



**Onsite Non-US Government-Owned
Controlled Article Authorization Form**

When properly executed, this form authorizes the described controlled article (see [P217 Controlled Articles](#)) to reside at, or be removed from, LANL during the specified period of time. No other controlled article may be substituted under this authorization. **The original, signed form must be kept with the controlled article at all times, and a copy sent to the Information Security Office by fax at 505-665-1799, or mail at Mail Stop MS B289.**

The controlled article may not be taken into a Sensitive Compartmented Information Facility (SCIF) or an area where Top Secret or Special Access Program (SAP) information is processed without prior approval of the SCIF or area security official.

Section 1: User and Controlled Article Identification

The controlled article shall be stand-alone OR connected to the LANL Visitor Network. Proof of required Information Security Training, if applicable, must be attached to this form when submitted.

I understand that the controlled article presents a risk to LANL information and information systems; therefore, steps must be taken to reduce the risk to sensitive and classified information while the device is on LANL property. I have received LANL Information Security Training (if applicable), discussed the security implications of my request with an Organizational Cyber Security Representative (OCSR), a System Administrator, or the Office of the Chief Information Officer (OCIO), understand my responsibilities, and will follow the LANL Rules of Use for Onsite Non-US Government-Owned Controlled Articles (see Page 4).

I agree to cooperate fully with LANL management in any investigation regarding misuse of the device. If the device becomes contaminated with sensitive or classified information while on LANL property, I will cooperate fully with Information Security personnel to ensure that the device is properly protected and sanitized. Further, I understand that failure to follow these rules may result in seizure of the device and its media and issuance of a security infraction.

_____ Device User's Signature _____ Date _____

Period of authorization at LANL:
 Start Date: _____ Expiration Date: _____

Non-US Government-Owned Controlled Article Identification		
Device User <i>[print name]</i>	Government Agency/Sponsored Company	Visitor's Z Number or ID Number
Email Address	Phone Number	Fax Number
Mail Stop and Office Location	Controlled Article Model and Serial/Property No.	
Where was the controlled article obtained? (e.g., country; colleague; retail outlet, etc.)		
Location of controlled article while in use at LANL: TA: _____ Bldg.: _____ Rm.: _____		
Will the controlled article be located in a LANL Security Area? <input type="checkbox"/> Yes <input type="checkbox"/> No		
Is the anti-virus software installed and functioning, and is the virus definition (DAT) file current? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A (If No or N/A, explain):		
Audio Recording (<i>sound recording through a microphone</i>)? <input type="checkbox"/> None <input type="checkbox"/> Enabled <input type="checkbox"/> Disabled: _____		
Radio Frequency (RF) Transmit (<i>cell 802.11, Bluetooth, satellite, RFID, etc.</i>)? <input type="checkbox"/> None <input type="checkbox"/> Enabled: Type: _____ <input type="checkbox"/> Disabled: _____		
Video Record/Photos? <input type="checkbox"/> None <input type="checkbox"/> Enabled <input type="checkbox"/> Disabled: _____		
Infrared (IR) Port? <input type="checkbox"/> None <input type="checkbox"/> Enabled <input type="checkbox"/> Disabled: _____		
Detailed description of how the controlled article device will be used for business at LANL (<i>explain why government-owned and controlled equipment is not being used instead.</i>) Attach additional descriptions if needed.		

Sections 2, 3 and 4 - Exception Requests

Please complete sections 2, 3, and 4, for a non-US government-owned controlled article, to request an exception to:

- process and store Controlled Unclassified Information (CUI) (complete **Section 2**);
- connect device to a LANL information system or network, other than the Visitor (Gray) Network (complete **Section 3**); and/or
- introduce the device inside a Limited Area (LA) (complete **Section 4**).

Section 2: Sensitive Government Information on a Non-Government Controlled Article

Describe the encryption and other information-protection mechanisms that will be used to protect the information, where the device will be while it is storing the sensitive government information, and how and when the device will be sanitized.

If the source of the sensitive information to be stored on the device is not from LANL, from where will the sensitive information be received? (e.g., country, organization, colleague/citizenship, etc.)

What type of data will be stored on the device?

Identify the sensitivity level of the information to be stored on the device (*check all that apply*):

Non-sensitive (*skip to next section*) Official Use Only (OUO)

Personally Identifiable Information (PII) (Privacy Act)

Cooperative Research and Development Agreement (CRADA)

Unclassified Controlled Nuclear Information (UNCI)

Naval Nuclear Propulsion Information (NNPI) Export Controlled Information (ECI)

Other No LANL Information

Based on the information provided, I agree that this controlled article may be used to record and store identified LANL information.

Responsible Line Manager (RLM) (*signature*): _____ Date: _____

Section 3: Non-Government Controlled Article Connected to LANL Information System or Network

For information on access to the Visitor (Gray) Network and other LANL networks, visit the [Network Access](#) website.

While connected to any Laboratory network, all non-US government controlled articles should be protected, scanned, and managed as if the devices were LANL-owned devices (all software licensed, operating system configured according to LANL Information Architecture [IA] Standards, automatic anti-virus updates and patches installed). Explain how the LANL network will be protected from potential vulnerabilities introduced by this device.

If the approved device will be connected to a LANL networked computer, identify the computer:

Property Number: _____ IP Number: _____

What LANL network will the device connect to: Yellow Turquoise Gray

Based on the information provided, I certify that this device has been configured for use on the LANL network.

LANL Network Administrator (*signature*): _____ Date: _____

Section 4: Non-US Government-Owned Controlled Article Introduced into a Limited Area (LA)

Section 4a: Non-US Government-Owned Controlled Article in a Limited Area (LA)

All data transmission and information recording features (on non-medically-necessary devices) must be disabled on this device while it is located in an LA.

Device User's Clearance Level: Q L DOD Uncleared & Escorted

Escort's Signature (*if applicable*): _____ Date: _____

Section 4b: Medically Necessary Non-US Government-Owned Controlled Article in a Limited Area (LA)

Device description (*please do not include personal information*): _____

LANL Occupational Medicine's Verification: This device is required for the continued wellbeing of the user and is considered medically necessary for the ongoing treatment of the patient.

Physician or Physician's Assistant Signature: _____ Date: _____

Note: This verification does not give final approval for the device to be introduced in all LANL areas. Safety and security concerns in certain areas may deem use of this device inappropriate. Check with the local safety and security personnel if the approved location of this device changes.

LANL Information Security Approvals for Required Exception(s)

A LANL System Administrator (SA) or OCSR must verify that device features are described and disabled as stated.

SA or OCSR (*signature*): _____ Date: _____

Based on the information provided, I certify that this device is configured as stated.

Local RLM (*signature*): _____ Date: _____

For LANL Information Security Use Only

Submit request to Information Security (Fax 665-1799 or MS B289). Do not introduce the controlled article into an LA or connect to a LANL system until approvals are obtained.

Information Security Approval:
This approval is required for controlled articles that cannot disable audio, video, or wireless in a Security Area. This device is approved to operate as identified and configured.

Approved for use in a Security Area:	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Approved for use on the Yellow Network:	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Approved for storage of CUI	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Request denied - see notes below for explanation	<input type="checkbox"/> Yes	<input type="checkbox"/> No

LANL Information Security Site Manager (ISSM) (*or LASO Designated Approving Authority [DAA]*):

ISSM (*signature*): _____ Date: _____

LASO DAA (*signature*): _____ Date: _____

Technical Surveillance Countermeasures (TSCM) Approval
This approval is required for controlled articles that cannot disable audio, video, or wireless in a Security Area. This device is approved to operate as identified and configured.

TSCM Manager (*signature*): _____ Date: _____

Information Security Notes:

- All conversations that occurred and agreements that were made while investigating this request must be documented.
- Attach any e-mail correspondence that was used to approve or disapprove the request.
- If LASO approval or concurrence was sought, attach associated documentation.
- If the authorization was not approved, document the reason and suggested alternatives.
- In all cases, the controlled article may not be taken into a classified workspace, a SCIF or an area where Top Secret or SAP information is processed without the approval of the area security official.
- This form cannot be used to request wireless networks (802.11, Bluetooth, etc.) anywhere at LANL.
- A full accreditation is required for wireless networking.
- Non-LANL-issued cellular phones cannot be approved for introduction into Security Areas.
- Contact LANL Information Security for further guidance, if needed.

LANL Rules of Use for Onsite Non-US Government-Owned Controlled Articles

A non-US government-owned controlled article is defined as a device that includes the following categories of items:

- Desktop computers, laptop computers, and tablet computers
- Recording equipment
- Copiers and/or scanners with a hard drive
- Compact Disc/Digital Video Disc (CD/DVD) write drive and media
- External hard drive and media and/or thumb drive and media

This form authorizes onsite use of non-US government-owned controlled articles in the following situations.

- A stand-alone controlled article device is allowed in General Access Areas (GAAs), Property Protection Areas (PPAs), and with authorization, LAs.
- Gray network connections are allowed.

The RLM for the organization or facility where the assigned user/visitor will work is responsible for ensuring that all requirements for use of controlled articles are communicated and implemented. A non-US government-owned controlled article device may be brought onsite during the course of authorized LANL and/or government business. When the device is onsite, the following conditions must be met.

1. Each device must have a properly executed [Form 1897](#), *Onsite Non-US Government-Owned Controlled Article Authorization Form* that is kept with the device at all times. The period of residence at LANL for the device must not exceed the expiration date authorized on the form.
2. If LANL information is to be processed on the device, the device user must successfully complete required security training as specified in the LANL Site Security Plan. See the following online course (available through UTrain) before accessing LANL computing resources:
 - a. [Course #9369](#), *Initial Information Security Briefing*.
 - b. **Note:** a Z number is required to get credit through UTrain.
3. The device will not be used to store any US Government or LANL CUI without prior authorization using [Form 1897](#).
4. The non-US government-owned device may not be connected to any other LANL computing or telecommunication resource without authorization documented on [Form 1897](#).
5. The device must not be introduced into a LANL Security Area without prior authorization using [Form 1897](#).
6. The device must not be introduced into a SCIF or an area where Top Secret or SAP information is processed without prior approval of the SCIF or area security official.
7. Wireless capabilities must be disabled while the device is on LANL property, with the exception of the Visitor Network in GAAs and PPAs.
8. All non-US government-owned controlled articles that process LANL information are subject to audit and monitoring of user activities.