

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)	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - 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