed (licensing agencies will be involved in making those decisions).

.08 Advance Notice and Information Required by Category of Foreign National. The following information shall be provided to the servicing security office by the requesting DSN based on the expected number of days of the visit.

Category	**VISITOR** Foreign Nationals - accessing NOAA facilities 3 days or less, or - Attending conferences for 5 or fewer days	**GUEST** Foreign Nationals accessing NOAA facilities more than 3 days – including employees under contracts, grants, cooperative agreements
Advanced Notice Required	Provide servicing security office with required information as soon as the information is received but no later than one full business day prior to the visit and prior to access beyond an access control point	Provide servicing security office with required information 30 calendar days prior to arrival
Information Required (same for both categories)	- 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/phone 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/phone number - DS email address

.09 Approvals. Based upon the information obtained on each foreign national, the 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 DSN of approval or denial of access. In the event of denial of access, a NOAA senior executive may appeal to the Director for Security who will consider whether the benefits of a proposed visit justify the risks.

.10 Escort Requirements. Foreign national visitors must be escorted at all times by a U.S. citizen employee of NOAA while on NOAA property. Foreign national guests may be granted unescorted access to certain areas of a facility upon approval by the servicing security office. Approval rests on the favorable completion of applicable agency checks and a determination that no unauthorized physical, visual, or virtual access to classified, SBU, export controlled, or

otherwise controlled, proprietary, or not-for-public release data, information, or technology is likely to occur.

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

.12 Export Licenses. Approval of a visit by a foreign national visitor or guest under this Order does not substitute for a license issued by BIS under the provisions of the EAR.

.13 On-Site Reviews. Servicing security offices will conduct announced and unannounced on-site reviews of guests to ensure denial of unauthorized access to controlled information or technology (e.g., National Security Information and SBU material, unlicensed deemed export), to ensure adherence to physical security procedures (e.g., wearing of building badge, adequate access controls), and to ensure overall compliance with DAO 207-12.

.14 Debriefing. During the course of a visit by, or upon the departure of, select foreign national visitors or guests assessed as high risk or from a country designated by the Department of State as a state sponsor of terrorism (see http://www.state.gov/), the servicing security office or OSY Headquarters will conduct a debriefing of the foreign national's DSN and other NOAA employees who have had contact with the foreign national.

SECTION 6. DEEMED EXPORT CONTROLS.

.01 General Requirement. Under the EAR, an export of technology or source code is "deemed" to take place when it is released to a foreign national within the United States. Technology can be considered to be released to a foreign national when it is available to the foreign national for visual inspection (such as reading technical specifications, plans, blueprints, etc.), when technology is orally discussed, or when technology is made available by practice or application under the guidance of persons with knowledge of the technology. The analysis under the EAR is governed by the specifics of the transaction: what the item is, where it is going, who will receive it, and what it will be used for. Many U.S. commercial exports do not require a license, but the analysis under the EAR must be completed for each specific situation to determine if the release of technology requires a license. If an item or technology requires a license in order to be released to a foreign national, application must be made to BIS for an export license.

.02 Access Controls. Each LO/CO/SO responsible for technology subject to EAR controls must ensure appropriate access controls are established and documented for each facility within its control where there are EAR controlled items. Each such facility will have an access control plan that identifies all measures and procedures implemented at that facility to control foreign national access to technology regulated under the EAR, and demonstrates that the facility has instituted sufficient measures and procedures to assure full compliance with the EAR. One component of each access control plan is an access control information sheet for each controlled item at that facility, as discussed below.

a. To prepare the access control plan for each facility, each LO/CO/SO must review the particular situation found at that facility and take appropriate steps to control access based on site-specific factors. Such factors include physical layout of the facility, locations of EAR controlled technology within the facility, proximity of the facility to other parts of NOAA and other entities, and security measures already in place, or that may be put in place, for reasons other than export control. Additional factors include number, duties, and home country designation of foreign national guests and visitors at the facility as well as the frequency and nature of the visits. Even within a facility, there may be different approaches to controlling access to different groups of technology, depending on the nature of the technology and other factors.

b. An access control information sheet must be completed for each controlled item (with limited exceptions, where justified in the access control plan) and shall contain the information identified below.

- Date Access Control Information Sheet Prepared
- Item Name (and ECCN – Export Control Classification Number, if applicable)
- Responsible Individual/Title
- Organization
- Description of Item
- Physical Location(s) of Item(s)
- EAR Controls and Restrictions
- Individuals Authorized Access to Item
- Physical/Electronic Security/Access Control Measures Implemented to Ensure Only Authorized Access to Item
- Where to Report Access Control Violations

c. In most instances, EAR 99 items do not need individual access control information sheets. However, facilities that house such items do need an access control plan that describes how access is controlled.

d. The original access control plan shall reside with the LO/CO/SO's CTC or Steering Committee member. A copy of the access control plan for each facility requiring such a plan must be submitted to the Office of the Chief Administrative Officer (OCAO). Copies of all information sheets for controlled technology items at the facility shall accompany the plan. The original information sheet must be retained with the controlled item.

.03 Grants and Contracts. Grantees and contractors are required to comply with the EAR requirements (15 CFR Parts 730-774) regarding deemed exports and all other exports. NOAA grants and contracts entered into, modified, or renewed shall contain the standard clause/term and condition issued by the Acquisition and Grants Office to address these requirements.

SECTION 7. RESPONSIBILITIES.

.01 Department of Commerce Office of Security (DOC/OSY). DOC/OSY is responsible for approving or disapproving requests for foreign national visits to NOAA facilities.

.02 Office of the Chief Administrative Officer (OCAO). The OCAO is responsible for the overall accountability for establishing and administering the NOAA deemed exports compliance program, including policies and procedures required to execute the program. The OCAO is responsible for maintaining NOAA's central inventory of technology on the CCL. The OCAO is also responsible for ensuring appropriate training programs are developed and executed, and for maintaining accurate central inventories of controlled technology and foreign national guests working in NOAA facilities. The OCAO is also responsible for conducting annual assessments of compliance with EAR controls and requirements under this Order.

.03 NOAA Office of General Counsel (NOAA OGC). NOAA OGC is responsible for providing legal advice and guidance to the OCAO, as well as NOAA management and staff, on legal issues related to the Export Administration Act and regulations, particularly as they apply to NOAA's facilities and activities, including NOAA's preparation of export license applications. Among NOAA OGC's responsibilities are the following:

a. keeping NOAA management and staff apprised of current federal laws and regulations regarding export control technology;

b. responding to requests for legal advice on the Export Administration Regulations (15 CFR Parts 730-774) and accompanying regulations as well as advising on development of NOAA policy;

c. consulting with NOAA management regarding whether an export license is required to authorize access to controlled technologies by foreign nationals; and

d. providing advice on preparation of formal license applications.

.04 Line Offices (LO)/Corporate Offices (CO)/Staff Offices (SO). Each NOAA LO Assistant Administrator (AA), CO Director, and SO Director is responsible for ensuring that DOC and NOAA policies and procedures are adhered to prior to granting access by foreign nationals to NOAA employees, buildings, facilities, property, and/or assets; and for ensuring compliance with deemed export control requirements.

a. Each AA, CO Director, and SO Director shall designate a representative, and an alternate, to serve as the Controlled Technology Coordinator (CTC) for his/her LO/CO/SO. The CTC shall serve as the point of contact for the LO/CO/SO regarding foreign national access and export

control matters. The CTC will assist the DSNs with the process of sponsoring a foreign national and will communicate NOAA corporate policies on foreign national access, and export compliance and licensing matters. The CTC will be a member of the Deemed Export Steering Committee.

b. The CTC may delegate responsibilities to multiple DSNs within the LO/CO/SO to ensure compliance with this Order.

c. Upon receipt of DOC/OSY approval to grant access, each DSN is responsible for ensuring that visits by foreign nationals are conducted in accordance with DOC and NOAA policies and procedures pertaining to foreign national visitors and guests, and in accordance with U.S. export control laws and regulations.

SECTION 8. DATABASE MAINTENANCE.

.01 DOC/OSY Headquarters and the servicing security office will maintain a database containing identifying data for all foreign national visitors and guests to whom this Order applies.

.02 NOAA OCAO is responsible for maintaining a central inventory of all EAR controlled technology (other than EAR 99 items) within NOAA and for maintaining an annual list of foreign national guests working in NOAA facilities.

.03 NOAA LO/CO/SOs shall:

a. provide OCAO with copies of pertinent data related to the maintenance of the controlled technology inventory and the list of foreign national guests working in NOAA facilities; and

b. provide DOC/OSY with required biographic and visit data for entry into the foreign national database.

SECTION 9. EFFECT ON OTHER ISSUANCES.

None.

Signed
Under Secretary of Commerce
for Oceans and Atmosphere

Appendices

Office of Primary Interest:
Office of the Chief Administrative Officer

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 (SBU) 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 _____. I further understand, acknowledge, and certify that I
(insert facility name and location)
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)