DOE F 1325.8e Electronic Form Approved by Forms Mgmt. 04/26/2012
(08-89)

United States Government **Department of Energy**

Bonneville Power Administration

memorandum

DATE: June 22, 2026

REPLY TO ATTN OF: CP

SUBJECT: Bonneville Purchasing Instruction (BPI) FY26-1 Interim Policy Update

TO: Lynnial Trusty – NSS

The purpose of this memorandum is to provide detailed guidance (referred to as the "Interim Policy") to the Bonneville Purchasing Instructions (BPI) regarding (1) an increase to the Competition Threshold for materials, services, and construction and an increase to the and Micro-Purchase Threshold for supplies and some services; (2) updated language in clause 15-16, Access to Bonneville Facilities and Computer Systems, to hold Contractors more accountable for NERC-CIP violations; (3) updated Safeguarding Bonneville Information guidance and clause language to align with FISMA policy; (4) updated policy guidance on Pre-Registration of Foreign Nationals in compliance with DOE Order 142.3C, Unclassified Foreign Visits and Assignments Program; (5) new guidance and clause language to address the inclusion of Classified Information in contracts; and (6) updated Privacy policy guidance and clause language to address third-party websites and public-facing applications in compliance with OMB Memo 10-23.

This memorandum, in addition, addresses administrative changes within policy. This interim policy updates prescriptions, provisions, and clauses with the changes captured within this memorandum. The conformed policy and clauses presented supersede BPI 24-1, dated April 30, 2024. Everything else remains unchanged.

Interim Policy Applicability and Effective Dates:

Applicable clauses shall be included in solicitations and contracts as follows:

- New solicitations issued on or after October 1, 2026; and
- New contracts awarded on or after October 1, 2026.
- New task or delivery orders awarded on or after October 1, 2026; and
- Option years exercised on or after October 1, 2026.

At the Contracting Officer's discretion, these clauses may also be incorporated into existing contracts on or after October 1, 2026.

Summary of Changes:

(1) The competition threshold is increased from $25,000 to $150,000 for Construction, A&E and Services and $50,000 to $150,000 for Supplies. The Competition Threshold is now the same for services and supplies. The micro-purchase threshold for supplies and services ***not*** subject to Wage Rate Requirements or Service Contract Labor Standards are increased from $50,000 to $150,000. Construction subject to Wage Rate Requirements is still statutorily limited to $2,000, and services subject to Service Contract Labor Standards are still statutorily limited to $2,500. As a result of these changes, the purchase limits in 1.8.4.2, Training and Education, 26.3(s)(4), Micro-Purchase Program, 12.8.2, Notification to Unsuccessful Offerors, and 24.5.25 Field Contract Modifications are also increased to $150,000.

(2) Clause 15-16, Access to Bonneville Facilities and Computer Systems, is updated to clarify consequences for a Contractor's failure to comply with notification requirements that may result in a NERC CIP violation reportable to WECC. The Contractor may receive a Cure Notice from the CO or be required to pay liquidated damages if BPA incurs any cost due to mitigating a violation.
(3) Policy and prescribed clause(s) in Part 15.9 are updated to reflect changes in how Bonneville complies with FISMA. Rather than defining FISMA application by High, Moderate, and Low, all solicitations and contracts will include the base Safeguarding Bonneville Information clause (formerly Information Assurance). If the contract involves CUI, an additional new clause will be required that raises the level of protection to include NIST requirements. If the contract involves CUI stored in the cloud (SaaS, PaaS, IaaS), an additional new clause will be required that further raises the requirements to include FedRAMP Moderate Authorization.
(4) Policy in Part 15.7.2, Pre-Registration of Foreign Nationals, is updated to remove the requirement to complete Bonneville form 5632.08 and add the requirements that Contractors shall notify Bonneville, prior to the execution of any project, if any Foreign Nationals will be involved, either on site or remote and that Foreign Nationals shall provide a copy of their passport, their visa (if applicable), CV or resume, and any additional documentation upon request.
(5) A new Part 15.3, Classified Information, was created along with two new clauses, Clause 15-19.1, Security Requirements for Classified Contracts, and Clause 15-19.2, Security Classification Specification. Bonneville has not previously handled Classified Information in contracts, so there is no existing procurement policy. Bonneville will have contracts in the future that may involve Classified Information, necessitating the creation of new policy and clauses.
(6) Part 5.1, Protection of Individual Privacy, and prescribed clauses have been updated to clarify definitions and to add policy requirements and a new clause, Third-Party Website Privacy, when Bonneville (or a Contractor on our behalf) hosts a third-party website or application to engage with the public. Privacy Assurance and Privacy Protection clauses are also updated to require a Contractor to notify Bonneville within 1 hour of suspicion of or discovery of a PII privacy breach.

Contracting Officers must abide by all the changes issued under this interim policy update. All applicable awards issued after the effective date of this transmittal shall comply with the requirements of this update unless otherwise directed or waived by the HCA.

KELLI BOWEN Digitally signed by KELLI BOWEN
Date: 2026.06.22 10:15:10 -07'00'

Kelli Bowen
Head of the Contracting Activity
Bonneville Power Administration

cc:
Melanie Spraggins – C
Christopher Wilk – J
Tom McDonald - F
Donna Oden-Orr – LG
Steve Capps – NS
Sarah Laylo – NN
Nicole Rutherford – JA
Candice Palen – CGI
Ryan Josephson – FTO
Stephanie Green – NSSS
Christina Craig – NSSV
Bill Cochenour - NSSP
Krista McCracken – NSSF

New, Revised, and/or Revoked Policy, Provisions, and Clauses:

Part 1.8.4.2 – Training and Education:

Policy

1.8.4.2 Training and Education
The Learning and Workforce Development Office (NHT) is authorized to make purchases up to $150,000 for training and education courses. This authority is only for purchases with commercial firms or educational institutions and shall be procured utilizing the purchase card as outlined in Part 26.

Part 2.2 – Definitions:

Policy

2.2 Definitions
Competition Threshold means purchases at or below the competition threshold of $150,000 for Construction, Services, and Supplies.

Federal Contract Information (FCI) means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Micro-Purchase Threshold means:
(a) $2,000 for construction subject to 40 U.S.C. chapter 31, subchapter IV, Wage Rate Requirements (formally known as Davis Bacon Act);
(b) $2,500 for services subject to 41 U.S.C. chapter 67, Service Contract Labor Standards (formally known as Service Contract Act);
(c) $150,000 for services not subject to (a) or (b); and
(d) $150,000 for supplies.

Part 5.1 – Protection of Individual Privacy:

Policy

This part prescribes policies and procedures that apply privacy best practices and the requirements of the Privacy Act of 1974 (5 U.S.C. § 552a) (the Act) to Government contracts. It also prescribes the procedures for complying with the Freedom of Information Act (5 U.S.C. § 552, as amended).

5.1 PROTECTION OF INDIVIDUAL PRIVACY

5.1.1 Definitions

As used in this subpart –

Improper disclosure includes loss, theft, and unauthorized release or sharing of PII.

Maintain means maintain, collect, use or disseminate.

Operation of a Privacy Act system of records means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

Personally identifiable information (PII) means any information collected or maintained by Bonneville (and Contractors on Bonneville's behalf) about any individual. This includes information that can be used to distinguish or trace an individual, either alone or when combined with other information that is linked or linkable to a specific individual.

Privacy Act System of Records means a group of any records, under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Record means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger, voice print, or a photograph.

Safeguards means protective measures, such as policies, procedures, hardware, or physical controls implemented in an information system to meet security requirements, primarily protecting the confidentiality, integrity, and availability of the system and its data.

Security breach means any act or omission that compromises the security, confidentiality, or integrity of PII, or the safeguards put in place by the contract for the protection of PII.

Sensitive PII means PII that must be protected against loss because improper disclosure could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. This includes, among other things, medical history and conditions, workplace performance and discipline history, and financial information.

5.1.2 General

(a) Federal privacy laws and OMB memoranda establish requirements when government funds are used to collect or maintain information about individuals.
(b) The Privacy Act of 1974 provides specific safeguards for individual privacy of citizens and lawfully admitted aliens when Bonneville contracts for the design, development, or operation of a system that will contain Privacy Act records on behalf of Bonneville. The Act requires that the Contractor and its employees comply with the Privacy Act when handling Bonneville Privacy Act records.
(c) A Bonneville employee may be criminally and/or civilly liable for violations of the Privacy Act. When a contract provides for operation of a Privacy Act system of records, Contractors and their employees are considered agents of Bonneville, and are subject to the criminal penalties of the Act.
(d) If a contract specifically provides for the design, development, or operation of a Privacy Act system of records on individuals on behalf of Bonneville, Bonneville must apply the requirements of the Act to the Contractor and its employees for work on the contract. The system of records operated under the contract is deemed to be maintained by Bonneville and is subject to the Act.
(e) OMB memorandum M-10-23 requires Bonneville to take additional specific steps to protect individual privacy whenever Bonneville uses a third-party website or application to engage with the public.

5.1.3 Procedures

(a) The CO shall review requirements to determine whether the contract:
    (1) May involve the Contractor receiving or accessing limited amounts of non-sensitive PII from Bonneville; and/or
    (2) Will involve the Contractor receiving or accessing any sensitive PII or significant amounts of non-sensitive PII from Bonneville; and/or
    (3) Will involve the Contractor designing, developing, or operating a system that will maintain Bonneville Privacy Act records; and/or
    (4) Will involve the operation of a third-party website or application that engages with the public for the purposes of increasing transparency or openness.
(b) If it is unclear whether the contract requirements may involve PII, the CO should seek clarification from the requisitioner and the Bonneville Privacy Officer.
(c) If the contract requires designing, developing, or operating a system that will maintain Bonneville Privacy Act records, the CO shall ensure that in the contract documents the relevant Privacy Act

System of Records identification number, as well as the design, development, or operation work to be performed are identified. The CO shall also make available Bonneville policies and procedures implementing the Privacy Act.

5.1.4 Contract Clauses

(a) The CO shall insert clause 5-1, Privacy Assurance, in all solicitations and contracts, except for commercial supplies when no exchange of PII from Bonneville occurs (see 5.1.3) or when Clause 5-2 is used.
(b) If the work of the contract requires the Contractor to receive or access sensitive PII or significant amounts of non-sensitive PII from Bonneville, the CO shall insert the clause 5-2, Privacy Protection, in the solicitation and contract.
(c) If the work of the contract requires designing, developing, or operating a system that will maintain Bonneville Privacy Act records, the CO shall insert in all solicitations and contracts, both the clause 5-2, Privacy Protection, and 5-3, Privacy Act.
(d) If the work of the contract includes developing, creating, or maintaining a website or application on behalf of Bonneville (sometimes referred to as a Third-Party Website) that will interact with the public then the CO shall insert both the clause 5-2, Privacy Protection, and 5-4, Third-Party Website Privacy.

Clauses

35.2.20 Clause 5-1 Privacy Assurance

As prescribed in 5.1.4, insert the following clause in solicitations and contracts:

PRIVACY ASSURANCE (OCT 2026)

The Contractor acknowledges and agrees that, in the course of its contract with Bonneville, Contractor may receive or access personally identifiable information (PII) belonging to Bonneville. Contractor represents and warrants that its collection, access, use, storage, disposal, and disclosure of PII will comply with all applicable privacy laws and regulations, including the Privacy Act (5 U.S.C. § 552a), the E-Government Act (44 U.S.C. § 101), and DOE regulations (10 CFR § 1008, et seq.). Contractor is responsible for the actions and omissions of its employees for the handling of PII. The Contractor agrees not to share PII with any entity not explicitly authorized by the contract. The Contractor agrees to report any security breach of PII within 1 hour of suspicion or discovery of the breach. The Contractor shall seek express consent from Bonneville before storing any PII on data servers, including redundant servers, which reside outside of the United States.

(End of clause)

35.2.21 Clause 5-2 Privacy Protection

As prescribed in 5.1.4, insert the following clause into solicitations and contracts:

PRIVACY PROTECTION (OCT 2026)

The Contractor acknowledges and agrees that, in the course of its contract with Bonneville, Contractor will receive or access personally identifiable information (PII) belonging to Bonneville. Contractor represents and warrants that its collection, access, use, storage, disposal, and disclosure of PII will comply with all applicable privacy laws and regulations, including the Privacy Act (5 U.S.C. § 552a), the E-Government Act (44 U.S.C. § 101), and DOE regulations (10 CFR § 1008, et seq.). Contractor is responsible for the actions and omissions of its employees for the handling of PII. The Contractor agrees to:

(a) Maintain all PII in strict confidence, using such degree of care as is appropriate to avoid improper access, use, or disclosure;
(b) Limit access to PII to Contractor employees who need the information to complete a job function;
(c) Have a documented process for training Contractor employees on PII security and privacy;
(d) Have a documented process for reporting and handling PII security breaches;

(e) Report any PII security breach to Bonneville within 1 hour of suspicion or discovery of the breach;
(f) Use and disclose PII exclusively for the purposes for which the PII, or access to it, is provided, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available PII for the Contractor's own purposes or for the benefit of anyone other than Bonneville without prior written consent;
(g) As permitted under current Federal law, allow access to data to authorized Federal agencies, and to individuals wishing to verify their own PII;
(h) Agree that the Federal Government retains ownership of the data at all times;
(i) Seek express written consent from Bonneville before storing any PII on data servers, including redundant servers, which physically reside outside of the United States;
(j) Implement administrative, physical, and technical safeguards to protect PII that are no less rigorous than accepted industry and government practices (NIST 800-53 rev4 and Moderate FIPS-199), and ensure that all such safeguards comply with applicable Federal data protection and privacy laws, as well as the terms and conditions of this agreement;
(k) Participate in the BPA Privacy Office process to document analysis of how information is handled through a Privacy Threshold Assessment (PTA) and/or a Privacy Impact Assessment (PIA).
(l) Maintain a documented process to address the removal of PII upon termination of the contract; and
(m) Upon completion or termination of the contract, promptly return to Bonneville a copy of all Bonneville data in its possession, securely destroy all other copies, and certify in writing to Bonneville that all Bonneville PII has been returned to Bonneville or securely destroyed.

(End of clause)

35.2.22 Clause 5-3 Privacy Act

As prescribed in 5.1.4, insert the following clause in solicitations and contracts:

PRIVACY ACT (OCT 2026)

(a) The Contractor shall be required to design, develop, or operate a Privacy Act System of Records subject to the Privacy Act of 1974 (5 U.S.C. § 552a) and applicable DOE regulations.
(b) The Contractor agrees to:
  (1) Comply with the Privacy Act and the DOE rules and regulations issued under the Act in the design, development, or operation of any Privacy Act system of records.
  (2) Include this clause in all subcontracts awarded under this contract which require the design, development, or operation of such a system of records.
(c) In the event of a violation of the Act, a civil action may be brought against Bonneville if the violation involves the design, development, or operation of a system of records on individuals. Employees of Bonneville may be subject to criminal penalties for violation of the Privacy Act. Under the Act, when a contract is for the operation of a Privacy Act system of records, the Contractor and its employees are considered employees of Bonneville.

(End of clause)

35.2.23 Clause 5-4 Third-Party Website Privacy

As prescribed in 5.1.4, insert the following clause in solicitations and contracts:

THIRD-PARTY WEBSITE OR APPLICATION PRIVACY (OCT 2026)

(a) The Contractor shall post a notice on the Third-Party website or application itself that is clearly labeled and prominently displayed at all locations where the public might make PII available to the agency.
(b) The notice shall include:
  (1) An explanation that it is a Third-Party website or application on behalf of Bonneville;
  (2) A description of how Bonneville will maintain, use, or share the PII that the site or application collects; and

(3) An explanation that, by using the Third-Party website or application, the public may be providing PII to Bonneville and a nongovernment third party.
(c) The Contractor shall provide a link to Bonneville's website and Bonneville's Privacy Policy.
(d) The Contractor shall include Bonneville branding to facilitate the recognition by the public that the website is associated with Bonneville.

(End of clause)

Part 12.8.2 – Notification to Unsuccessful Offerors:

Policy

(a) Unsuccessful offerors shall be notified as soon as reasonably possible that their offer is no longer being considered. The notification may be made orally and shall include a general explanation of the reasons for elimination.
(b) For contracts over $150,000, unsuccessful offerors shall also be notified at the time of award of the name of the successful offeror, total contract price, date of award.
(c) This policy does not apply to transactions where notifications to unsuccessful offerors are not a common business practice. However, the CO shall consider the benefits of full and open communication with all of Bonneville's suppliers when making the decision regarding notification.

Part 15.7.2 – Pre-Registration of Foreign Nationals:

Policy

(a) In compliance with DOE Order 142.3C, Unclassified Foreign Visits and Assignments Program, a contract employee who is a non-US citizen (foreign national) must be preregistered and approved prior to visits or assignments at Bonneville facilities. The Foreign National must be registered and approved for any work, physical or remote, for the Bonneville Power Administration (Bonneville).
(b) Bonneville cannot permit any Foreign National ─ whether onsite or remote to access facilities, participate in business conversations (including telephone or email), or provide business support until approval has been granted. Accordingly, all Contractors shall notify Bonneville prior to the execution of any project if any Foreign Nationals will be involved, either on site or remote. Depending on the individual's country of citizenship, the approval may take up to 12 months or may ultimately be denied.
(c) Foreign Nationals shall provide a copy of their passport, their visa (if applicable), CV or resume, and any additional documentation upon request.

Part 15.8 – Access to NERC CIP Sites and Computer Systems

Clause

35.2.181 Clause 15-16 Access to Bonneville Facilities and Computer Systems

As prescribed in 15.8.3, insert the following clause in solicitations and contracts:

ACCESS TO BONNEVILLE FACILITIES AND COMPUTER SYSTEMS (OCT 2026)

(a) Contract workers with unescorted physical access to a Bonneville facility and/or computer system shall comply with applicable procedures and requirements, as follows:
(1) Bonneville Policy 434-1: Cyber Security Program;
(2) Bonneville Policy 430-2: Managing Access and Access Revocation for NERC CIP Compliance;
(3) Bonneville Policy 433-1: Information Security;
(4) Bonneville Control Center document, Dittmer Control Center Access – Frequently Asked Questions;

(5) Bonneville Substation Operations Rules of Conduct Handbook: Policies and Procedures, Permits, Energized Access, and Clearance Certifications (if unescorted access will include energized facilities); and
(6) Any additional requirements and procedures that may be included in the statement of work and the technical specifications.

(b) The Contractor shall notify Bonneville within four (4) hours of the determination that a worker with unescorted physical access to a Bonneville facility or computer system no longer requires access or is no longer employed by the Contractor.
At a minimum, the Contractor shall:
(1) Send notification to Bonneville Security Services by email to Revoke@bpa.gov or call (503) 230-3779 to provide notification;
(2) Provide written notification to the Contracting Officer and, if assigned, the Contracting Officer's Representative to confirm that notification required in the above subsection (1) occurred; and
(3) Surrender to Bonneville the physical badge and computer access assets within 24 hours.

(c) The provisions of this clause shall be included in all subcontracts where workers have unescorted access to Bonneville facilities or computer system access.

(d) Failure to comply with the requirements in this Clause 15-16 may result in a Cure Notice from the Contracting Officer, providing the Contractor with an opportunity to document why this procedure was not followed and what they will do to remedy the violation.

(e) If the Contractor has failed to comply with the stated requirements of paragraph (b) above, and the Contracting Officer determines the Contractor failed to make a good faith effort to comply with the requirements therein, the Contractor may be required to pay liquidated damages in the amount stated below:
(1) If the Contractor's failure to comply results in a reportable violation as confirmed by the Western Electricity Coordinating Council (WECC), and Bonneville is required to complete a Mitigation Plan, the Contractor shall, in place of actual damages, pay the lesser of 1% of the contract value or *[CO fill in amount]*, the amount assessed based on attributable costs incurred by Bonneville to meet WECC requirements.
(2) The Contractor will not be charged liquidated damages when the delay in notifying Bonneville of Contractor Personnel Changes is beyond the control and without the fault or negligence of the Contractor as defined in the Termination for Default clause in this contract.
(3) These liquidated damages may be in addition to any other remedies that the Government may have.

(End of clause)

Part 15.9 – Safeguarding Bonneville Information:

Policy

15.9 Safeguarding Bonneville Information

This subpart prescribes the policies and procedures for the protection of Bonneville's information and information systems. These systems are subject to the requirements of the E-Government Act (Public Law 107-347) of 2002, Title III Federal Information Security Management/Modernization Act (FISMA), as amended, and other relevant federal regulations concerning safeguarding Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

As used in this part, Federal Contract Information (FCI) is defined as information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

15.9.1 General

(a) FISMA establishes security controls to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure the integrity, confidentiality, and availability of information and information systems.
(b) Bonneville Power Administration is a federal agency and a balancing authority for the western United States electrical transmission grid. Due to this critical role, Bonneville's cybersecurity requirements may exceed those of other Federal agencies, depending on the product or services being procured and their intended use.
(c) The safeguarding of Bonneville information is critical to its mission and operations, encompassing FCI and various categories of Controlled Unclassified Information (CUI), as defined in Bonneville Policy 433-1.

15.9.2 Policy

(a) The level of risk and required care for Bonneville information shall be assessed by Bonneville's Chief Information Security Officer (CISO) and determined by Bonneville's Chief Information Officer (CIO). Any additional requirements shall be incorporated into the contract Statement of Work or specification document.
(b) This policy applies to all solicitations and contracts for supplies, services, materials, equipment, construction, and intergovernmental contracts.
(c) Bonneville, as a Federal agency, will contract in compliance with the requirements of FISMA and other applicable federal regulations.
(d) Bonneville requires that a Contractor's internal information systems that store Bonneville's FCI shall comply with Bonneville's minimum security controls. Contractor's internal information systems that store Bonneville's CUI shall be protected as set forth by the National Institute of Standards and Technology (NIST) for non-federal systems. If the Contractor stores Bonneville CUI in a cloud solution, the cloud solution must be FedRAMP authorized at the Moderate level or higher. Any variations or deviations from these policies and standards shall be approved by the CIO or the HCA, as appropriate.

15.9.3 Procedure

(a) The Information Owner and requisitioner are responsible for informing the CO of the level of care required as determined by the CIO, i.e., whether FCI or CUI will be involved as part of the procurement.
(b) The Information Owner and requisitioner are responsible for ensuring the Statement of Work, requirements document, or specifications include additional requirements based on whether FCI or CUI will be involved.
(c) The Office of Cyber Security shall provide assistance if the Information Owner, requisitioner, or CO is unsure if additional safeguarding requirements apply.

15.9.4 Contract Clause

(a) The CO shall include the clause 15-17.1, Safeguarding Bonneville Information, in all solicitations and contracts.
(b) The CO shall include the clause 15-17.2, Safeguarding Bonneville Controlled Unclassified Information (CUI), in all solicitations and contracts that include CUI data provided by or generated for Bonneville.

Clauses

35.2.182.1 Clause 15-17.1 Safeguarding Bonneville Information

As prescribed in 15.9.4, insert the following clause in all solicitations and contracts:

SAFEGUARDING BONNEVILLE INFORMATION (OCT 2026)

(a) This procurement involves or contains Federal Contract Information (FCI) that shall be protected pursuant to minimum security controls as defined below.
(b) Federal Contract Information (FCI) is defined as information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government

to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

(c) Bonneville's FCI must be protected in accordance with the following minimum security controls:
    (1) Ensure only approved personnel or systems can access the information system. Limit information system access to authorized users, processes, or devices.
    (2) Implement the principle of "least privilege," restricting authorized users to only the necessary functions for their roles. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
    (3) Verify and control/limit connections to and use of external information systems, including managing and restricting access to systems outside the Contractor's direct control.
    (4) Control information posted or processed on publicly accessible information systems to prevent sensitive contract information from being exposed on public platforms like websites or social media.
    (5) Identify information system users, processes acting on behalf of users, or devices. Establish unique identifiers for all users and system components.
    (6) Authenticate (or verify) the identities of those users, processes, or devices before allowing access, including but not limited to using passwords, multi-factor authentication, or biometrics.
    (7) Sanitize or destroy information system media containing FCI before disposal, release, or reuse.
    (8) Restrict who can physically interact with the systems. Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
    (9) Ensure accountability and oversight for physical access. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
    (10) Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of information systems.
    (11) Implement sub-networks for publicly accessible system components that are physically or logically separated from internal networks.
    (12) Address vulnerabilities and ensure prompt remediation. Identify, report, and correct information and information system flaws in a reasonable and timely manner.
    (13) Provide protection from malicious code at appropriate locations within organizational information systems, including but not limited to antivirus software and malware scanners.
    (14) Ensure defenses are current against evolving threats. Update malicious code protection mechanisms immediately when new releases are available.
    (15) Proactively identify and neutralize potential risks. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(d) Dispose of all Bonneville information post contract. All Bonneville information will be removed and destroyed from all vendor corporate systems as well as from all physical storage immediately following the end of the contract and subsequent warranty period, as applicable.

(e) Subcontract flow-down: Contractors are required to include this clause in subcontracts where Bonneville FCI may reside in or transit through a subcontractor's information system.

(End of clause)

35.2.182.2 Clause 15-17.2 Safeguarding Bonneville Controlled Unclassified Information (CUI)

As prescribed in 15.9.4, insert the following clause in all solicitations and contracts that include CUI data provided by or generated for Bonneville.

SAFEGUARDING BONNEVILLE CONTROLLED UNCLASSIFIED INFORMATION (CUI) (OCT 2026)

(a) Bonneville Power Administration (Bonneville) is providing the Contractor with, or the Contractor is generating on Bonneville's behalf, Controlled Unclassified Information (CUI) that shall be

protected in accordance with the security controls outlined in NIST SP 800-171 (the version effective at the time of award).

(b) If the Contractor stores Bonneville CUI in a cloud solution, the cloud solution must be FedRAMP authorized at the Moderate level or higher.

(c) Dispose of all Bonneville information post contract. All Bonneville information will be removed and destroyed from all vendor corporate systems as well as from all physical storage immediately following the end of the contract and subsequent warranty period, as applicable.

(d) Subcontract flow-down: Contractors are required to include this clause in subcontracts where Bonneville CUI may reside in or transit through a subcontractor's information system.

(End of clause)

Part 15.13 – Classified Information:

Policy

15.13.1 Policy

(a) It is Bonneville's policy to ensure that all contracts involving access to, generation, processing, storage, or transmission of classified information strictly adhere to national security regulations and standards. This policy is critical given Bonneville's role in national energy infrastructure and any contracts with the Department of Energy (DOE) that require handling classified information.

(b) The National Industrial Security Program (NISP), as codified in 32 CFR Part 117, and any successor regulations, establishes the mandatory requirements for safeguarding classified information in industry. Compliance with these requirements is paramount, regardless of contract value or type.

(c) Requisitioners shall work closely with the Bonneville Chief Security Officer, a.k.a. Bonneville's Officially Designated Federal Security Authority (ODFSA), and COs to identify contracts or procurements that involve classified information. The requisitioner shall ensure that all Contractors and their personnel meet the necessary security clearances and facility clearance requirements.

15.13.2 Procedure

(a) Identification of Classified Requirements: The requisitioner, in consultation with the Bonneville Chief Security Officer, shall clearly identify if a contract will involve classified information. This identification must specify the classification level(s) and the nature of Contractor involvement (e.g., access, generation, storage, transmission).

(b) Security Classification Specification (SCS): For all contracts identified under 15.13.2(a), a Security Classification Specification (or equivalent document) must be prepared by the requisitioner with input from the Bonneville Chief Security Officer. This document shall detail the specific security requirements for the contract, including facility clearance level, personnel clearance levels, safeguarding procedures, and reporting requirements. The SCS shall be incorporated into the contract as an Attachment.

(c) Contractor Responsibilities: The CO shall ensure that prospective Offerors and Contractors are aware of their obligations regarding classified information handling, including the requirements to obtain a valid Facility Clearance (FCL) at the appropriate level within 180 days of award, maintain the FCL in accordance with 32 CFR Part 117, and ensure all personnel have the necessary security clearances and a need-to-know.

(d) Reporting: The CO shall ensure that all security incidents or violations related to classified information are reported immediately to the Bonneville Chief Security Officer and subsequently to the relevant government authorities as required by 32 CFR Part 117.

(e) NISP Waivers: Any waivers or deviations from the NISP requirements or this policy must be reviewed by the Bonneville Chief Security Officer and approved by the Head of the Contracting Activity (HCA) in consultation with the Office of General Counsel (OGC).

15.13.3 Contract Clauses

(a) The CO shall include the Clause 15-19.1, Security Requirements for Classified Contracts, in all solicitations and contracts requiring contractor personnel to have access to classified information or requiring the generation, processing, storage, or transmission of classified information.

(b) The CO shall include the Clause 15-19.2, Security Classification Specification, in all solicitations and contracts requiring contractor personnel to have access to classified information or requiring the generation, processing, storage, or transmission of classified information. The CO shall incorporate the completed Security Classification Specification into the contract as an attachment and reference it in Clause 15-19.2, Security Classification Specification.

Clauses

35.2.184 Clause 15-19.1 Security Requirements for Classified Contracts

As prescribed in 15.13.3(a) insert in all solicitations and contracts:

SECURITY REQUIREMENTS FOR CLASSIFIED CONTRACTS (OCT 2026)

(a) Applicability. This clause applies to contracts requiring contractor personnel to have access to classified information or requiring the generation, processing, storage, or transmission of classified information.
(b) Regulatory Compliance. The Contractor shall comply with all applicable requirements of the National Industrial Security Program (NISP) as set forth in 32 CFR Part 117, and any successor regulations. Compliance with these requirements is mandatory regardless of contract value or type.
(c) Facility Clearance. The Contractor shall obtain a valid Facility Clearance (FCL) at the appropriate level required by this contract within 180 days of award and maintain the FCL in accordance with 32 CFR Part 117. The FCL shall be granted by the Department of Energy or another Cognizant Security Agency. The Contractor shall immediately notify the Contracting Officer and Bonneville Chief Security Officer if the FCL is suspended, revoked, or otherwise becomes invalid.
(d) Personnel Security Clearances. The Contractor shall ensure that all personnel requiring access to classified information possess appropriate personnel security clearances at the required level and have a need-to-know. The Contractor shall verify clearances through the appropriate Government security channels prior to granting access.
(e) Security Classification Specification (SCS). The specific security requirements for this contract are detailed in the Security Classification Specification (or equivalent document) incorporated into this contract. The Contractor shall implement all security measures identified in the SCS, including but not limited to, compliance with the following:
    (1) Proper classification levels for information generated or processed;
    (2) Approved storage requirements for classified material;
    (3) Transmission and transportation procedures;
    (4) Visitor access controls;
    (5) Security incident reporting procedures; and
    (6) Subcontractor security requirements.
(f) Safeguarding Classified Information. The Contractor shall safeguard classified information in accordance with 32 CFR Part 117 and any additional security requirements specified by the Contracting Officer or Bonneville Security Officer. Classified information shall be protected at the level of its classification and shall not be disclosed to unauthorized persons.
(g) Security Incidents and Violations. The Contractor shall report any security incidents, violations, or compromises of classified information to the Bonneville Security Officer and Contracting Officer immediately upon discovery, but no later than one (1) business day after discovery. The Contractor shall conduct preliminary inquiries as required by 32 CFR 117.8(D) and cooperate fully with any Government investigation.
(h) Subcontracts. The Contractor shall flow down this clause, including this paragraph (h), to all subcontracts that involve access to classified information or require a facility clearance. The Contractor shall ensure that subcontractors meet all applicable security requirements before granting access to classified information.
(i) Security Reviews and Inspections. The Contractor shall permit the Bonneville Security Officer, DCSA, or other authorized Government representatives to conduct security reviews, inspections, and assessments of the Contractor's facility and security practices at any reasonable time.
(j) Termination of Access. Upon completion, termination, or cancellation of this contract, the Contractor shall return all classified materials to Bonneville or dispose of them in accordance with written

instructions provided by the Bonneville Security Officer. The Contractor shall certify in writing that all classified materials have been properly returned or destroyed.

(k) Points of Contact.
  (1) Bonneville Chief Security Officer: securityservices@bpa.gov ; 503-230-5295
  (2) Bonneville Contracting Officer: See Signature Page

(End of clause)

35.2.185 Clause 15-19.2 Security Classification Specification

As prescribed in 15.13.3(b) insert in all solicitations and contracts:

SECURITY CLASSIFICATION SPECIFICATION (OCT 2026)

(a) A formal, completed Security Classification Specification shall be incorporated into the contract as an attachment. The specification shall identify:
  (1) Contract security classification level;
  (2) Classified information to be provided to the Contractor;
  (3) Classification guidance for information generated under the contract;
  (4) Special security requirements, if any;
  (5) Visitor authorization procedures; and
  (6) Subcontracting security requirements.

(End of clause)

Part 24.5.25 – Field Modifications

Policy

24.5.25 Field Modifications

The CO may include the Clause 24-25, Field Modifications, in solicitations and contracts for construction only when delegated individuals have completed established COR Field Modification Training.

(a) A field modification is a formal, limited-scope contract change issued at the jobsite (or field level) under delegated authority from the CO, allowing authorized personnel (such as a COR or designated field representative) to direct minor changes to contract work without issuing a full CO modification in real time.

(b) The CO shall provide Field Modification forms, appropriately tailored to the contract, to the delegated individuals to utilize. This procedure applies to individual changes up to a maximum of $10,000 and aggregate changes up to a maximum of 5% of the original contract award or $150,000, whichever is lower.

(c) Prior to authorizing a field modification, the COR shall confirm that sufficient funds are available to support any priced changes. Any individual priced changes above $10,000 or aggregate changes exceeding 5% of original contract award, up to a maximum aggregate amount of $150,000, shall be submitted to the CO for a contract modification. No additional field modifications may be issued under this authority until all previously issued field modifications have been formally incorporated into the contract by the CO.

(d) All executed field modifications shall be provided to the CO within 10 business days of issuance. Failure to timely submit executed field modifications may result in unilateral revocation of field modification authority by the CO.

Clause

35.2.307 Clause 24-25 Field Modifications

As prescribed in 24.5.25, the CO may insert the following clause in solicitations and contracts:

FIELD MODIFICATIONS (OCT 2026)

(a) A field modification is a formal, limited-scope contract change issued at the jobsite (or field level) under delegated authority from the Contracting Officer (CO), allowing authorized personnel (such as a COR or designated field representative) to direct minor changes to contract work without issuing a full CO modification in real time.
(b) Field modifications shall apply only to individual changes up to a maximum of $10,000 and aggregate changes up to a maximum of 5% of the original contract award or $150,000, whichever is lower. Any individual priced changes above $10,000 or aggregate changes exceeding 5% of original contract award, up to a maximum aggregate amount of $150,000, shall be submitted to the CO for a contract modification.
(c) Prior to authorizing a field modification, the COR shall confirm that sufficient funds are available to support any priced changes.
(d) If either party desires a qualifying modification as defined in paragraph (a), a field modification form shall be executed by both parties, which shall constitute a full, complete, and final settlement for the agreed upon change.
(e) The Contractor shall identify an authorized representative to execute a field modification form on behalf of the Contractor. This person shall be on the job site at all times during contract performance.
(f) All field modifications must be submitted to the CO within ten (10) days of its execution for final incorporation into the contract.
(g) No additional field modifications may be issued under this authority if any previous field modifications are still pending incorporation into the contract by the CO.

(End of clause)

Part 26.2 – Definitions:

Policy

26.2 Definitions

Competition Threshold means purchases at or below the competition threshold of $150,000 for Construction, Services, and Supplies.

Federal Contract Information (FCI) means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Micro-Purchase Threshold means:

(a) $2,000 for Construction subject to 40 U.S.C. chapter 31, subchapter IV, Wage Rate Requirements (formally known as Davis Bacon); and
(b) $2,500 for Services subject to 41 U.S.C. chapter 67, Service Contract Labor Standards (formally known as Service Contract Act); and
(c) $150,000 for Supplies.
(d) $150,000 for services not subject to (a) or (b).

Part 26.3 – Micro-Purchase Program Policy:

Policy

26.3 Policy
[…]
(s)(4) The P-Card shall be used by Learning and Workforce Development Office (HT) personnel to pay for government, non-government and/or off-the-shelf training and education up to $150,000 for an individual or planned series of the same training event, activity, or course material.

Part 29.5 – Use of Federal Supply Schedules:

Policy

29.5.1 Contract Clauses

COs are to use the following clauses in orders or BPAs against Federal Supply Schedules, when applicable.
[…]
(d) COs shall include the Safeguarding Bonneville Information clauses 15-17.1 and 15-17.2, in all solicitations, orders, and BPAs where the conditions of subsection 15.9.4 exist.

Administrative Changes:

Part 15.10 – Homeland Security:

Replacing Foreign Nation with Foreign Country to align with industry terminology.

Policy

15.10.1 Definitions

Sensitive Foreign Country. A country in which particular attention is given during the review and approval process for foreign visits and assignments. Countries may be designated as sensitive for reasons of national security, nuclear nonproliferation, regional instability, threat to national economic security, or terrorism support. Department of Energy Sensitive Countries are listed in: Appendix 15, Attachment 15-2, Export Control and Home Security Links. A Foreign National is considered to be from a Sensitive Foreign Country if he/she is a citizen residing in a country or is employed by the government of an institution, or a corporation of a country on the Sensitive Foreign Country list.

Clause

35.2.183 Clause 15-18 Homeland Security

As prescribed in 15.10.3, insert the following clause in solicitations and contracts:

HOMELAND SECURITY (OCT 2026)

(a) No portion of the contractor's services, equipment, hardware, software, maintenance, or support shall be performed in a country designated as a State Sponsor of Terrorism or by nationals of a country designated as a State Sponsor of Terrorism by the U.S. Department of State. Additionally, no portion of the contractor's services, equipment, hardware, software, maintenance, or support shall be subcontracted for performance in a country designated as a State Sponsor of Terrorism or by nationals of a country designated as a State Sponsor of Terrorism by the U.S. Department of State.
(b) No portion of the Contractor's services, software, maintenance, or support shall be performed in a Sensitive Foreign Country or by Sensitive Foreign Country National. Additionally, no portion of the Contractors services, software, maintenance, or support shall be subcontracted for performance in a Sensitive Foreign Country or by Sensitive Foreign Country Nationals.
(c) If any portion of the contractor's services, software, maintenance, or support is located in a foreign country, then the contractor shall disclose those foreign Countries to the CO in writing before contract performance. Bonneville will then determine if the foreign country is a Sensitive Foreign Country or a country designated as a State Sponsor of Terrorism by the U.S. Department of State.
(d) If any portion of the contractor's services, software maintenance or support is located in a foreign country, Bonneville shall notify the contractor in writing whether or not it can allow an intangible export of Bonneville's data, critical energy infrastructure information or critical information and if a deemed export license, export end user agreement or other export documentation is required.
(e) The contractor shall notify the CO, in advance, of any consultation with a Foreign National that would expose to such parties, Bonneville data, critical energy infrastructure information, critical information, or controlled unclassified information. The notice shall be in writing. Bonneville will approve or reject the consultation with the Foreign National.

(End of clause)

Part 15.12 – Restriction on Foreign Entity and Service Location:

Replacing Foreign Nation with Foreign Country to align with industry terminology.

Policy

15.12 Restriction on Foreign Entity and Service Location

Performance, including research, design, development, maintenance and support, under Bonneville's information technology, operational technology or intellectual property contracts may not be located in countries identified on the Sensitive Foreign Country list, as described in 15.10.1, or a country designated by the U.S. Secretary of State as a state sponsor of terrorism.

15.12.1 Policy

Bonneville will not contract, for IT, OT, or other research, design, development, support or maintenance services, with entities located within countries identified on the Sensitive Foreign Country list, or a country designated by the U.S. Secretary of State as a state sponsor of terrorism. Additionally, the location of contract performance for such services shall not be within any country identified on the Sensitive Foreign Country list, or a country designated by the U.S. Secretary of State as a state sponsor of terrorism.

Part 15.3 – Contractor Compliance with Bonneville Policies

Citation to Smoke-Free Workplace Policy is updated

Clause

35.2.169 Clause 15-4 Contractor Compliance with Bonneville Policies

As prescribed in 15.3.1.1, insert the following clause in solicitations and contracts:

CONTRACTOR COMPLIANCE WITH BONNEVILLE POLICIES (OCT 2026)

(a) The contractor shall comply with all Bonneville policies affecting the Bonneville workplace environment. Examples of specific policies are:

(1) Bonneville Smoke-Free Workplace Policy (Bonneville Policy 440-86) […]

(END OF CHANGES)