

**U.S. DEPARTMENT OF ENERGY- BONNEVILLE POWER ADMINISTRATION (BPA)
 SECURITY PRIVILEGE REQUEST
 BPA CONTROL CENTERS**

OMB Control Number:1910-5188
 Expiration Date:

SECTION 1. REQUESTER INFORMATION (Required)

A. Requester Name (Last, First, MI)		B. Address (BPA Mail Stop or Business Address)		C. Work Phone Number (10-Digit)	
D. BPA Supervisor or COR Name (Last, First, MI)			E. Routing (BPA Mail Stop)		F. Work Phone Number (10-Digit)
G. Employment Status Federal Employee Non-Federal (Company) Student Program Other (Explain)			H. BPA Logon ID:		I. HRMIS ID: (If Known)

SECTION 2. BUSINESS NEED DESCRIPTION (Required)

Describe specific duties which require access to Control Center resources. For physical access, indicate anticipated frequency of entry (per week/month) and if 24 hour access is needed. If requester is a student program participant, request temporary access and specify expiration date.

SECTION 3. REQUESTED PRIVILEGES

SECTION 6. RESOURCE MANAGER (RM) APPROVAL

PRIVILEGE #	Privilege Type:		Duration	Permanent *Expiration Date: Temporary*	RM Signature	
	Resource:				Date	
Domain/Privilege Name:					Internal Processing Notes (Required)	
PRIVILEGE # 1	Privilege Type:		Duration	Permanent *Expiration Date: Temporary*	RM Signature	
	Resource:				Date	
	Domain/Privilege Name:					Internal Processing Notes (Required)
PRIVILEGE # 2	Privilege Type:		Duration	Permanent *Expiration Date: Temporary*	RM Signature	
	Resource:				Date	
	Domain/Privilege Name:					Internal Processing Notes (Required)
PRIVILEGE # 3	Privilege Type:		Duration	Permanent *Expiration Date: Temporary*	RM Signature	
	Resource:				Date	
	Domain/Privilege Name:					Internal Processing Notes (Required)

SECTION 4. SIGNATURES (Required)

VALID SIGNATURES: Per OMB A-130, Digital Signature (web link to instructions) or Electronic Signature (handwritten signature scanned into electronic format) are recognized as a valid signatures. Use of "/s/" is NOT a valid signature.

A. Requester Signature*		Date
* Signature certifies information provided is correct and Requester has read and agrees to comply with NERC CIP training and Control Center Rules of Conduct.		
B. Check if "Acting"	C. BPA Supervisor or COR Signature** (Must be same as Block 1D unless "Acting" checked)	Date
** Signature certifies information provided is correct and Supervisor/COR agrees to make appropriate notifications if Requester no longer requires requested access privileges or separates.		

SECTION 5. SECURITY PRIVILEGE COORDINATOR (SPC) USE ONLY

A. Completion Checklist		
Signatures Verified	Required Account Actions Completed	Notated Requester's Security Records
B. SPC Signature (Requested Actions Taken)		Date
CC Version	CIP Training	PRA
Security Record Number		

(SECTIONS 1 - 4A) Requester Instructions:

- Two requirements must be met prior to granting access which will be validated by the Security Privilege Coordinator (SPC) before a request is processed:
 - Requesters must successfully complete annual NERC CIP training course. (Control Center version required for physical access)
 - Current Personnel Risk Assessment (PRA) must be on file.
 - Completely fill out required Sections 1 and 2. Be specific in Section 2 when describing duties to be performed. Resource Managers (RM) must be able to determine the privilege being requested based on the information provided. A "least privilege" security policy will be followed providing only the accesses or privileges needed to perform the work.
 - Use the drop down to indicate the privilege type requested in each privilege block. Up to 3 privileges can be requested per form, and a separate block is required for each privilege. It is advisable to submit requests for Physical and Cyber Access Requests using separate forms, to ensure the most expedient processing can occur.
 - Complete the remainder of Section 3 to the best of your ability and contact the Security Privilege Coordinator (SPC) for help as needed.
 - Place your digital signature in block 4A, add date if using a hard copy signature.
 - After block 4A is signed, obtain an approval signature from your BPA Supervisor or Contracting Officer Representative (COR) in block 4C.
7. Send the completed form to the appropriate SPC location:

Dittmer Control Center Security Privilege Coordinator – All Cyber and DCC Physical Access Privileges

Phone: (360) 418-2111 or x2286 (*after hours*)

E-mail: Control Center Privileges ControlCenterPrivileges@bpa.gov

M-Stop: TTOM-DITT-1

FAX: (360) 418-8417

Address: P.O. Box 491

Vancouver, WA 98666-0491

Munro Control Center Security Privilege Coordinator – MCC Physical Access Privileges

Phone: (509) 822-4500

E-mail: Munro Control Cntr Privileges MCCP@BPASite1.bpa.gov

M-Stop: TTOM-MEAD

FAX: (509) 466-3513

Address: P.O. Box 939

Mead, WA 99021-0939

(SECTION 4B) BPA Supervisor or COR Instructions:

- Verify Sections 1-3 are complete and the Requester signed block 4A.
- Ensure Requester has a business need for the requested privileges.
- Check box 4B if you are an "Acting" Supervisor.
- Place your digital signature in block 4C, add date if using a hard copy signature.

NOTE TO BPA SUPERVISOR OR COR:

Notify the appropriate office(s) for revocations and changes in assignments which may impact physical or cyber access privileges. For questions regarding current policy, contact Revoke@bpa.gov directly or call 503-230-5625 (LOCK). Information is available on the BPA Security office web page <https://connection.bud.bpa.gov/workplace-resources/security/>. Failure to comply with these policies may result in violation of NERC regulatory standards and heavy fines being levied against BPA.

(SECTION 5) SPC Instructions:

- Verify appropriate signatures appear in blocks 4A & 4C.
- Resolve any deficiencies in Section 3.
- Validate and record CIP Training & PRA dates on form.
- Forward forms to appropriate RM(s) and Implementers.
- Input fully authorized privileges into CAPA, assign Security Record # and sign finalized form.
- Send email grant confirmation to Requester, Supervisor, and PRA NERC CIP Verification mailbox.
- Save final documents in appropriate network and/or database locations, and maintain for appropriate retention record periods.

(SECTION 6) Resource Manager (RM) and Implementer Instructions:

- RM will:
 - Verify signatures appear in blocks 4A & 4C and Section 5 indicates CIP Training and PRA Dates appropriately noted by SPC staff.
 - Review each requested privilege block from Section 3 and justification in Section 2.
 - Digitally sign corresponding privilege blocks in Section 6 to certify approval.
 - Immediately return form to SPC Office for further processing and ensure time-line compliance conditions are met.
- SPC Office will:
 - Send forms approved by RM to appropriate Implementer(s).
- Implementer will:
 - Activate approved privileges, digitally sign corresponding implementation field to certify privileges have been created.
 - Immediately return form to SPC Office, to be finalized and ensure time-line compliance conditions are met.
- RM, Implementer or SPC will:
 - Send confirmation to Requester with any associated training materials, passwords or procedures as needed.

IMPORTANT NOTE: Completed forms cannot be used to change, escalate or add privileges.

Privacy Statement:

Authority: 42 U.S.C. 7101 et. seq., 5 CFR Parts 5 and 736, and Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004, permit collection of the data requested on this form.

Purpose: Trainer-Requester must complete the annual NERC CIP training course and BPA Personnel Risk Assessment must be current. BPA will use this information (a) to determine suitability of a BPA/DOE Credential; (b) to identify proof and register applicants as part of the Personal Identity Verification process; and (c) to determine the specific privilege(s) that need to be granted for physical access to the Dittmer and/or Munro Control Centers.

Routine Uses: We do not disclose your information to third parties without your consent, except to fulfill the purpose for collection or as legally required. See Privacy Act System of Records DOE-63, "Personal Identity Verification (PIV) files" for additional details. Records may be disclosed: to BPA employees and contractors as required to complete job duties.

Disclosure:

Providing this information is voluntary; however, failure to submit this information may result in denial of a BPA/DOE Credential which will then deny access to the Dittmer and Munro Control Centers that is needed to perform the work.

Paperwork Reduction Act Burden Disclosure Statement:

This data is being collected to ensure the security and safety of its employees, contractors, and facilities. The data you supply will be used by security personnel to provide employees access to specific physical sites. Public reporting burden for this collection of information is estimated to average .25 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining that data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of the Chief Information Officer, Enterprise Policy Development & Implementation Office, IM-22, Paperwork Reduction Project (OMB control number 1910-5188), U.S. Department of Energy, 1000 Independence Ave SW, Washington, DC, 20585-1290; and to the Office of Management and Budget (OMB), OIRA, Paperwork Reduction Project (OMB control number 1910-5188), Washington, DC 20503.

Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB control number.

The Paperwork Reduction Act (PRA) of 1995 requires each Federal agency to seek and obtain approval from the Office of Management and Budget (OMB) before undertaking a collection of information directed to 10 or more persons of the general public, including persons involved in or supporting the operations of Government-owned, contractor-operated facilities.

Submission of this data is required.