VISITOR PORTABLE ELECTRONIC DEVICE (PED) AUTHORIZATION

PED VERIFIED BY: *(Uniformed Security Officer)* ______________________ *(Type or print full name)* DATE: __________

SIGNATURE: ______________________

I. REQUESTOR INFORMATION

1. NAME: ______________________ *(Type or print full name)*
2. BADGE: __________ *(If applicable)*
3. ORGANIZATION: ______________________
4. OFFICE DESIGNATION: __________
5. LOCATION: __________
6. SECURE PHONE: __________
7. E-MAIL: ______________________
8. REQUESTOR SIGNATURE: ______________________
9. DATE: __________

II. VISITOR CONTROLLED PED INFORMATION

1. TYPE/NAME OF DEVICE: ______________________
2. MAKE/MODEL NUMBER: ______________________
3. SERIAL NUMBER: ______________________
4. CLASSIFICATION: ______________________
5. EXTERNAL COMPONENTS: *(e.g., storage devices, complete Section VII, if required)* □ YES □ NO
6. OPERATING SYSTEM AND SOFTWARE LIST: *(continue in Section VIII, if required)* ______________________
7. JUSTIFICATION / INTENDED USE FOR PED: *(continue in Section VIII, if required)* ______________________
8. □ GOVERNMENT-OWNED
9. □ CONTRACTOR-OWNED
10. COMPANY/AGENCY NAME: ______________________
11. COMPANY/AGENCY ADDRESS: ______________________

III. LAPTOP *(Complete for a laptop; list additional drives on continuation page, if necessary)*

1. DRIVE: __________ CLASSIFICATION: __________
2. DRIVE: __________ CLASSIFICATION: __________
3. NRO ISSO INSPECTION COMPLETION DATE: __________
4. REGISTRATION NUMBER: *(If applicable)* __________

IV. DESCRIBE SYSTEM CONNECTIVITY *(Continue in Section VIII, if necessary)*

V. VISITOR PED ENTRY / EXIT PROCEDURE

The visitor must have the cognizant NRO PSO and ISSO complete this section prior to entering and / or exiting with the PED to / from NRO secure facilities and show a copy to the uniformed Security Officer in order to enter / exit with the identified PED.

I VALIDATE THAT THIS USER MAY □ ENTER □ EXIT WITH THE IDENTIFIED PED TO / FROM NRO SECURE FACILITIES. UPON EXIT, I HAVE ENSURED ALL NRO LABELS ARE REMOVED AND SANITIZED ANY UNAUTHORIZED DATA.

1. PSO NAME: ______________________ *(Type or print full name)*
2. BADGE OR PCN: __________
3. PSO SIGNATURE: ______________________
4. DATE: __________
5. ISSO NAME: ______________________ *(Type or print full name)*
6. BADGE OR PCN: __________
7. ISSO SIGNATURE: ______________________
8. DATE: __________

PRIVACY ACT STATEMENT

Authority: Relevant authorities for this system include Title III of the E-Government Act of 2002 (P.L. 107-347); Subtitle III of 40 U.S.C., Information Technology Management; 10 U.S.C. 2224, Defense Information Assurance Program; E.O. 12333, as amended, United States Intelligence Activities; DoD Directive 8500.1, Information Assurance; DoD Instruction 8500.2, Information Assurance Implementation; Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation; Intelligence Community Standard (ICS) 500-18, Removable Media Management; ICD 705, Sensitive Compartmented Information Facilities.

Purpose(s): To identify, administer, monitor, and track the use and access via GPEDs of NRO networks, computers, software, and databases. Records may also be used to identify the occurrences of and assist in the prevention of computer misuse.

Routine uses: In addition to the statutory disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act, under QNRO-32 these records may specifically be disclosed outside the NRO as a routine use pursuant to 5 U.S.C. 552a(b)(3). Disclosures may be pursuant to the following DoD 'Blanket Routines Uses' published in the Federal Register at the beginning of the NRO compilation of systems of records notices:

1. *Law Enforcement*
2. *Disclosure When Requesting Information*
3. *Disclosure of Requested Information*
8. *Disclosure to the Office of Personnel Management*
9. *Disclosure to the Department of Justice for Litigation*
12. *Disclosure of Information to the National Archives and Records Administration, (NARA)*
14. *Counterintelligence Purpose*
15. *Data Breach Remediation Purposes*

Disclosures: Disclosure of information is voluntary; however, failure to provide complete information may delay processing of the form.

CL BY:
DECL ON:
DRV FM:

OPR: OS&CI/MSD/PB

PREVIOUS EDITIONS ARE OBSOLETE

VISITOR PORTABLE ELECTRONIC DEVICE (PED) AUTHORIZATION (Continued)

VI. APPROVALS FOR USE WITHIN NRO FACILITIES

1. NRO GOVERNMENT VALIDATOR NAME: ____________________ *(Type or print full name)* 2. BADGE OR PCN: __________

3. NRO GOVERNMENT VALIDATOR SIGNATURE: ____________________ 4. DATE: __________

5. PROGRAM MANAGER NAME: ____________________ *(Type or print full name)* 6. BADGE OR PCN: __________

7. PROGRAM MANAGER SIGNATURE: ____________________ 8. DATE: __________

9. PSO NAME: ____________________ *(Type or print full name)* 10. BADGE OR PCN: __________

11. PSO SIGNATURE: ____________________ 12. DATE: __________

13. ISSO NAME: ____________________ *(Type or print full name)* 14. BADGE OR PCN: __________

15. ISSO SIGNATURE: ____________________ 16. DATE: __________

VII. INFORMATION SYSTEMS SECURITY OFFICER ONLY *(Continue in Section IX, if required)*

1. DEVICE CAPABILITIES:	2. RISK MITIGATIONS:	3. VERIFICATION: *(ISSO initials)*

4. REGISTRATION NUMBER: __________ 5. DATE REGISTRATION LABEL AFFIXED: __________

6. DATE ADDED TO DATABASE: __________

7. SYSTEM SECURITY PLAN, CO-LOCATION, OR CONOP ON FILE: □ YES □ NO

8. ISSO SIGNATURE: ____________________ 9. DATE: __________

VIII. VISITOR CONTROLLED PED INFORMATION *(Continued)*

IX. EXTERNAL COMPONENT CONTINUATION *(As required)*

1. DEVICE CAPABILITIES:	2. RISK MITIGATIONS:	3. VERIFICATION: *(ISSO initials)*

4. ADDITIONAL INFORMATION:

VISITOR PORTABLE ELECTRONIC DEVICE (PED) AUTHORIZATION (Instructions)

NOTE: Approval must be coordinated with the Program Security Officer (PSO) and Information System Security Officer (ISSO) prior to authorizing entry, use and exit of the device. The visitor must also obtain the PSO's approval prior to taking the device to the ISSO for functionality review.

UNIFORMED SECURITY OFFICER VERIFICATION

An NRO Uniformed Security Officer will verify the visitor has coordinated PED entry / exit with the NRO PSO and ISSO. Verification will consist of completion of the form and checking the PED serial number(s) against the data provided below.

I. REQUESTOR INFORMATION

The visitor will enter pertinent information, sign and date.

II. VISITOR CONTROLLED PORTABLE ELECTRONIC DEVICE (PED) AUTHORIZATION

1-3. Type, model, serial # of PED.

4. Highest Classification of information authorized to be stored or processed by PED.

5. External add-ons, such as removable media, peripherals, etc. If present, list and complete Section VII.

6. Operating system / software installed on the PED.

7. Justification for bringing PED into NRO Secure Facilities and intended use of the PED.

8-9. Is the PED Government owned or Contractor owned?

10-11. Contractor-owned PED information.

III. LAPTOP INFORMATION ***(Laptops are the only PED that may be approved for CLASSIFIED processing)***

1-2 Provide the highest classification of the information to be stored / processed on this laptop. Include a listing of drives or other removable storage media and their classifications.

3. The ISSO will inspect and register, if appropriate, the PED.

IV. DESCRIBE SYSTEM CONNECTIVITY

The requestor will indicate if connectivity for which the PED is approved. Provide details such as description of the connected system (e.g., NMIS, UMIS), where it is located (WF), and how the PED is connected (e.g., wired, wireless). An NRO Government PM must justify connectivity of any PED. Approval must be coordinated with the PSO, ISSO, and F&ISD and may require an SSP on file and CIO approval in accordance with NRO Directive 50-20 and other applicable directives and regulations indicating that this PED is approved for connectivity.

V. VISITOR PED ENTRY / EXIT PROCEDURES

1-8. The PSO and ISSO will enter this data, sign, and date to validate that the device may enter and / or exit from NRO secure facilities. The PSO will review data on the PED to ensure no unauthorized information is exfiltrated. The ISSO will remove the PED registration label and make the appropriate changes in the database, if applicable. The visitor must show this Form to the Uniformed Security Officer in order to enter / exit NRO facilities with the PED.

VI. APPROVALS FOR USE WITHIN NRO FACILITIES

The visitor must obtain approval signatures prior to introducing the PED into NRO Secure Facilities. The Uniformed Security Officer will validate that the PSO has approved the device and sign and date the form upon initial entry. This form and device must be immediately taken to the ISSO for PED review and mitigation, if required. The ISSO will also register the device, as appropriate.

VII. ISSO ONLY

1. Device capabilities: list PED functions.

2. Risk Mitigations: describe how NRO Directive 50-20 and NRO Instruction 50-20-1 requirements have been implemented to mitigate the PED's risk-related functions.

3. Verification: the ISSO will verify that these risk mitigation requirements have been met and initial each item.

4-6. The ISSO will affix the facility PED registration label and add the information to the PED tracking database, as required.

7. The ISSO will annotate the date of a verified, approved System Security Plan, Co-Location request, or CONOP for this PED.