

DOC Foreign National Request Form

Instructions *(This form must be typed).*

This form, once completed and submitted to your Field Servicing Security Office (FSSO), constitutes your obligation to meet the notification requirements outlined in DAO 207-12, Section 5.06.

Part A, B, C, D, E, F, and G, must be completed for all Foreign National (FN) Guest requests. **Note: Only Part A is required for visitors. For a multi-member visitor group/delegation/conference, use Appendix (p. 6) to provide or attach required information (Part A #1-8).**

Part A. *(To be completed by Departmental Sponsor)*

1. Name: Last _____ First _____ Middle _____

2. Title(s): _____

3. Date of Birth (MM/DD/YYYY): _____

4. Gender: M ☐ F ☐

5. Place of Birth (City/State/Country): _____

6. Country of Citizenship (List all): _____

7. Country of Permanent Residence: _____

(If lawfully admitted into the U.S. for permanent residence, provide alien registration (i.e., Green Card) number)

8. Passport Number and Issuing Country (List All): _____

9. Sponsor Organization (Non-DOC/Home Country Affiliation): _____

10. Sponsor's Name and Signature: _____

(Must be a Federal Employee of the Department of Commerce)

11. Sponsor Bureau: _____ Sponsor Phone Number: _____

12. Sponsor Email: _____

13. Facility Number, Name and Address: _____

City, State and Zip Code: _____

14. Visit Arrival Date: _____ Visit Departure Date: _____

(Per DAO 207-12, the FSSO must be notified about itinerary changes or changes related to the visit)

15. Alternate Point of Contact (name, email, phone): _____

16. Is this a RENEWAL? Yes ☐ No ☐ *If YES, provide dates of previous visits in Appendix (p.6).*

17. Purpose of Visit: (No acronyms; Be specific (i.e., associated program name, meeting purpose))

1 CONTAINS PII – Send by Secure File Transmission or other approved methods for PII materials.

Name: Last _____

First _____

Visit Arrival Date: _____

Visit Departure Date: _____

Part B. Justification

1. Please define the collaboration, program, or project scope, and expected contributions by the FN Guest. Include specific detail regarding the FN's affiliations (contract/organization/government/education), qualifications, expertise, scope of work, and how this work will further the Department's mission. The provided justification must also include how the foreign national visit is in the best interest of the DOC Bureau being visited (no acronyms).

2. List previous entry (dates) into the United States:

From: _____ To: _____

From: _____ To: _____

From: _____ To: _____

3. Accounting Code (if required): _____

Part C. Deemed Export: *(To be completed by Departmental Sponsor)*

1. Will the FN Guest have access to technology/information that is NOT publicly available? Yes ☐ No ☐
2. Will the FN Guest have access to any classified, Controlled Unclassified Information (CUI), export controlled, proprietary, or not-for-public release data, information, or technology? Yes ☐ No ☐
(15 C.F.R. § 734.3(b)(3) <https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/412-part-734-scope-of-the-export-administration-regulations>)
3. Will the FN Guest have access to export controlled items that would require an export license? Yes ☐ No ☐
If YES, was written authorization obtained by the owner or originator, or the requisite export license issued by the Bureau of Industry and Security, Department of State, or other regulatory agency? Yes ☐ No ☐
4. Was a controlled technology assessment conducted at the site(s) identified to be accessed by the FN Guest? Yes ☐ No ☐
- a. If controlled technology is resident, is a controlled technology inventory (i.e., equipment, data, etc.) and Access Control or Technology Control plan on file? Yes ☐ No ☐
- b. If not, describe compensatory measures in place to reduce the risk of unauthorized disclosure of classified CUI, export controlled, proprietary, or not-for-public release data, information, or technology:

Name: Last _____ First _____
Visit Arrival Date: _____ Visit Departure Date: _____

Part D. Logical Access Requirements (*To be completed by Departmental Sponsor*). Complete below to define FN Guest logical access requirements as basis for Information Technology Security Officer (ITSO) FIPS 199 risk assessment. Basic logical access may include access to a Bureau email address and standard Bureau unclassified network access. **Note: This form does not replace any other Bureau specific requirements for logical access. FN Guest access to classified/National Security information is prohibited per CAM 1337.70 (Nov 2015), §3.4.3.**

1. Does this FN Guest require basic, on-site logical access? Yes ☐ No ☐

If NO, completion of this part is not required.

- a. Does this FN Guest require remote access?¹ Yes ☐ No ☐

If yes, from what physical location is the FN Guest remoting in from? Home/address?

Has the FN Guest been issued a RSA token or another method of 2FA?

- b. Is privileged access required?^{2,3,4} If yes, proceed to #2. Yes ☐ No ☐

2. In addition to basic logical access to Bureau email and standard unclassified network access, below is a description of the additional IT access that the named FN Guest may be granted permission to use. Include the FIPS 199 security categorization level of the information to be accessed. Security categorization level will be assigned at the highest level in which access is requested.

Low ☐ Moderate ☐ High ☐ Privileged⁵ ☐

Provide details on any Privileged Access required:^{2,3,4} Use Appendix (p. 6) to provide or attach additional information.

3. Access end date (one year maximum from approval date, unless privileged access is required)³: _____

¹ See CITER-022, "End User Responsibilities, Commerce Information Technology Requirement" of April 15, 2015 for guidance. (Email docitsecurity@doc.gov for a copy of CITER-022). Remote Access defined per 2014 ITSP as, "Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). Remote access uses telecommunications to enable authorized access to non-public DOC computing services that would otherwise be inaccessible from work locations outside a DOC LAN or DOC-controlled WAN computing environment. This includes access to non-public DOC IT systems and data that are exposed to the public Internet (e.g., web access to electronic mail by the home user or business traveler) as well as modem dial-up and/or Virtual Private Network (VPN) access to internal DOC IT servers and desktop workstations."

² Privileged Access defined per 2014 ITSP as, "Root or Administrator Access."

³ If privileged access is required, permission must be granted in writing by the system's Authorizing Official and a Tier 2 Minimum Background Investigation (5 year U.S. residency) must be successfully completed and adjudicated prior to privileged access being granted.

⁴ See CITER-026, Privileged Account Management, June 1, 2017. Email docitsecurity@doc.gov for a copy.

⁵ Additional approval from the system's Authorizing Official will be required for overall FIPS199 security categorizations of Moderate or High or Privileged.

Name: Last _____ First _____

Visit Arrival Date: _____ Visit Departure Date: _____

Part E. Limited Unescorted Access (LUA): *(Optional. To be completed by Departmental Sponsor, if required.)*

1. Will the FN Guest require program or project requirements at any point during the duration of the visit?

Yes ☐ No ☐

If YES, provide additional mission-essential justification for the expanded physical and/or logical access including designation of required facility work space or locations, specified hours, and a favorable adjudication of any implications upon contiguous work spaces, locations, programs, and associated Access Control or Technology Control Plans. Final approval is subject to favorable completion of applicable agency checks and related administrative requirements.

Name: Last _____ First _____
Visit Arrival Date: _____ Visit Departure Date: _____

Part F. FN Guest Request Certification: Digital or written signatures acceptable.

1. I certify the benefits to be gained from hosting _____ will further the Department's mission and have been balanced against the need to protect sensitive assets at the Department and the risks associated with failure to protect these assets. I have signed Attachment 2, to the DAO 207-12. "Certification of Conditions and Responsibilities for Departmental Sponsors of Foreign National Guests," and I accept the responsibility for performing the duties set forth in the DAO in order to manage the risks involved with sponsoring foreign nationals in federal facilities. In this regard, I will take all reasonable steps to ensure that my Guest will not have unauthorized physical, visual, or virtual access to classified, CUI, export controlled, proprietary, or not-for-public-release data, information, or technology. I acknowledge by signing below that my FN Guest may not be granted access to classified, CUI, export controlled, proprietary, or not-for-public-release data, information, or technology without written authorization from the owner or originator, or the requisite export license issued by the Bureau of Industry and Security, Department of State, or other regulatory agency.

Printed Name of Departmental Sponsor	Signature of Departmental Sponsor	Date	Organization
--------------------------------------	-----------------------------------	------	--------------

Printed Name of Escort, if required	Signature of Escort	Date	Organization
-------------------------------------	---------------------	------	--------------

Printed Name of Escort #2, if required	Signature of Escort #2	Date	Organization
--	------------------------	------	--------------

2. I certify that the FN Guest collaboration defined above remains within the Span of Control of the Departmental Sponsor and concur that the program/project scope and benefits gained by providing access to Department facilities and resources is balanced with the need to protect classified, CUI, export controlled, proprietary or not-for-public release data, information or technology.

Printed Name of Supervisor	Signature of Supervisor	Date	Organization
----------------------------	-------------------------	------	--------------

3. I concur that the FN Guest collaboration defined above and the benefit gained by access to Departmental facilities and resources is consistent with the need to protect classified, CUI, export controlled, proprietary or not-for-public release data, information or technology, and the strategic interests of the Department of Commerce.

Printed Name of Senior Bureau Official (or designated official)	Signature of Senior Bureau Official (or designated official)	Date	Organization
--	---	------	--------------

Name: Last _____ First _____
Visit Arrival Date: _____ Visit Departure Date: _____

Part G. FIPS199 Validation (*To be initialed and completed by the ITSO upon review of Part D*). Digital or written signatures acceptable.

Based on a review of Part D and the electronic information to be accessed, the overall risk level of the logical access required specified in Part D is accurate:

Printed Name of ITSO or Designee	Signature of ITSO or Designee	Date	Organization
----------------------------------	-------------------------------	------	--------------

If the overall FIPS199 Security Categorization is Moderate or High or Privileged Access is required:

Printed Name of System's Authorizing Official	Signature of System's Authorizing Official	Date	Organization
---	--	------	--------------

Appendix. Space below may be used to insert additional information, visit justification, or supporting documents.