Clear Form

U.S. SOUTHERN COMMAND

Electronic Equipment Entry & Exit Form

PRIVACY ACT STATEMENT

PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting to enter and/or exit USSOUTHCOM facilities with Electronic Equipment (e.g. laptops, personal electronic device (PED), digital cameras, cellular phones, removable hard drives, USB flash drives, etc.). NOTE: Records may be maintained in both electronic and/or paper form.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

REFERENCES. USSOUTHCOM, Policy Memorandum 07-13, Wireless Communications and Personal Electronic Devices, 10 October 2013.

PART I - *(To be completed by individual requesting to enter and/or exit with Electronic Equipment)*

1. Name (*Last, First, Middle Initial*):

2. Designation/Persona:

3. Organization:

4. Citizenship: ☐ US ☐ FN (Country Code: ☐)

5. Official e-mail Address:

6. Phone (DSN or Commercial):

7. Duration of Requirement *(Not to exceed 1yr)*: ☐ — ☐

8. Sponsoring Office:

9. Operational Need / Mission Justification:

10. Is the Electronic Equipment the property of the government or employer?: Yes ☐ ☐ No ☐

11. Identification of Electronic Equipment. (*Provide the Type, Make, Model, Serial #*):

Type	Make	Model	Serial #

Note: If additional items are required, check this box and proceed to page 3. ☐

12. Acknowledgment of Responsibilities (*Place your initials next to each statement as a confirmation of understanding*):

- ☐ I understand that the misuse of electronic equipment and/or violation of USSOUTHCOM Policy Memorandum 07-13 will result in a revocation of any potential approval(s) for a minimum of 30 calendar days. Reinstatement of an approval will require an additional request form accompanied by proof of remediation training.
- ☐ I agree to not connect electronic equipment to any USSOUTHCOM information system (e.g. NIPRNet/SIPRNet/ COM-ISP enclaves) unless explicitly authorized in writing the by the USSOUTHCOM Authorizing Official.
- ☐ I understand my responsibility to protect Controlled Unclassified Information and Classified Information and will ensure all information that is processed, transmitted, and/or stored on approved electronic equipment does not exceed the devices designated classification level.
- ☐ I will ensure Wi-Fi, RF, Bluetooth, image capturing (e.g. camera), and audio capturing capabilities are disabled prior to entering USSOUTHCOM facilities.
- ☐ I understand any potential approvals associated to this request does not pertain to facilities outside of the US Army Garrison - Miami compound and additional coordination with external organizations is required.
- ☐ I understand any potential approvals associated to this request does not automatically pertain to Sensitive Compartmented Information Facilities (SCIFs) and additional coordination with SCIF Security Managers is required.

13. Requester Digital Signature. *By signing this request, I certify that all information provided is true and I will uphold the responsibilities.*	13. Date *(YYYY-MM-DD)*:

PART II - Endorsement of Request by Sponsoring Office *(Government Leadership Signature Required)*

By signing this request, I certify this request is mission essential, and accept responsibility for ensuring the reduction of the overall risk to spillage(s), espionage, insider threat(s), and that privileges are utilized in accordance with Joint Ethics Regulation and applicable DOD policies. I understand the responsibilities and will ensure the requester adheres to the standards set forth in the references and section 11.

If the Electronic Equipment will require access to a SCIF check this box and have Requester complete page 4 (SCIF Addendum): ☐

1. Name *((Last, First, Middle Initial))*:	2. Digital Signature:	3. Date *(YYYY-MM-DD)*:

PART III – Information System Security Manager (ISSM) Approval

Based on the documentation and other evidence provided, I certify that the applicant has satisfied the requirements for the entry and/or exit of the Electronic Equipment identified in section 10.

1. Name *(Last, First, Middle Initial)*:	2. Digital Signature:	3. Date *(YYYY-MM-DD)*:

PART IV – SCIF Management Approval (*Only required if accessing a SCIF*)

Based on the documentation and other evidence provided, I certify that the applicant has satisfied the requirements for the entry and/or exit of the Electronic Equipment identified in section 10. See attached SCIF Approval.

1. Name *(Last, First, Middle Initial)*:	2. Digital Signature:	3. Date *(YYYY-MM-DD)*:

11. Identification of Electronic Equipment. (*Provide the Type, Make, Model, Serial #*):

Type	Make	Model	Serial #

U.S. SOUTHERN COMMAND

Electronic Equipment Entry & Exit Form

Sensitive Compartmented Information Facilities (SCIF) Addendum

REFERENCES. USSOUTHCOM, Policy Memorandum 07-13, Wireless Communications and Portable Electronic Devices, 10 October 2013.

Defense Intelligence Agency Instruction (DIAI) 8460.002, Portable Electronic Devices, 03 March 2015

PART V— Requested Entry Areas

1. BUILDING:	2. FLOOR:	3. SECTION/ROOM #:	4. SCIF ID:

5. NOTES: *(Remarks if additional requirements are required)*

6. Acknowledgment of Responsibilities (*Initial next to each statement as confirmation of understanding*):

☐ I understand my responsibilities and will comply with procedures set forth in the Defense Intelligence Agency Instruction (DIAI) 8460.002, "Portable Electronic Devices," dated 03 March 2015.

☐ I am fully aware that it remains my inherent responsibility as an employee, contractor, or member of the armed forces assigned to DoD, to fully protect all Sensitive material in my custody, ensuring against loss or compromise. Nothing in the foregoing shall be constructed to excuse my use of good judgment and common sense to provide maximum security protection of the information entrusted to my possession.

☐ I understand that USB storage devices are not allowed in USSOUTHCOM spaces without prior notification and approval from Information Assurance Managers (IAMs).

☐ I understand that I am only allowed to bring in those devices approved by my Special Security Office (SSO) annotated on this form.

☐ I understand that the U.S. Government (USG) through a designated representative of the Department of Defense (DoD) may seize my electronic equipment for security purposes and that the USG or its designee may conduct a physical and forensic examination of the equipment. I understand that electronic equipment seized as evidence of a crime or security violation will be handled under DoD Investigative Policies. In some cases, electronic equipment may be permanently retained, destroyed, or have their data and operating systems wiped resulting in loss of information.

☐ I understand that if I have a legitimate claim or loss or damage to a personal electronic equipment, not lost or damaged through my own negligence or violation of security procedures, that I may file a claim in accordance with claims procedures administered by the military departments.

ACKNOWLEDGEMENT (*Acknowledge of the above responsibilities is in addition to the responsibilities outlined in Part I, Section 11*):

7. SIGNATURE:	8. DATE: