



**OnSite Non-LANL-Owned but Government-Owned  
Unclassified Controlled Article Authorization Form**

**This Form must be kept with the **Unclassified** Controlled Article at all times while at LANL**

When properly executed, this form authorizes the described **unclassified** controlled article (see [P217 Controlled Articles](#)) to reside at, or be removed from, LANL during the specified period of time. No other unclassified controlled article may be substituted under this authorization.

**This **unclassified** 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.**

The controlled article shall be stand-alone OR connected to the following **Unclassified** LANL system(s)/network(s):

\_\_\_\_\_ Network Name(s)

The assigned user/visitor of the unclassified controlled article agrees to follow the LANL *Rules of Use for Onsite Non-LANL-Owned but Government-Owned **Unclassified** Controlled Articles* ([see page 3](#)).

*I agree with these terms and accept responsibility for the proper use of the non-LANL-owned but government-owned **unclassified** controlled article device in the performance of my work at LANL. Further, I understand that failure to follow these rules may result in seizure of the unclassified computer and its media and issuance of a security infraction.*

\_\_\_\_\_  
Assigned User/Visitor Signature

\_\_\_\_\_  
Date

**Period of authorization at LANL:**

Start Date: \_\_\_\_\_  
(Approved for a maximum of one year)

Expiration Date: \_\_\_\_\_

**Unclassified Controlled Article Identification**

Assigned User/Visitor [print name]	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.	Controlled Article Accreditation ID No.

Location of controlled article while in use at LANL: TA: \_\_\_\_\_ Bldg.: \_\_\_\_\_ Rm.: \_\_\_\_\_

Will the controlled article be located in a LANL Security Area?  Yes  No

Is the anti-virus software installed and functioning, and is the virus definition (DAT) file current?

Yes  No  N/A

(If No or N/A, explain):

Audio Recording (sound recording through a microphone)?  None  Enabled  Disabled: \_\_\_\_\_

Radio Frequency (RF) Transmit (cell 802.11, Bluetooth, satellite, RFID, etc.)?

None  Enabled: Type: \_\_\_\_\_  Disabled: \_\_\_\_\_

Video Record/Photos?  None  Enabled  Disabled: \_\_\_\_\_

Infrared (IR) Port?  None  Enabled  Disabled: \_\_\_\_\_

**Attach the accreditation documentation from the accrediting site and any additional information.**

**Certification by the Sponsoring Organization's Organizational Computer Security Representative (OCSR)**

I have been advised that the <b>unclassified</b> controlled article device described above is onsite, configured according to the appropriate security plan and the assigned user/visitor has been provided the appropriate LANL security training.			
Print or Type Name	Organization	Signature	Date

**Authorization by LANL Responsible Line Manager (RLM)**

This non-LANL-owned but government-owned <b>unclassified</b> controlled article device is required for use in the performance of authorized LANL and government business.			
Print or Type Name (RLM)	Organization	Signature	Date

**After completion by the Sponsoring Organization's OCSR, with authorization from the LANL RLM, send completed form and associated documentation to the Information Security Office Point-of-Contact at:  
E-mail: [cheryla@lanl.gov](mailto:cheryla@lanl.gov); or fax: 665-1799.**

**Authorization by LANL Information Security Site Manager (ISSM)**

LANL accepts the accreditation of this system.

Signature of ISSM	Date
-------------------	------

**Certification of Cancellation**

LANL authorization of this system has been cancelled. After cancellation, E-mail or fax this form to the Information Security Office Point-of-Contact at: E-mail: [cheryla@lanl.gov](mailto:cheryla@lanl.gov); or FAX: 665-1799.

Signature of OCSR	Date
-------------------	------

## Instructions for Onsite Non-LANL-Owned but Government-Owned **Unclassified** Controlled Articles

This form is to be used to identify, authorize and manage a non-LANL-owned but government-owned **unclassified** computer, defined as a controlled article. A controlled article device, if authorized and certified, may be used on LANL property and connect to authorized networks for up to one year.

If the controlled article device will be on LANL property longer than one year, it will have to be re-approved.

1. The assigned user's/visitor's host is responsible to notify his or her Organizational Computer Security Representative (OCSR) of an upcoming visit to LANL that involves the use of a non-LANL-owned but government-owned **unclassified** controlled article device.
2. The host must receive a copy of the accreditation documentation from the accrediting site for the assigned user's/visitor's system, which is to be attached to [Form 1865, Onsite Non-LANL-Owned but Government-Owned \*\*Unclassified\*\* Controlled Article Authorization Form](#) (see Page 1).
3. The assigned user/visitor is required to sign and date the form.
4. If the LANL Responsible Line Manager (RLM) authorizes the visitor's controlled article device, the RLM shall sign and date the authorization on Form 1865 (see Page 1).
5. LANL's sponsoring organization's OCSR completes, signs, and submits Form 1865.
6. LANL's sponsoring organization's OCSR must ensure that the system owner has read and understands the *Rules of Use for Onsite Non-LANL-Owned but Government-Owned **Unclassified** Controlled Articles*.
7. A copy of the completed, signed Form 1865 must remain with the assigned user's/visitor's controlled article device at all times while on LANL property.
8. The OCSR is responsible to e-mail or fax a copy of Form 1865, with accreditation documentation included, to the Information Security Office at: e-mail: [cheryla@lanl.gov](mailto:cheryla@lanl.gov); or fax: 665-1799.
9. The Information Security Site Manager (ISSM) will review Form 1865 and, if appropriate, approve the visitor's system for use at LANL by signing the form and sending it back to the ISSO and/or OCSR. **Note:** ISSM approval is required prior to the controlled article device being connected to the unclassified Local Area Network (LAN).
10. Upon completion of the visit, as indicated by the Expiration Date on Form 1865, the sponsoring organization's OCSR must ensure that the controlled article will no longer be used at LANL in the capacity it was approved for under the current, signed Form 1865. The visitor must return the original, signed Form 1865 (that has accompanied the controlled article throughout the visit), along with the device for ID verification, to the OCSR before the device is due to be removed from LANL property. If an extension to the visit is necessary, the OCSR may complete and submit the appropriate forms for re-approval.
11. To document the closure, upon removal of the controlled article from LANL property, the OCSR will note on Form 1865 that the system is no longer accredited at LANL and send a copy of the Form 1865 to the Information Security Office at mail stop B289; where it will be stored for a minimum of one year.

## Rules of Use for Onsite Non-LANL-Owned but Government-Owned **Unclassified** Controlled Articles

A non-LANL-owned but government-owned **Unclassified** 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 unclassified onsite use of non-LANL-owned but 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 Limited Areas (LAs).
- Yellow or 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 controlled article use are communicated and implemented. A non-LANL-owned but government-owned **unclassified** controlled article may be brought on site during the course of authorized LANL and/or government business. When the non-LANL-owned but government-owned unclassified controlled article is on site, the following conditions must be met.

1. Only **unclassified** information may be processed on the device.
2. Each **unclassified** controlled article device must have a properly executed [Form 1865 Onsite Non-LANL-Owned but Government-Owned \*\*Unclassified\*\* 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 one year.
3. Each **unclassified** controlled article device must have a copy of the accreditation documentation (this documentation is from the information system's security organization at the site that accredited the system) attached to Form 1865.
4. If LANL information is to be processed, the assigned user/visitor must successfully complete required security training as specified in the LANL unclassified Site Security Plan (see the following online courses in UTrain before accessing LANL unclassified resources).
  - [Initial Computer Security Briefing, Course 9369](#).
  - Note: a Z number is required to get credit for online classes through UTrain.
5. The non-LANL-owned but government-owned controlled article approved on Form 1865 ([see Page 1](#)) may **not** be connected to any other LANL computing or telecommunication resource without authorization documented on Form 1865.
6. If the controlled article device will be on site for 30 days or longer, the assigned user/visitor must register as a LANL computer user, receive a Computer User Profile, and sign a Computer User Profile Acknowledgment. This can only be completed by the device's assigned user/visitor if they have a LANL Z number. Users may visit the [XCP/XTD Information Security Website](#) and click on the XTD Forms Tab to reach the registration Web page.
7. A non-LANL-owned controlled article device must 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.
8. Wireless capabilities must be disabled while the controlled article is on LANL property, with the exception of GAAs.
9. All non-LANL-owned but government-owned controlled articles which process LANL information are subject to audit and monitoring of user activities.

**Note:** A non-government-owned **Unclassified** controlled article brought on site and used to access LANL networks requires a different form:

- Access to the unclassified Protected (Yellow) network or Visitor (Gray) network requires [Form 1897, Onsite Non-U.S. Government-Owned Controlled Article Authorization Form](#).