Department of Commerce · National Oceanic & Atmospheric Administration · National Weather Service

NATIONAL WEATHER SERVICE INSTRUCTION 60-704
APRIL 5, 2021

Information Technology
Information Technology Security Policy 60-7

FOREIGN NATIONAL ACCESS AND TECHNOLOGY TRANSFER

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W/ACIO (J. Stuart, P. Cypress-Reis)   **Certified by:** ACIO (B. Koonge)
Type of Issuance: Routine

SUMMARY OF REVISIONS: This directive supersedes the NWSI Technology Controls and Foreign National Access 60-704, dated AUGUST 08, 2016. Changes include: a) guidance on the new National Oceanic and Atmospheric Administration (NOAA) automated system, the Foreign National Registration System (FNRS), b) updated alignment with Department of Commerce (DOC) and National Oceanic and Atmospheric Administration (NOAA) policies; and c) minor editorial changes to ensure clear and concise language.

KOONGE.BECKIE.A.1408306880
Digitally signed by KOONGE.BECKIE.A.1408306880
Date: 2021.03.22 07:35:32 -04'00'

Beckie Koonge   Date
ACIO/NWS Authorizing Official
Designated Representative (AODR)

FOREIGN NATIONAL ACCESS AND TECHNOLOGY TRANSFER

Table of Contents Page

1. Introduction

1.1 For the purposes of this program, a Foreign National (FN) 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). Foreign nationals entering NOAA facilities are considered to be either a Foreign National Visitor (FNV) or a Foreign National Guest (FNG).

1.2 The Foreign National Registration System (FNRS) is the main tool used to request National Weather Service (NWS) facility access. The Controlled Technology Coordinator (CTC) should implement paper documentation processing for FNs when FNRS is down for long periods. If a user cannot log onto FNRS, they should contact the NWS CTC.

1.3 Department of Commerce (DOC) Administrative Order (DAO) 207-12 defines the length of stays that determine whether FN is FNV or FNG. FNRS automatically designates the

FN as either a FNG or FNV based on the length of their stay. A FNG can stay up to one calendar year maximum; any FNG staying over a one-year period will require a renewal. If a FNG will be staying longer than one year (1), the sponsor must notify the NWS CTC and begin the renewal process in FNRS a minimum of 60 days prior to departure date ending.

1.4 FNs staying past the initial one-year maximum, we refer as “renewals” FN renewals will require a memorandum from the office/region director addressed to the Chief Operating Officer (COO), the Director of the Office of Planning and Programming for Service Delivery (OPPSD), and the CTC. The memorandum should clearly state the reason why no U.S. citizen is available; explain the mission essential need for the FN’s skills and knowledge, reassure no technology transfer will happen, and provide information on the FN’s U.S. citizenship status, if any, such as waiting for Green Card.

2. Purpose

2.1 To provide the NWS employees with guidelines to professionally manage FNs who visit, work, or train in NOAA Government facilities, or who participate in in NOAA programs or activities. Guidelines include: to prevent the unauthorized release of classified, Controlled Unclassified Information (CUI), export controlled technology, proprietary, intellectual property and non-public information and data; to recognize espionage indicators and show where to report suspicious behavior and violations; and to prevent or mitigate technology transfer violations as stated in the following: the Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), embargoes enforced by the Department of Treasury Office of Foreign Assets Control (OFAC), and other applicable laws and regulations. These guidelines relate to the transfer of controlled items to FNs both outside the United States (exports) and in the U.S. (deemed exports).

2.2 To provide awareness on risks to our Information Technology (IT) networks/infrastructures when allowing FNs into our networks and computers. To educate NWS staff on technology transfer export requirements when shipping to foreign countries. To assist NWS staff with export/deemed exports classifications/licenses and highlight the importance of checking “Entities Lists” and Office of Foreign Asset Controls (OFAC) to capture the controlled technology before transfer in the United States to a FN or when transferring outside the United States.

3. Authorities

3.1 The DOC, through the Office of Security (OSY), regulates access by FNs to DOC facilities and activities (DAO 207-12, Foreign National Visitor and Guest Access Program. See also, NOAA Administrative Order (NAO) 207-12, Technology Controls and Foreign National Access.

3.2 OSY is responsible for identifying threats from foreign intelligence services, overseeing the investigation of security incidents, and protecting DOC personnel, facilities and activities (Department Organization Order (DOO) 20-6).

3.3 Presidential Decision Directives (PDD) and the Code of Federal Regulations (CFR) authorize OSY to identify threats from employee contacts with foreign nationals (PDD-12), to promulgate operations security actions (PDD-298), and to investigate the potential loss, compromise or unauthorized disclosure of classified material (32 C.F.R. § 2001.48).

3.4 The EAR establishes export control and deemed export control rules,, with criminal and civil penalties (15 C.F.R. Parts 300-799) for violations. The DOC Bureau of Industry and Security (BIS) manages and enforces the EAR with its Law Enforcement Office.

3.5 The ITAR (22 C.F.R. Parts 120-130) is administered by the Department of State controls/manages/enforced the export and import of defense articles and services ITAR implements the Arms Export Control Act (AECA) (22 U.S.C. Chapter 39) and Executive Order 13637. FNs will not be allowed visual or physical contact with ITAR items, including manuals, instructions, blueprints, software, etc. ITAR violations can result in severe penalties, fines, both criminal and civil, including jail time.

3.6 The OFAC enforces/manages economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, and those engaged in such activities. Violations for technology transfer to countries under OFAC carry similar violations to the EAR and ITAR, both civil and criminal including fines and/or jail time.

3.7 Controlled Unclassified Information (CUI) - Executive Order 13556, replaces the Sensitive But-Unclassified (SBU) regulations.

4. Roles and Responsibilities

4.1 The CTC and Alternate CTCs are NOAA Federal employees appointed by the Deputy Director of NWS to manage the NWS Technology Transfer Program, which includes exports and deemed exports as well as CUI, and espionage indictors for employees. The CTC and the Alternate CTCs manage the NWS FNRS, Technology Control Plans (TCPs), IT Security with FNs, export or deemed export license requirements/violations in EAR, ITAR, OFAC, and others. CTCs keep NWS senior management informed on new developments with FNs in the workplace and technology transfer issues. The CTCs train NWS personnel on exports, deemed exports, technology transfer, CUI, intellectual property, proprietary, remote access, network access, privileged network access regarding FNs. The CTCs can deny NWS staff as sponsors based on eligibility, prior violations, escorting, training, not working directly on day-to-day tasks with the FN, and other reasons that may cause harm to NWS. See Appendix A for details.

4.2 The Departmental Sponsor/NOAA (DSN) -– the NOAA Federal Government employees responsible for the day-to-day activities of a FNVs and FNGs, including escorting and ensuring other trained Federal employees assist with escorting/managing during absences. The DSN takes all reasonable steps to protect classified, CUI, export controlled, intellectual property, proprietary or not-for-public release data, information, or technology from unauthorized physical, visual, and virtual access by a FN. The DSN is also called "sponsor." See Appendix B for details.

4.3 The Point of Contact (POC) for the Technology Transfer and Foreign National Access Program are Federal employees, appointed by their Office or Region Director. POCs work with the CTCs and are leaders and advisors to sponsors on technology transfer, TCPs, FNRS, FN memos, FN policy, annual FN and CT Management Review/Certification and more. POCs work with the CTC to prevent violations, report violations, assist sponsors with their FNs, ensure exports are properly researched, identify controlled technology, etc. (See appendix C). Each Office and Region Director will appoint two Federal employees as POCs for their area by email to the NWS CTCs.

4.4 The Senior Bureau Official (SBO) reviews the FN information provided by the CTC, the Designated Official, and the DSN to ensure the value of collaborative efforts gained by FN access to DOC facilities, staff, and information remains balanced or tips toward the "value gained" side. NOAA balances the need to protect classified, Controlled Unclassified Information (CUI), export controlled, intellectual property, proprietary or not-for- public release data, information, or technology against the benefit gained from FN collaboration. The SBO signifies his/her endorsement of the NOAA assessment in the appropriate location on the Certification of Conditions and responsibilities for the Departmental Sponsors of FNG or in the appropriate location in the FNRS, and ensures this completed Certification is submitted to the proper Servicing Security Office (SSO).

4.5 The Designated Official (DO) is the FNRS term for senior manager responsible for concurring with the request and recommending approval or denial of access for a FN to NOAA facilities. In NWS, we have three DOs: the Deputy Director of NWS (DAA), the Chief Operating Officer (COO) and director of the Office of Planning and Programming for Service Delivery (OPPSD). The CTC will determine which, if not all, DOs review/approve based on country of citizenship and/or country of permanent residence. Remote access requests for foreign nationals also plays a major role in DO selection for reviews/approvals, as does renewals.

4.6 The Escort is a DOC Federal employee responsible for monitoring the day-to-day activities associated with the successful accomplishment of a FN visit and for taking all reasonable steps to protect classified, CUI, 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.

4.7 The Servicing Security Office (SSO) is a field offices of the DOC/OSY that provides security services, support, and guidance to DOC organizations. SSOs may provide services and support to a single bureau or may provide services and support to all DOC organizations in a given geographical area.

5. Equipment, Network Access and Telework Restrictions

5.1 FNs must use Government Furnished Equipment (GFE) when conducting work on behalf of the NWS. These devices need to be hardened and only include what is necessary to conduct the FN's work. Any exception on use and issuance of these devices (i.e., computer, tablets, phones, etc.) needs to be communicated with CTCs prior to being deployed.

5.2 Do not allow FNs to use their personal computers, cameras, thumb drives, external storage drives, cell phones, etc., in the Government facility. Especially important, no thumb drive or other device connections to NOAA computers or LAN servers. Note: in NWS, we normally do not take these items away from the FNs, we instruct them not to use these devises or bring them into the Government facilities.

5.3 Inform FNs not to bring devices into the office that takes pictures or captures documents. Note: in NWS, we do not take away these items from the FNs, we instruct them not to bring these devises into the Government facilities.

5.4 Do not allow FNs access to U.S. Government shared network drives that contain proprietary, intellectual property, CUI, classified, or other sensitive information, etc.

5.5 Do not allow FNs to attend NOAA briefings, meetings, conferences, etc., dealing with potentially sensitive information unless their participation is cleared by the CTC and senior management.

5.6 Do not allow FNs to remove Government Furnished Equipment (GFE) from their authorized physical work location.

5.7 Any change to a designated physical work location previously approved in FNRS must be communicated to a CTC prior to the change being implemented.

5.8 FNs are normally not allowed to work outside of the United States or its Territories on Government activities or projects/programs. Any exception must be communicated to the CTC and approved by the DAA prior to implementation.

5.9 Visit duration of over 30 calendar days allows FNs to have a "NOAA.gov" email and limited network access when required for their NOAA assignment.

5.10 Network access for FNs needs to be limited to only what is necessary to perform their assigned tasks.

5.11 Network access and email accounts are not permitted for stays fewer than 30 calendar days. In addition, NWS will not authorize network access or "NOAA.gov" email accounts if they are not required for the FN's work or training.

5.12 Any change to network access requires approval from the CTCs prior to being deployed.

5.13 No privileged network access allowed for FNs.

5.14 No remote access or VPN accounts allowed for FNs without DAA approval.

5.15 No telework allowed for FNs unless approved by the NWS DAA.

5.16 Remote access, if approved, from a Government approved facility only. Any exceptions require CTCs and DAA approval prior to allowance.

6. Training and Awareness

6.1 Sponsors require training on technology transfer to include understanding OFAC regulations, ITAR, EAR, end use, dual-use, re-exports, license exceptions, reasons for controls, CUI, etc. Office of Security offers anti-terrorist training, Counter Intelligence training, physical security training, and espionage indicator training. The CTC offers IT security awareness training, export and deemed export training, CUI training; proprietary and data/information NWS does not release to the public training, FNRS training, remote access training, logical access training, and more.

6.2 An online training course on “Foreign National Guest and Visitor Access” is under NOAA in the Commerce Learning Center. Sponsors must complete this course annually.

6.3 Sponsors or POCs can also request formal training from CTCs. Training options are classroom or network media. There is usually no cost for training.

6.4 New sponsors need to reach out to the CTCs for training and advice. NWS highly recommends that new sponsors discuss with the CTCs the types of controls relating to OFAC, ITAR, EAR, CUI and other regulations. Discussions will focus on FNRS, TCP, OSY forms, Appendix C, and more.

7. Technology Control Plans and Technology Inventory

7.1 Both Technology Control Plan (TCP) and Technology Inventory are critical in preventing inappropriate/unauthorized release or transfer of technology to foreign nationals in the workplace. It is important to work with your CTC to ensure the TCP and inventory include current/accurate information.

7.2 TCPs need to have the minimum sections: Purpose, Facility/office name and location; rules for specific citizenships identified in EAR and OFAC Sanctions list (i.e. Iran, North Korea, Cuba, Sudan, Syria, Russia, Ivory Coast, Belarus, etc.) The TCP must include extra precautions on technology transfer to these countries' citizens since non-controlled items may require deemed export license before release.

7.3 TCPs are training and guidance tools for the sponsor; they do not contain all the controls. Sponsor should check with the CTC before transferring any items to the FN or to allow FNs to use/view non-public information/data. Important note: if the information/data provided to the FN will or can be used for other than weather operations/training, then a deemed export license may be required before release of the technology. For example, if use will be for military or police and other uses prohibited by EAR and ITAR.

7.4 TCPs need review and updating when new technology arrives in the region/office or at least quarterly. POCs should alert the CTCs when new technology arrives and discuss controls. It is important to include all the technology (hardware and software) in the area including the network in the TCP. The TCP serves as one of the best tools to prevent release of technology to FNs if followed by staff working with the FN.

7.5 NWS senior management reviews the TCP each year as part of the annual certification. The CTC will request you to update your TCP before management review and the CTC will work with you to ensure the TCP contains complete information on reporting violations and identifying controlled technology.

8. Preventing Technology Transfer

8.1 No disclosure or transfer of classified information/items to a FN permitted in NWS. Classified information or items must be out-of-sight and locked when a FN is in the area. This includes any classified networks/computers; these devices should not be used with FNs present or in visible area.

8.2 Preventing technology transfer to FNs requires escorting, knowledge, restrictions, and vigilance. The TCP and escorting are two important ways to mitigate technology transfer as well as closure of accounts soon after FNs departure.

8.3 Prevention of technology transfer of prohibited items to FNs, although complex, requires understanding of EAR, ITAR, OFAC regulations as related to countries. Ensure you discuss with your CTC and understand any prohibitions, CUI, proprietary, and deemed exports/export regulations regarding your FN.

8.4 With FNs in the workplace, deemed export rule focuses on technology and software regarding technology transfer. The commodity, testing equipment and material normally do not require deemed export license. Most of the time, we need to focus on the technology and software, CUI and information/data not released to the public to avoid technology transfer violations. There is also a "Use Rule" that plays an important role in deemed export license determination; this "Use Rule" does not apply to all circumstances. When the "Use Rule" applies, a deemed export license is most likely not required for the FN to use the controlled item in the United States. See definition of "use technology" to understand the "Use Rule".

8.5 Sponsor should avoid technology transfer of the following items: 1. Blueprints; 2. schematics of networks/infrastructures and other systems; 3. Unpublished research items or information; 4. Proprietary information and items; 5. Intellectual Property, and 6. Non-published manuals/information on production or development.

8.6 Use of SNAP-R, the automated Bureau of Industry and Security's (BIS) export control classification system. SNAP-R will indicate if the item does or does not need deemed export license with FNs. Contact CTC or BIS directly for access to SNAP-R.

8.7 Again, escorting and keeping FNs in designated areas remain one of best ways to prevent unauthorized technology transfer. Sponsor must ensure their FN has multiple Federal staff trained in sponsorship of FNs, who can step-in and escort when sponsor is unavailable. The FN cannot work alone in the office; doing so results in violation of DAO 207-12 and greatly increases risk for NWS infrastructures and information/technology transfer.

8.8 Knowing and listing the technology in the work place, including CUI, prevents technology transfer. The sponsor needs to ensure staff awareness and understanding concerning the FN's specific work assignment and any restrictions on technology use or transfer. The office's TCP, if accurate and updated, will provide the necessary technology and information under controls.

8.9 Limited Unescorted Access (LUA): Not allowed in any NWS office. This is for public access area only in NWS.

8.10 Conducting Controlled Technology (CT) Inventories: This is very important to ensure you identify all the controlled technology in the facility/office. CT inventories start with listing all equipment and materials in the facility/office. For example; you have a Global Positioning System receiver in your office, you would list this on your CT inventory. Then you need to look in the EAR's Commerce Control List (CCL) to find out if the GPS receiver is export controlled. If the GPS receiver is export controlled, you need to obtain the export Control Classification Number (ECCN) and then look at any material, software (within the GPS receiver) and technology (usually manuals, blueprints, schematics, etc. to build or produce the GPS receiver). The GPS receiver's software and technology will have their own ECCNs and export as well as deemed export controls. Recommend you work with your CTC to conduct the Controlled Technology inventory.

9. Violations and Reporting

9.1 In the event of controlled technology violation: you must self-report the violation to your CTC and /or Bureau of Industry and Security Office of Export Enforcement as soon as possible. For ITAR violation, report to Department of State and CTC as soon as possible. Same procedure for OFAC violation.

9.2 For violations involving entering the NWS facility without proper authorization from OSY, CTC will work with the FN sponsor and POCs to complete a Violation Report.

9.3 The Violation Report will include the following information:

- *Header*: Violation Report – NWS Facility Access Without Approval with FNs name and Country of Citizenship
- Full name of FN, country of citizenship, summary of violation (what happened, why, for how long, any release of controlled technology, how could this have been prevented, and how to prevent from happening again.
- Sponsors name and telephone number
- Supervisor of sponsor and telephone number
- *Investigation summary*: names of persons interviewed by email or telephone with dates and report of statements
- *CTC must interview sponsor, the staff involved* and provide OSY and NOAA a brief summary and estimated completion date. Provide name and telephone numbers of those interviewed with dates of interview.
- What steps will you take to prevent future violations?
- Who will be responsible for implementing the preventative measures?
- The report must address release of controlled technology and if occurred, the CTC and sponsor will report to proper authorities as soon as possible.
- CTC should summarize the duties of the FNs, purpose of the visit, length of stay, state if or if not NOAA networks accessed, if so, which network system.
- CTC will seek review and approval of this report with signature from the Designated Official (DO) or Officials currently active in FNRS. After DO signature, email the report to OSY and NOAA, with copies to alternate CTC, ACIO, and DOs.

9.4 Export Violation determination based on several factors: the item, the country, the use, re-export (FN sends to another country), Entity List, OFAC, ITAR, etc. Violations must be reported to the CTC, the Bureau of Industry and Security (BIS) and to the OSY.

9.5 Types of export violations penalties, fines, etc., from the Bureau of Industry and Security (BIS), ITAR and OFAC are: a)Warning Letter, b) Charging Letter, c) Administrative Sanctions, d) Civil monetary penalty. (Civil fines up to $500,000 per violation or twice the amount of the transaction that is the basis of the violation), e) Denial of export privileges, f) Exclusion from practice, g) Criminal Prosecution: In addition to pursuing an administrative enforcement action, criminal fine up to $10,000,000 ; Jail time up to 30 years.

10. Shipping Outside United States or its Territories

10.1 NOAA's National Logistics Support Center (NLSC), the National Reconditioning Center (NRC), the Logistics Management Branch as well as any NWS office or staff must coordinate with the CTC before shipping any item (commodity, material, software, technology, etc.) outside the United States or its territories. Any NWS office can ship outside the United States; before doing so, it is highly recommended to check first with the CTC to ensure no export license required.

10.2 The CTC needs at least 30 calendar days in advance to research the item to ensure no export license requirements. Highly recommended that you coordinate thoroughly with your CTC on shipments outside the United States. You can always chose to self-classify your export or deemed export, which is not recommended unless you previously classified your export. We recommend you at least classify your deemed export/export with the Bureau of Industry and Security (BIS) before releasing or transferring to the FN.

10.3 Check the Office of Foreign Assets Control's website to ensure no restrictions on certain exports. Note: this is separate from the Export Administration Regulations and SNAP-R.

10.4 Check the Entities list. You should do this for the organization and individual receiving the item. Note: SNAP-R checks for the country and item only, not the organization or individual who may or may not be on the Entities List. If on the Entities List, do not ship the item. Discuss with the CTC.

10.5 Know what the end user will do with the item or items shipped and make clear no re-export allowed without your permission. For example, if the end use is for something other than meteorology, you may require an export license to ship.

10.6 The office/staff trained in export can do their own research and if so, should use the automated system currently known as SNAP-R in the Bureau of Industry and Security website to determine if controlled technology before the transfers occurs. Again, it is highly recommended to coordinate or discuss with the CTC before any shipment/transfer of any data, information, software, equipment, manuals, chemicals, material, items, etc.

10.7 Office and staff should not rely on brokers, freight forwarders, etc., to do their export checks. In most cases, the shipper (NWS and staff member) is solely responsible for any violation pertaining to their shipment. The broker, freight forward, etc., that is used to determine the items classification will not be held fully accountable for violations.

10.8 Ensure the item shipped outside the United States – referred to as export – has written instructions on the shipping documents to state, "end use will be for weather forecasting only and this item will not be shipped to another country without the written consent of the NWS" or something similar to this statement.

Appendix A: CTC Responsibilities

The CTC responsibilities may also include:

A1. Responsible for managing and executing the Line Office's foreign national program and export program including protecting networks. The Office of Security responsibility centers on physical and espionage security while the CTC assists OSY with physical and espionage by ensuring sponsors' knowledge and training are on these concerns. The CTC assists OSY with some of these responsibilities with FNs, and handles the deemed exports, exports, logical access, CUI, information/data not released to the public. OSY responsibilities cover safeguarding information and data throughout NOAA which includes: classified, proprietary, intellectual property, exports, deemed exports, logical access, CUI, and technology transfer. The CTCs assist OSY with safeguarding information and data with FNs.

A2. The CTC needs to work directly with NWS senior managers throughout the National Weather Service. The CTC reports to the Assistant Chief Information Officer (ACIO), as several controlled and sensitive information exist in the NOAA IT networks, and protecting NWS' infrastructures from FN interventions remains large part of CTC responsibilities.

A3. The CTC reviews and updates (annually or if there is a significant change) policy concerning FNs access, controlled technology, sponsors, in coordination with senior NWS managers and the Governance Board for the Foreign National Registration System (FNRS).

A4. The CTC ensures policy aligns with Department of Commerce policy, NOAA policy, Department of State policy, Department of Treasury policy and Executive Orders pertaining to FNs in Government facilities. This includes but not limited by: a) Policies in Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), Office of Foreign Assets Control (OFAC), Office of Security (OSY), Executive Orders, Presidential Directives, and others such as Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) and cybersecurity, b) Policies/Instructions by the FNRS Governance Board, c) Instructions by NWS Senior management, and d) Instructions/procedures by CTC based on specific events or circumstances.

A5. The CTC and alternates resolve issues with FNs working in NWS. CTC will act as a mediator/arbitrator/adviser in disagreements between sponsor, staff, management and/or senior management concerning FN responsibilities, network use, restrictions and duties, etc., in NWS. The OSY will have final authority on issues with FNs concerning physical access to facilities and/or suspicion of espionage.

A6. For any Real Property leases, revocable license (Outgrants) for non-Federal use of Real Property, etc., the CTC must review prior to approval. CTC will ensure controlled technology and FNs procedures exist in the facility and the CTC will provide clause/words for inclusion in the lease/Outgrant. The CTC ensures up-to-date Technology Control Plan for the leased facility and the leasee understands NOAA foreign national access requirements as well as controls established to prevent the unauthorized released of controlled technology.

A7. The CTC will provide advice/guidance to General Counsel in matters pertaining to FNs in the workplace, export and deemed export law, Bureau of Industry and Security Enforcement visits and other concerns with exports. This includes providing references to current law, policies, executive actions pertaining to exports and foreign nationals.

A8. The CTC will work with the Region Directors, National Centers for Environmental Prediction (NCEP) Director, Office Directors, Senior Management, through the POCs, to complete the annual certification report to Department of Commerce and NOAA. This report acknowledges by manager's signature and statement (certificate) that NWS maintained due diligence to mitigate and prevent improper technology transfer to FNs both in NWS and outside of the United States.

A9. The CTC conducts training for sponsors of FNs and training on exports and other restrictions regarding technology transfer to FNs for the NWS. This includes training on FNRS. The CTC will work with the NWS' Training Center to develop and maintain Commerce Learning Center sponsorship and export online training for NWS staff. The CTC will also add FN awareness to the IT Security Awareness training module, if possible.

A10. The CTC and alternate require training to ensure that he/she remains informed on the latest laws and regulations pertaining to exports and foreign national access program. The CTC updates the TCP template to reflect major changes in export law impacting NWS.

A11. The CTC and alternates handle FN violation reports and investigations in NWS. Usually these reports, once completed go to NOAA Chief Administrative Officer and then to Office of Security. In NWS, the reports will go to the Deputy Director of NWS (DAA), through the Chief Operating Officer (COO) and director of the Office of Planning and Programming for Service Delivery (OPPSD). These reports will include interview with sponsor, staff involved, and IT security staff with the purpose to find any technology transfer or espionage indicators. If technology transfer without deemed export license occurred, must self-report the violation to Bureau of Industry and Security.

A12. The CTC and alternate represent NOAA LOs concerning exports, deemed exports, FNRS, sponsors, Real Property Outgrants, contracts with FNs and/or involving exports, foreign national access, IT network access, remote access, and other information involving FNs. As a result, the CTC and alternates may meet with senior NOAA leadership, Department of Commerce leadership, and other Government agencies to discuss FNs and exports/technology transfer.

A13. The CTC and alternate prepare the following reports annually with assistance from the

POCs:

a. NWS Foreign National List Report: this report lists FNs at NWS by fiscal year and after final quarterly review, becomes part of annual certification. This report contains the FNGs in NWS with status. The status reported with color codes for departed, canceled, Green Card holder, Needs More Information, and FN at NWS site in foreign country (Pacific Region only). This report contains the following categories:

- First and Last Name,
- Line Office,
- Foreign National's Country of Citizenship,
- Country of Permanent Residency,
- Duty Station,
- Position Code (See Note on List),
- Program under which F/N is working at NOAA (include Contractor Name, Program, Joint Institute, etc.),
- Starting Date (mm/dd/yy),
- Scheduled Departure Date (mm /dd/yy),
- Federal Employee Sponsor Name (e.g., Doe, John),
- Sponsor Phone Number,
- Specify NOAA Facilities/Platforms (including Ship(s)/Plane(s)) to Be Accessed by Foreign National,
- Country of Birth
- Denied List Entities List (Yes/No),
- Description of Work,
- Controlled Equipment Technology, if any

b. NWS facilities with Technology Control Plans Report – separate into Critical and Non-Critical Infrastructures for NWS contains:

- Facility short Name
- Facility Name
- Location
- POC Name and telephone number

c. List of NWS' Facilities and Controlled Technology Inventories Report consist of:

- Facility short name
- Facility name
- Location
- POC Name and telephone number
- Controlled Technology, including CUI, proprietary, for NWS use only, PII, contracts, etc., at office/facility or "none" in column

d. Technology Control Plan contains at least the following:

- Purpose
- Explanation of exports, deemed exports, CUI, classified, proprietary, PII, etc., that need protection from FNs

- List of Controlled Technology at the office/facility
- Special cautions with certain countries' foreign national from EAR and OFAC: with explanation of what has to be accomplished before they arrive and during their time in the office
- Local point of contact name and telephone
- Responsible individual to report violations and brief staff on this plan
- Name of Controlled Technology Coordinator (CTC) and email
- Actions to mitigate the transfer of technology to FNs
- Each office/facility must have a separate TCP. For example: in Western Region, each Weather Forecast Office, Weather Service Office, Center Weather Support Unit, Weather Port Office, etc., will have their own TCP.

e. Create Correspondence Cover Sheet for high risk FNs to summarize and recommend specific action to senior management. Brief senior management, if necessary. Ensures FNRS and supporting documents are accurate and complete for senior management review in FNRS.

Appendix B: Departmental Sponsor/NOAA (DSN) Responsibilities

The DSN responsibilities include:

B1. Highly recommended, but not mandatory, that sponsor be GS-14 or higher (or equivalent in pay banding) and most important for the sponsor to work with the FN daily. NWS will not allow administrative staff or staff not working directly with the FNs to become the sponsor. Administrative staff can assist the sponsor and help complete the FNRS request.

B2. Use the Foreign National Registration System (FNRS) for requesting foreign national access to NWS facilities and other activities/programs with FNs. Foreign National Registration System (FNRS) requires training and registration with your NWS CTC, currently Jeffrey.Stuart@noaa.gov and alternate CTC, Paula.Reis-Cypress@noaa.gov. Do check as the NWS CTC names may change.

B3. Log-on to FNRS at: https://fnrs.rdc.noaa.gov/fnrs/. You should use Google Chrome browser and requires CAC ID. If have multiple CAC certifications – select the one with "email" in the description. If accessing remotely, you must use VPN to enter FNRS. Note that: a. You may have to reboot your computer if you tried the above and still cannot log into FNRS; and b. Email or call your CTC to discuss your issue with FNRS login and if cannot resolve, we will call or email FNRS help/support.

B4. Request Letter of Invitation (LOI) from International Affairs Office. LOIs are formal/semi-formal letters/emails normally written by the International Affairs Office (IAO) and receives approval by senior management. Sponsors should ensure the LOI originates from IAO or receives approval from IAO. Denial for your FNRS request without proper LOIs increases greatly. Short visits by FN visitors (as defined in NAO 207-12) do not require LOIs.

B5. Ensure written justification in FNRS clearly describes work/training of the FN with emphasis on benefits to NWS. Examples of benefits to NWS include more accuracy of Numerical Weather Prediction models; improvements in: weather products, observations, lead times, public watches and warnings, forecaster training, technology, etc. Write about what you expect the FN to accomplish and the technology involved. Write the details of their assignment with emphasis on the benefits to NWS' mission.

B6. Ensure FNRS documents are accurate, especially spelling of name, Date of Birth, most recent Country of Citizenship, Country of Permanent Residence, Passport Number, and the Funding Code. For these FNs' categories, the reviewers rely solely on the sponsor to get it right, and if incorrect will delay access. Sponsor must have their budget officer/financial officer verify that the funding code is correct.

B7. Routine FNs: Submit in FNRS at least 45 calendar days in advance of FN's start date for Routine Foreign Nationals (friendly country, at NWS for less than one year, training with NWS, etc.); your FNRS record will be reviewed by CTC and then Chief Operating Officer

(COO) or Director of the Office of Planning and Programming for Service Delivery (OPPSD). Note: FNRS gives warning if under 30 days in advance, these entries may not receive all their approvals and background checks in time for their start date and Sponsors must ensure they have permission to enter the facility by Office of Security before doing so.

B8. Know the High-Risk Foreign Nationals: Submit at least 60 calendar days in advance of start date for High-Risk Foreign Nationals (China, Russia, Sudan, Syria, Iran, North Korea and Cuba and other countries identified by the Office of Foreign Asset Control (OFAC) such as Belarus, Ivory Coast, Zimbabwe, Burma, etc.) and more (check with OFAC and CTC). Note that: a. Memorandum Requirement: You will need to submit memorandum to the Deputy Director of NWS for high-risk FNs; b. Your memorandum should go through the Chief Operating Officer (COO), Director of Office of Planning and Programming for Service Delivery (OPPSD), and the NWS CTC. Send the final draft memo to your NWS CTC for review.

B9. Submitting Renewals: Submit at least 60 calendar days in advance for FN staying over one calendar year (renewal) in NWS, FNRS will require at least 60 calendar days in advance for renewing for additional days. These FNs require memorandum along with FNRS entry. Memorandum Requirement: Submit memorandum to the Deputy Director of NWS for renewals. Memorandum must route through the COO, Director of OPPSD, and the NWS CTC. Send the signed memo by your office/region director to your NWS CTC for routing to COO and OPPSD.

B10. Requesting Remote Access: Understand that remote access provides network access beyond some security measures and therefore we need to take extra precautions with limited resources. Remote access for FNs is normally to access the Research and Development High Performance Computing System (RDHPCS) from the Government facility. We do not allow FNs to remote access from home or other locations. Remote access requests for FNs have more controls and management reviews before allowing. Remote access requests for FNs require 60 calendar days in advance of start date entry to CTC, including the memorandum. FNs remote access require memorandum, usually the CTC will have a separate FNRS entry that says “For Remote Access Only”. Check with CTC before submitting as FNRS entry for remote access could change. Memorandum Requirement: Deputy Director of NWS receives Memorandum, through the COO, Director of OPPSD, the System Owner and the CTC must approve Remote Access..

B11. Office of Security (OSY) may have other documents and forms to complete such as the fingerprint card, sponsors must ensure they deliver completed OSY documents for their FNs, as required. Sponsors need to check with OSY to determine the specific forms/documents requirements for their FNs.

B12. Take the Sponsorship of Foreign National Guest training located in the Commerce Learning Center webpage under NOAA. This course is mandatory for sponsors to complete annually. Denial of FN request may happen if course not completed by the sponsor each year. Sponsor can request training by CTC, either formal training that involves person-to-person in classroom or informal training using the telephone and/or video-conferencing.

Approval of the training will be determined by CTC and with available funding.

B13. Take escorting seriously; maintain visual contact with FN in the workplace except for kitchen area and restrooms in the vicinity. Assign other Federal employees to assist you with escorting your FN if you are off work or at meetings. Schedule the FN to be out of the office when no Federal escorts are available. Keep the office informed on the importance of escorting to prevent technology transfer and protect infrastructures.

B14. Technology Transfer: Read and review your office Technology Control Plan (TCP). Warning: violations can occur even with non-controlled technology transfer to a foreign national. Highly recommended: talk to your CTC before you or office staff transfer any technology or items to a foreign national in the United States or abroad. The Entities List in the EAR, OFAC and Category E Country Groups (in EAR as terrorist supporting countries) require licenses before release of non-controlled technology or software while in the United States. End use of items given to foreign nationals also make a large difference in controlled versus non-controlled and with the need for an export/deemed export license.

B15. Sponsors must ensure FNs network accounts, especially VPN (allowed only with Deputy Director of NWS approval) and emails, are deactivated before or on the day of departure. Coordinate with the Information System Security Officers (ISSOs) to ensure FNs network access terminated no later than two days after departure.

B16. Attach the “Certification of Conditions and Responsibilities for a Foreign National Guest” form, signed by the FN to the FNRS’s record within three days after arrival. OSY provides final authorization for access after this completed form in FNRS.

B17. After final approval from OSY, sponsor needs to go back into FNRS and enter the FNs actual arrival date. This helps the CTC and OSY keep track of FNs in the workplace.

B18. Very important: Sponsor must enter arrival date into FNRS no later than (NLT) two workdays after actual arrival. This alerts the Office of Security, CTC and other approving officials that the FN arrived. Just as important: Sponsor must enter the FNs departure date in FNRS, NLT two workdays after FN departs. When sponsor enters departure date in FNRS, this alerts the IT staff to close the network account, if applicable, and alerts the Office of Security the FN is no longer with NWS. The IT staff will close the FNs network and email accounts and also wipe clean the FN’s GFE. Sponsors must follow-up with the Information System Security Officer (ISSO) or help desk until completion of the account closure and GFE “cleaning” for their FNs.

B19. Sponsors are responsible for ensuring OSY clearance received before allowing FNs into the Government facility or conducting activities with the FN. Meeting FNs outside the Government facility requires OSY clearance and entry into FNRS. Enter in FNRS long-term activities with FNs and NWS employees such as programs and projects that involve exchange of technology and information.

B20. Work with the NWS CTC on FNRS changes, modifications and/or adjustments. The CTC votes as a member of the NOAA FNRS Governance Board for changes to FNRS.

B21. Sponsor remains responsible for alerting CTC immediately on FN change of status and receiving approval before implementation of the change. For instance, if a FN transfers to another office or out of NWS, the sponsor needs to inform the CTC before the change takes place and seek approval. The CTC will determine if senior management needs to reapprove. This applies to any change in FN work/training status. Another example, the FN gets sick and the sponsor allows the FN to work from home without using remote access. Changes in work location in FNRS require approval by the CTC, Designated Official and Office of Security. The sponsor must ensure FNRS clearly states the work location and any other work location including the room number. For example, if sponsor wants FN to work at home, then before allowing, the sponsor must receive approval by FNRS, through the CTC.

Appendix C: Point of Contacts (POCs) Responsibilities

The POC responsibilities include:

C1. Highly recommended that POCs attend sponsorship of foreign national on-line training as well as attend formal training offered by the CTC. POC can request formal training from the CTC at any time.

C2. Assist the CTC with any violations in the region/office. This includes conducting interviews with the sponsor, staff and supervisor regarding the violation and checking the Technology Control Plan for any omissions of controlled technology.

C3. Identify all the standalone Government facilities in the region/office to the CTC, including unmanned facilities and leased facilities. Unmanned facilities may not require TCPs, check with the CTC. Staffed Government facilities – owned or leased by the Government (NWS) – require controlled technology inventories and TCP.

C4. Do not allow sponsors to provide VPN (allowed only with Deputy Director of NWS approval) access or high-level (above "user") network access to FNs. FNs remote access and higher-level network access above "user" requires DAA approval.

C5. Emphasize the importance of escorting the FNs in the workplace to the sponsors. Escorting is one of the best deterrents in mitigating technology transfer.

C6. Work with the CTCs to perform thorough controlled technology inventories to include export/deemed export controlled items, proprietary, CUI, and information/data not released to the public. Blueprints, how to develop items, new research not published are some of the items that could have controls.

C7. Brief at Region/Office/Branch staff meetings the importance of technology transfer, CUI, not-for-release to public data and information, the TCP, and understanding IT network concerns relating to FNs in the workplace. Talk to your CTC to receive briefing presentations or assistance..

C8. Assist CTC with annual certification. The annual certification involves the following:

a. Verify accuracy of foreign national guests on the NWS list
b. Confirm all staffed facilities entered into the NWS facilities list
c. Verify critical infrastructures properly annotated
d. Update and confirm Technology Control Plans (TCPs) have local contacts, responsible individuals who know how to report technology transfer violations and espionage indicators.
e. Reconcile controlled technology identified in the TCP and inventory spreadsheet. The CTC normally performs this task after receiving updated TCPs.
f. Ensure accurate reporting of FNs who entered NWS facilities or conduct activities with NOAA staff.

g. Discuss the export and foreign national program with your office or region director to obtain their signature on the annual certification

h. Work closely with the CTC to ensure timely and accurate information. Understand that the annual certification goes to the Chief Operating Officer, Director, Office of Planning and Programming for Service Delivery, and the NWS Deputy Director (DAA). After NWS DAA signs, then the annual certification goes to NOAA senior managers and to the Department of Commerce Office of the Secretary's Office. Possibility exists for audits by the Department of Commerce's Inspector General.

i. Ensure each facility and office has TCPs and stays current on quarterly or annual basis. Submit your updated TCP(s) to your CTC whenever changes occur or during the annual update time.

C9. Provide accurate and timely updates to the NWS FN list and Controlled Technology (CT) Technology Control Plans each quarter.

C10. Work with the NWS CTC on FNRS changes, modifications and/or adjustments. The CTC votes as a member of the NOAA FNRS Governance Board for changes to FNRS and will submit your change if it has merits.

Appendix D: NOAA Network Use and Monitoring

D1. Controlled technology exists in NOAA networks as; proprietary, intellectual property, export controlled, CUI, information/data not shared with the public and more. When allowing FNs network access, risk increases to expose the FN to controlled technology and software. FN use of NOAA networks must be restricted to their work assignment only and their work assignment must not include controlled items, technology or software without obtaining deemed export licenses.

a. Most past FN violations in NWS involved NOAA network access and lack of proper escorting.

D2. The network serves as the cornerstone to weather forecasting, communications on watches and warnings, interface with news media and emergency managers, and more. The networks serves as infrastructure for:

a. Decision Support Services (DSS)
b. National Digital Forecast Database (NDFD)
c. Advanced Weather Interactive Processing System (AWIPS)
d. Automated Surface Observations Systems (ASOS)
e. Numerical Weather Prediction (NWP) models
f. Emergency Managers Weather Information Network (EMWIN)
g. Meteorological Aviation Reports (METAR)
h. Incident Meteorologists (IMET)
i. Cooperative Observation Network (COOP)
j. National Data and Buoy Center (NDBC)
k. Upper Air Systems (UAS)
l. Radar Operations Center
m. Satellites
n. Weather radio
o. SKYWARN Weather Spotter Program
p. Aviation Weather Center
q. Climate Prediction Center
r. Environmental Modeling Center
s. Office of Weather Prediction
t. Ocean Prediction Center
u. Space Weather Prediction Center
v. Storm Prediction Center
w. Tropical Prediction Center (National Hurricane Center)
x. NCEP Operations Center
y. Light Detection and Ranging (LIDAR)
z. Other NWS systems and programs

D3. Protecting our network is critical for weather services to continue, with accuracy and without interruptions. Thus protecting our networks from foreign intervention and invasion needs our undivided attention when we allow FNGs to use the networks.

D4. System Owners (SOs), Authorizing Officials (AOs), and Information System Security Officers (ISSOs) need to know about FNGs in their area accessing the network, type of access (user only); the reason for access, remote access (if approved by DAA), and length of access. Monitor the FNGs computer for any activities outside of the work assignment, if possible. Report to Office of Security, CTC, supervisor and Incident Commander on any issues

1. ISSO or System Administrator with sponsor assistance need to close FNs network accounts within three days of end/departure date. This is important to prevent network entry after terminating with NWS.

D5. Foreign national guests (FNGs) staying for at least 30 calendar days may have "user only" network privileged access and a noaa.gov affiliate email address, if essential for their training or work assignment. The Information System Security Officer (ISSO) and CTCs will make network access and email account determination based on the sponsor's descriptions in Foreign National Registration System (FNRS).

a. No network access or email accounts for stays fewer than 30 calendar days. In addition, no network or NOAA.gov email accounts if not required for his or her work/training.

b. No network access or email accounts allowed for FNs working/training conducting activities, programs, etc., outside the United States or its Territories. FNs outside the United States and its Territories will not have VPN or logical access to Government information not available to the general public.

D6. FNGs will not receive remote access using VPN or other means without the written approval of the NWS' Deputy Director (DAA).

a. Remote access request most likely require separate entry into FNRS. Talk to the CTC to obtain latest requirements for remote access.

b. Remote access, if granted, can only be from Government Furnished Equipment (GFE)

c. Remote access can only be from the Government facility during normal daytime work hours with Federal employee escort present.

d. Remote access duration in FNRS allows maximum of one calendar year. For stays over one calendar year, the sponsor must reapply in FNRS at least 60 calendar days from the current departure date.

e. Remote access requires memorandum to NWS' DAA, through COO, OPPSD Director, CTC and System Owner.

f. Memorandum required for each additional calendar year stay in NWS.

D7. Sponsor must ensure remote access for FNs, once approved, is for work only, used in Government facility, GFE, and if needed renewed another year. Submit renewals with memorandum no later than 60 calendar days in advance of new start date.

D8. Closeout of network accounts and email upon departure of FNs. Information System Security Officers (ISSOs) and system administrators with sponsor assistance are responsible for deleting FNs network accounts within three days or sooner after departures.

D9. The System Owner or ISSO should periodically monitor the FNs computer including saved files, use of storage drives, email and attachments, deviations from work assignment, internet searches, thumb drives or other device attached, etc. Report violations to the CTC, your supervisor and the OSY.

D10. Upon departure, the FNs Government Furnished Equipment (GFE) computer requires wiping by Information System Security Officer (ISSO). The sponsor must retrieve any other materials, shared, or provided to the FN.

D11. During assessments, the team will check if FNs are/were accessing the network and look for any malware, verify FN's GFE computer was wiped clean after departure, check for viruses or if any abnormalities in network. If possible, check FNs emails, storage drives, if attached other devices to GFE computer, etc. Report any issues to CTC.

D12. Information System Security Officer (ISSO), System Owner (SO), and/or Authorizing Official (AO) should restrict FNs computer as such, when possible:

a. Eliminate or reduce attachments to emails on their GFE computer
b. Disable thumb drive
c. Do not allow access to network drives, or large storage drives
d. Keep computer/network access at "user" or work/training assignment only
e. Do not allow remote access
f. Eliminate camera/pictures on their GFE computer
g. No fax capability on their GFE computer

D13. ISSO require export/controlled technology training, either by the CTC, Bureau of Industry and Security, or private organization specializing in deemed export, ITAR, FNs use of Government computers/networks, etc.

a. Annual training required. Commerce Learning Center has the Sponsorship of Foreign National Guest training course. This is required for ISSO to complete each year.
b. Special training: upon request to CTC, ISSO may receive technology transfer training.

Appendix E: Benefits and Potential Dangers of Hosting Foreign Nationals (FNs) in NWS

E1. *Benefits*: Collaboration between employees and foreign nationals are in the best interests of the Department and our nation. They contribute to activities such as, Trade Agreements, Bilateral Agreements, and Memorandum of Understandings between countries, Scientific Research, International Standardization, and Environmental Stewardship to name some.

E2. *Potential Dangers*: Foreign powers and some nongovernmental organizations (NGOs) collect intelligence to advance their best interests. Absence of trained and attentive sponsors/staff provides a higher possibility for other countries or NGOs to successfully use Foreign National Visitors or Guests to:

- Acquire information to outstrip U.S. capabilities
- Influence U.S. decision-makers
- Cause the U.S. to unnecessarily deplete limited resources
- Map out NOAA networks to identify vulnerabilities for their advantage
- Gather blueprints, schematics, manuals or specific information on export controlled items especially dual-use (commercial and military items)
- Intend to request certain items for weather, such as radar parts, etc., to take to their country and re-export these to another country such as Iran, Cuba, Syria, Sudan, Russia, Ivory Coast, etc.
    - This violates export law in the EAR, ITAR and OFAC

E3. Be aware of the above and we recommend escorting as the best deterrent for mitigating technology transfer in the office. For transfer of items to their country, you should involve the CTC. The CTC will provide you statements to include on the shipping documents or if hand carrying the items on the airplane, will provide you with technology transfer release document.

E4. When hosting FNs, sponsor must provide orientation class. FN staying over three days in NOAA need orientation briefing from sponsor. Sponsors need to create office orientation discussion/training for the FN to cover important topics before they begin their assignment. Sponsors can ask for assistance from the CTC to create the orientation. The orientation should include, but not be limited to, topics listed below:

- Safety: cover at minimum the office hazards, driving (many FN countries have different laws), emergency numbers, reporting of accidents, etc.
- Fire reporting and what to do, where to report, where to evacuate, etc.
- Shelter-in-Place and Evacuation
- Have them complete the NOAA Employee Safety, Environmental and Sustainability Awareness Course
- Diversity and Equal Opportunity
- Security
- Ethics

- IT Security Awareness Course
- Health Insurance
- Customs and Courtesies

E5. Safety and evacuation procedures are very important to everyone in the workplace. The FN is no exception. NOAA requires the sponsor to provide adequate training or instructions prior to allowing the FN to work in NOAA facilities.

E6. Sponsor should discuss with International Affairs, the requirement for Government provided health insurance when hosting some FNs. For specific invitations, normally including Government stipend, require health insurance by law.

E7. Sponsor should verify the FN’s U.S. Visa expiration date does not end before the planned departure date at NOAA. If you are aware of the FN’s U.S. Visa renewal, you may enter a departure date (within the one-year timeframe) that goes beyond their visa expiration date. The sponsor will make the CTC aware of any Visa expiration date occurring before the NWS departure date. The sponsor must ensure the FNs expiration date changes to allow the FN to stay in NOAA.

E8. Hosting FNs takes good planning and preparations. Treat FNs with respect, courtesy and ensure their stay at NWS remains productive, positive and safe. The sponsor needs to know their FNs customs and courtesies, and country laws. The sponsor should utilize this knowledge to compare with United States customs and courtesies; and laws. For example, some traffic lights in other countries only turn “green” on one side at a time, thus you do not have to yield to oncoming traffic when turning. Others drive on the left-side of the road, instead of the right. Some hand gestures are looked at differently in other countries, etc. The word “Freeze” by police may not be known to our FN.

E9. Frequent communication with your CTC makes for good practices when transferring technology to FNs. After sponsors receive approval for their FN to enter NOAA facilities/offices and/or conduct activities in FNRS, the sponsors must continue to inform the CTC of any changes with the FN's status. For example and especially for changes involving: work location, work/training agenda, network access, and departure date; the sponsor must inform the CTC as soon as possible and preferably before the change happens.

E10. Sponsors cannot allow FNs to work/train with NWS when changes with FN status such as mentioned in E9 above happen. Sponsors must receive approval from the CTC to continue work/training for changes in: work/training location, sponsor, and network access to name some.

E11. When extreme circumstances, such as a catastrophic event occur, and the facility must close or evacuate; the sponsor must inform the CTC and receive approval prior to allowing the FN to continue work/training at a different location.

E12. NWS uses the Risk-Based Methodology to approve FNs. Senior managers and CTCs will use the following criteria to approve/deny access to NWS:

a) Does the Foreign National's organization or country operate in a manner consistent with U.S. research values and principles, including transparency, integrity, publication rights, open data sharing, and respect for intellectual property and legal rights?
b) Would the specific activity proposed benefit NOAA?
c) What is the sensitivity of the technology or information, or other material to which the Foreign National may have physical, visual, or virtual access?
d) Whether the value to be gained by NOAA by having the Foreign National present in NOAA spaces and having access to NOAA information is reasonably justified given the direct and indirect costs to NOAA to execute the security mechanisms necessitated by this presence?
e) Can an individual who presents less risk to NOAA information or national security accomplish the work by the Foreign National?
f) Is there legal authority for the specific activity proposed?

Appendix F: Other Definitions

F1. Letter of Invitation (LOI): This letter is a formal invitation to a foreign national to visit NOAA facility or the United States. NWS' International Affairs Office (IAO) manages LOIs. LOIs should be coordinated through IAO. IAO receives NWS senior management approval for LOIs for each FNG. Completed/approved LOIs required before entering FNGs into FNRS. LOIs are not required for FNVs.

F2. Controlled Technology: In the EAR, the items on the Commerce Controlled List (CCL, 15 CFR Part 774) are designated controlled technology. Controlled Technology includes dual-use (both military and commercial) items or any item with nuclear proliferation applications, etc. Furthermore, being controlled technology or not depends on: the latest country of citizenship of the foreign national; the country of permanent residence; the item (commodity, material, technology or software); end use of item; Entities List; and OFAC list. Controlled technology also includes items in the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120 – 130), Controlled Unclassified Information (CUI), proprietary, intellectual property, otherwise controlled and not-for-public-release data, information, or technology.

F3. Deemed Export: Any release of technology, software or source code subject to the EAR, ITAR, OFAC and other regulations to a FN within the United States. Release of technology in the United States, referred to as "Deemed Export" whereas release of technology outside the United States, we call "Export". Release of technology or items in general we label as Technology Transfer. Determination of license requirement depend on the country of citizenship, the item, end-use, Entity List, general prohibitions, license exceptions, etc. Export violations (including from ITAR, OFAC or CUI) can occur with technology transfer to a FN without obtaining the license prior to technology transfer.

F4. Renewal: FNs staying more than one calendar year. Or a renewal can be when FNs return to NOAA after departing within one month of their last departure date. Note: the CTC can designate any FN as a renewal based on past entries into NOAA facilities or doing past activities outside of NOAA. For example: if a FN worked or trained in the National Oceanic Service (NOS) and with a break from NOS arrived at NWS; the CTC can designate the FN as a renewal after discussing with OSY. Renewals need reentry into FNRS to extend their stay past the maximum initial duration of one calendar year or to reenter into FNRS after a one month absence. Enter the FNs renewals into FNRS at least 45- 60 calendar days ahead of their departure dates to prevent gaps in work/training. Renewals have higher chance of denial by senior management to extend for more time in the office/program.

F5. Routine FN: These are FNs from "friendly countries" and not on the Bureau of Industry and Security's Entities List as individual or organization. Routine FNs are also not terrorist-supporting countries under Country Group E of the EAR. In addition, routine FNs cannot be from a country flagged by Office of Foreign Assets Control (OFAC). Talk or email your CTC if you have any concerns on your FN being routine.

F6. High-Risk FN are FNs from Category E countries (terrorist supporting). Any FN from an organization on the Entities List (see BIS website for latest Entities List) or on the list by name – this is a high-risk FN. China and Russia remain high-risk countries at this time. Talk to your CTC to find out more about high-risk countries and extra precautions, if required.

F7. Foreign National Registration System (FNRS): automated system for registering foreign national visitors and guests accessing NOAA/NWS facilities. FNRS registers FNVs and FNGs for entry into specific NOAA facilities, seeking approval from CTC, Designated Official (DO), NOAA Chief Administrative Officer, and the Office of Security. The sponsor of the foreign national and escorts are responsible for entering the FNs information into FNRS including passport number, DOB, country of citizenship, country of permanent residence, prior long-term stays in the United States, job title, their affiliation/company, what they will do while working/training in NWS, etc.

- Not entering FNs into FNRS and/or allowing FNs to stay outside their approved duration period will result in violation of this instruction as well as DAO 207-12 and NAO 207-12. In some cases, law enforcement will investigate undocumented FNs in the workplace.
- Sponsor's First use of FNRS: The CTC or alternates must register you in FNRS upon email or telephone call. Before taking on FN Sponsorship duties: you must take the Espionage Indictors Briefing each year and send the last page (the completed certificate of training) to OSY. You need to take this briefing annually and enter the date of completion into FNRS. Sponsors need to take the Commerce Learning Center on-line course, under NOAA.
- Sponsors must take this course annually. Issues or problems with FNRS: Direct your inquiries on issues logging into FNRS or issues/questions using FNRS to the CTC or to FNRS support.

F8. Manned and Unmanned Facilities: Manned facility is the NWS designated building or office, leased or owned by the U.S. Government/National Weather Service with at least one staff member occupying the facility. Unmanned facilities are the same but without permanent staff occupation such as weather balloon launch buildings, NEXRAD buildings, storage buildings, vacant buildings, etc.

F9. Technology Control Plan (TCP): Each NWS office is responsible for their technology subject to Export Administration Regulations (EAR), International Traffic in Arms Regulation (ITAR), Office of Foreign Asset Control (OFAC), etc. This includes items identified as Controlled Unclassified Information (CUI). Violations can happen and thus each office in NWS will have Technology Control Plans to mitigate technology transfer to foreign nationals. Each manned building must have a TCP. Unmanned building/facilities do not require a separate TCP, but should be referenced in the responsible manned office's TCP. Technology control inventories are included in the TCPs along with CUI and network security. TCPs are very important in reducing and preventing release of controlled technology. The TCP is unique to each facility and/or office and thus each facility or office must have a TCP. The TCP needs to be a standalone document for each NWS facility and office.

F10. EAR99: This designation applies to items that fall under the purview of the EAR, but that are not controlled technology. EAR99 items normally do not require controls; however always check with the NWS CTC before release of any technology, including EAR99, to FNs. EAR99 (commercially available and normally non-controlled items) become controlled technology under certain situations. For example, technology transfer of an EAR99 item to an embargoed or sanctioned country, to a party on the Entities List, in support of a prohibited end-use, to terrorist-supporting country (currently Iran, Cuba, Sudan, Syria and North Korea) will result in controlled technology and violation without license.

F11. Remote Access: Any network access from outside the NWS or network access requiring Virtual Protocol Network (VPN) such as Cisco AnyConnect Secure Mobility Client from within the NOAA/NWS. NWS approves/denies remote access only to Research and Development High Performing Computer System (RDHPCS) and we require additional justification - see "Requesting Remote Access" section. Again, no temporary or permanent remote access allowed for FNs such as for telework and especially outside the United States or in Embassy/Consulates. FN's RDHPCS remote access, if approved, will be from the Government facility only and with a Federal employee escort present.

F12. Technology Transfer: Any export including shipping, giving, emailing, mailing, faxing, etc., to a foreign national, country, embassy or consulate. Technology transfer also means sharing technology or software with a foreign national while in the United States.

F13. Activities/Programs: Any NOAA work with Foreign Nationals such as meetings, training, projects, consulting, telephone calls, emails, etc., regardless of the location. Activities with FNs, even outside of NOAA or on the telephone are reportable to OSY and some events will need entry into FNRS. Talk to your CTC about activities with FNs and when/how to report.

- When conducting virtual meetings using Hangout, or other similar and approved tools attendance should be taken to ensure you are aware if a foreign national logged into the meeting. Virtual meetings that contain CUI or export controlled information should not allow FNs to view or participate. Report any release of controlled technology to your CTC.

F14. “Technology”. Technology means: Information necessary for the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control “technology”) of an item. N.B.: Controlled “technology” is defined in the General Technology Note and in the Commerce Control List (Supplement No. 1 to part 774 of the EAR). NOTE 1 TO DEFINITION OF Technology: “technology” may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection; NOTE 2 TO DEFINITION OF Technology: The modification of the design of an existing item creates a new item and technology for the modified design is technology for the development or production of the new item.

- “Development Technology” is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.
- “Production Technology” means all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance.
- “Use Technology” - we refer to as the “Use Rule” means each one of these six elements must apply for deemed export licensing to happen: Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing. NOTE: If an ECCN specifies one or more of the six elements of “use” in the heading or control text, only those elements specified are classified under that ECCN.