

Instructions for Filling out the F-2311 Computer Security Plan Form

The completed F-2311 form must be signed by the LLNL Host, ISSO, OISSO and Associate Director and submitted to Computer Security Operations for approval. In addition, a programmatic justification memo, signed by the Associate Directorate of the host directorate, must be submitted to CSO for all foreign nationals (see [Foreign National Information](#)).

1. Personal Identification & Information

- Visitor/Assignee Name: Full name as shown on the Form IA-473 or LLNL Form 6333.
- Citizenship: All countries of citizenship as shown on the Form IA-473 or LLNL Form 6333.
- VTS No. (if assigned): Specify the Visitor Tracking System number for the Visitor/Assignee.
- Time period access is required: The period of time (dates) for which access is requested. (Must correspond to with the information in the LLNL Foreign National Visitor Office database.)
- Permanent Resident Alien (PRA) Number (If applicable): If Visitor/Assignee is a PRA, enter their PRA number.
- Organizational Affiliation: The organization or company that the Visitor/Assignee is representing during their visit to LLNL.
- Location(s) approved for physical access at LLNL: The location(s) where the Visitor/Assignee will be performing their work using the approved computer(s). (Must correspond to with the information in the LLNL Foreign National Visitor Office data base.)

2. LLNL Host (Sponsor) Identification

The LLNL Host must be an LLNL employee with US citizenship who will have direct managerial responsibility for the Visitor/Assignee. The Host is responsible for all activities of the Visitor/Assignee including assurance of access to only the information and systems needed by the Visitor/Assignee to carry out their work assignment, and physical access of the Visitor/Assignee to those areas of the Laboratory authorized by the Foreign Visitors Office. The Host must have on file with CSO a signed copy of the Computer Security Responsibilities of Hosts form, F-2312.

3. Computer System(s) Identification

- Primary Computer System - DNS (Internet) Name: The hostname of the primary computer to be used by the Visitor/Assignee. (example: host.llnl.gov)
- IP Address: The numeric IP address assigned to the Primary Computer System (e.g., 128.115.1.1)
- Computer Location: The building and room number where Primary Computer System is located. If the Primary Computer System is located off site enter the general location. (example: University of New Mexico)
- DOE No.: The LLNL property tag number. If the computer is off-site and privately owned, state that fact.
- Manufacturer and Model: Enter if known.

If the Visitor/Assignee will be using more than one computer, please complete one additional entry for each additional system and, if needed, use the supplemental data sheet(s) supplied as part of this packet. The approval of the ISSO and OISSO responsible for each system accessed by the Visitor/Assignee is required.

4. Network Identification

Indicate all networks that will be used to access the computing resources used by the Visitor/Assignee.

5. Information Access

- Knowledge of the location and accessibility of sensitive unclassified information on each system used by the Visitor/Assignee is required. Explanation of the protection mechanisms for this information is required.
- If the Visitor/Assignee is required to have access to sensitive unclassified information, approval by an Associate Director is required for each directorate that has ownership of information accessed. Describe the mechanisms for assuring that the information is protected while being used by the Visitor/Assignee.
- If the Visitor/Assignee is required to have access to any hardware or software that may have an impact on any system's security features (e.g., Root accounts or Administrator privileges), describe the mechanisms to protect that machine and other machines on networks which could be compromised using these privileges.

6. Remote Access to LLNL

This section of the form, if signed by the Visitor/Assignee and submitted as part of a completed F-2311, can be used in lieu of form F-2410, "Record of Remote Access Accounts for Restricted Open (Yellow) Network".

Remote access accounts for each Visitor/Assignee must be renewed annually. If these accounts are for a Foreign National from a sensitive country, a new application with signatures is required.

3. Computer System(s) Identification

NOTE: All information here must match network registration information in the DevReg database.
See <http://www.olin.lnl.gov/devreg/>

Primary Computer System to be accessed:

DNS (Internet) Name _____ IP Address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

Additional system(s) to be accessed:

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

Note: The approval of the ISSO and OISSO responsible for each computer system accessed by the Visitor/Assignee is required (see signature area).

Risk Assessment

4. Network Identification

If any computer system to be accessed by the Visitor/Assignee is connected to a network(s), identify all network(s):

Yellow (LLNL.GOV) Green (LLNL.GOV) Green (UCLLNL.ORG)
 Other Network(s): _____

5. Information Access (attach additional sheets as needed)

- During the visit/employment, will any system accessed by this Visitor/Assignee contain sensitive unclassified information (SUI)? Yes No

If Yes, explain and describe the mechanisms used to protect the SUI:

- During the visit/employment, will this Visitor/Assignee require access to any SUI? Yes No

If Yes, indicate the type of SUI:

UCNI CRADA OOU Export Controlled Other (provide attachment)

If Yes, describe how the SUI is protected from disclosure to unauthorized personnel:

Note: If the Visitor/Assignee is required to have access to sensitive unclassified information, approval by an Associate Director is required for each directorate that has ownership of the information.

- Will the Visitor/Assignee require physical access to the machine room or the operator's console of servers or systems that contain SUI that the Visitor/Assignee does not have a need to access? Yes No

If Yes, describe how the SUI is protected from disclosure to unauthorized personnel:

- Will the Visitor/Assignee be granted privileged access to any hardware or software such that this person could impact the security features of any system (e.g., Root accounts, or Administrator privileges)? Yes No

If Yes, explain why this is necessary and describe the protections that mitigate the risk of unauthorized disclosure of information:

Will the Visitor/Assignee be accessing the computer system(s) from on-site at other than normal LLNL business hours? Yes No

6. Remote Access to LLNL (This section can be used in lieu of form F-2410.)

- Will the Visitor/Assignee be accessing the computer system(s) from off-site? Yes No

If Yes, please provide the following information and the Visitor/Assignee's signature.

User ID: _____
 (Official ID for UC/LLNL employees; Email address for others)

Specify remote access service(s): OTS ISDN
 Internet - normal access for collaborators: IPA VPN-C WPS-C
 Internet - requires access to "LLNL-only" content: VPN WPS)

Provide justification for remote access and requested access service(s):

Will all off-site computers used to access LLNL be U.S. Government owned? Yes No

All remote access to LLNL requires the Visitor/Assignee to read the following and sign below.
 This signature acknowledges that I agree to abide by the LLNL policies governing the use of this account including the policies and rules set forth in P-2329 - LLNL Computer Use Policy and Security Rules. I understand that failure to follow these policies can lead to administrative actions up to and including dismissal. I understand my request will be logged for auditing purposes.

 Signature Date

Required Signatures (indicates approval of this application):

LLNL Host (Sponsor) Name _____ Employee No. _____

LLNL Host Signature _____ Date _____

ISSO Name _____ Employee No. _____

ISSO Signature _____ Date _____

OISSO Name _____ Employee No. _____

OISSO Signature _____ Date _____

Associate Director Name _____ Employee No. _____

Associate Director Signature _____ Date _____

CPPM Name _____ Employee No. _____

CPPM Signature _____ Date _____

(If the Visitor/Assignee is from a sensitive country, CSO will seek CIO approval for this application.)

CIO Name _____ Employee No. _____

CIO Signature _____ Date _____

Additional Signatures (as required, based on information above):

Computation OISSO (for LC access) _____ Employee No. _____

Computation OISSO Signature _____ Date _____

Computation Associate Director (for LC access) _____ Employee No. _____

Computation Associate Director Signature _____ Date _____

ISSO¹ Name _____ Employee No. _____

ISSO¹ Signature _____ Date _____

OISSO¹ Name _____ Employee No. _____

OISSO¹ Signature _____ Date _____

(add signature sheets as required if user will require access to multiple LLNL computers)

Program Office Approval (Name & Title) _____ Employee No. _____

Program Office Approval Signature _____ Date _____

Associate Director¹ Name _____ Employee No. _____

Associate Director¹ Signature _____ Date _____

(add signature sheets as required if user will require access to multiple LLNL computers)

SAFE Program (Name & Title) _____ Employee No. _____

SAFE Program Signature _____ Date _____

¹ To be used when the ISSO, OISSO, and Associate Director are granting access to a computer/network not under the purview of the ISSO of the organization requesting access for the Visitor/Assignee.

Supplemental Data Sheet for Additional Signatures

ISSO Name _____ Employee No. _____

ISSO Signature _____ Date _____

OISSO Name _____ Employee No. _____

OISSO Signature _____ Date _____

ISSO Name _____ Employee No. _____

ISSO Signature _____ Date _____

OISSO Name _____ Employee No. _____

OISSO Signature _____ Date _____

ISSO Name _____ Employee No. _____

ISSO Signature _____ Date _____

OISSO Name _____ Employee No. _____

OISSO Signature _____ Date _____

Program Office Approval (Name & Title) _____ Employee No. _____

Program Office Approval Signature _____ Date _____

Associate Director Name _____ Employee No. _____

Associate Director's Signature _____ Date _____

Associate Director Name _____ Employee No. _____

Associate Director's Signature _____ Date _____

Supplemental Data Sheet for Multiple Computer Usage

NOTE: All information here must match network registration information in the DevReg database.
See <http://www-oln.llnl.gov/devreg/>

Additional system(s) to be accessed:

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____

DNS (Internet) Name _____ IP address _____
Computer Location _____ DOE No. _____
Manufacturer and Model _____