

11.0 SOLICITATION POLICIES

11.6 Protecting Agency Controlled Unclassified and Classified Information.

- (a) It is Bonneville policy to protect agency Controlled Unclassified Information (CUI). CUI, as defined in Bonneville Policy 433-1, must be safeguarded against loss, misuse, compromise, unauthorized access, or modification, by the originating organization and any other Bonneville organization that has a business need to distribute the information. COs, in co-ordination with the requisitioning organization, shall obtain written assurance from prospective offerors that any CUI provided to the offeror during the market research phase, solicitation of offers, or subsequent contract performance, will be safeguarded.
- (b) Contractors who must have access to CUI in order to effectively respond to Bonneville market research, a solicitation, or during contract performance, may be asked to affirm in writing that they will comply with Bonneville policy and procedures to safeguard CUI. Such affirmation may be obtained through a non-disclosure agreement (NDA). NDAs shall be in accordance with either the requisitioners' or Supply Chain Services' organizational Operations Security Plans. Unless information is specifically unmarked as CUI at a later date, the requirements for protection and non-disclosure obligation should be deemed permanent.
- (c) If an NDA disclosing Bonneville's CUI is required and has not already been signed by prospective offerors during the market research phase, the CO shall contact OGC for guidance prior to sending an NDA to prospective offerors. An NDA may be executed prior to issuing a solicitation or executing a contract, as appropriate. The specific nature of the information and any program specific instructions shall be identified in the NDA. OGC shall approve the NDA prior to execution.
- (d) The CO's warranted authority does not include the authority to sign an NDA where Bonneville's CI is being provided to the contractor. NDAs protecting Bonneville's CUI are filed and maintained by the respective Program Office. See BPI 17.6.2 for procedures regarding Bonneville's protection of contractor information.
- (e) COs shall coordinate with the requisitioning organization and OGC to provide disposition instructions to the successful contractor throughout the market research, solicitation, and contract performance, and post contract completion. Disposition instructions after contract completion shall be commensurate with the originating office's determination of the continuing sensitive or critical nature of the information.
- (f) In the event an NDA is agreed between Bonneville and any solicitation recipient or contractor, the requirements in sections 15.10 Homeland Security, 15.11 Export Control, and 15.12 Entity and Service Location Control shall continue to be followed. NDAs provide additional data and information security only and do not replace or supersede the requirements under sections 15.10 Homeland Security, 15.11 Export Control, and 15.12 Entity and Service Location Control.
- (g) CO's or the requisitioner, or the originator of the NDA shall ensure the NDA complies with BPI data and information security requirements and Bonneville Policy 430-3.

- (h) In the event of a Contractor breach of the NDA, the Contractor shall contact the CO, per the NDA. The CO shall immediately notify the Bonneville Security and IT organizations to identify and initiate prompt remedial action.

15 Environment, Safety, and Security

15.10 Homeland Security

15.10.1 Definitions

As used in this subpart –

Bulk Electric System Cyber System Information (BES CSI/BCSI): A category of BPA’s CUI that requires security controls. BES CSI/BCSI is identified by these characteristics:

- (a) Information about Bulk Electric System (BES) Cyber Systems that could be used to gain unauthorized access or pose a security threat to BES Cyber Systems.
- (b) BES CSI/BCSI may include, but is not limited to security procedures or security information related to safeguarding BES CSI/BCSI, Physical Access Control Systems, Electronic Access Control or Monitoring Systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution, collections of network addresses, and network topology of BES Cyber Systems. (NERC Glossary of Terms used in NERC Reliability Standards –Updated 8/12/2019).
- (c) BES CSI/BCSI within BPA is marked as Critical Energy Infrastructure Information (CEII).

Critical Energy Infrastructure Information (CEII): Information related to critical energy infrastructure or proposed critical energy infrastructure, generated by or provided to the Federal Energy Regulatory Commission (Commission) or other Federal agency other than classified national security information, that is designated as critical energy infrastructure information by the Commission or the Secretary of the Department of Energy pursuant to section 215A (d) of the Federal Power Act. CEII was formerly known within BPA as Critical Cyber Asset Information (CCAI), and continues to be known as Bulk Electric System Cyber System Information (BES CSI/BCSI) which is a NERC CIP term. CEII is associated with specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

- (a) BPA identifies CEII as Federal Information Processing Standards (FIPS) High Category rating as applying to each BES Cyber System used by or located at BPA’s Control Centers, and which perform functions pertaining to reliability, balancing, transmission, or generation authorities or operators, or:
- (b) BPA identifies CEII as FIPS Moderate Category rating applying to BES Cyber Systems not included in High Impact installations, but associated with transmission facilities operating at more than 200kV per line, and which are connected to generation, transmission, or reactive facilities, the failure of which, within fifteen minutes of scheduled operation, could adversely affect the reliable operation of the Bulk Electric System.
- (c) Relates details about the production, generation, transmission, or distribution of energy;
- (d) Could be useful to a person planning an attack on critical infrastructure;
- (e) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
- (f) Does not simply give the general location of the critical infrastructure.

Critical Information (CI): Any information which must be safeguarded from loss, misuse, compromise, unauthorized, access, or modification, because such actions may adversely affect the business, security or other interests of the government, or the privacy of individuals; or which may otherwise be used by Bonneville's competitors or adversaries (including, but not limited to, other utilities, contractors, foreign interests, or disgruntled employees) to harm or embarrass Bonneville, or to gain an unfair advantage. Examples of Critical Information include confidential legal strategies, employee personnel files, contract negotiations, pricing and business strategies, active investigations, critical infrastructure addresses, e-mail addresses, physical and personal system entry codes, badges, equipment (model numbers, name, quantity, software (vendor, product name), passwords, or Data. Critical Information can exist in the form of printed documents, electronically stored information, telecommunications traffic, or the spoken word.

Controlled Unclassified Information (CUI): Information the government creates or possesses, or that an entity creates or possesses on behalf of the government or provides to the government, that Law, Regulation, or Government-wide Policy (LRGWP) requires or permits an agency to handle using safeguarding or dissemination controls. Unauthorized disclosure of CUI has the potential to damage governmental, commercial or private interests. CUI categories approved by National Archives and Records Administration (NARA), the CUI Executive Agent (EA), published in the CUI Registry, and authorized for DOE use, are the exclusive designations for identifying CUI within DOE. No other safeguarding and dissemination controls can be implemented for any Controlled Unclassified Information other than those permitted by the applicable LRGWP and as indicated in the CUI Registry. The CUI Registry can be found at <https://www.archives.gov/cui>.

Cyber Security: The physical, technical, and administrative controls and risk management processes for providing the required and appropriate level of confidentiality, integrity, availability and accountability for Department of Energy information stored, processed, or transmitted on electronic systems (and networks). This includes the protection of information systems against unauthorized access to, or modification of information, denial of service to authorized users and including those measures necessary to protect against, detect, and counter such threats.

Data: Recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. Data are discreet elements of information processed in a computer system, printed on paper or other medium such as CD-ROM, DVD, or diskette, and the analysis, combination or association of such elements can impart both content and context. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing or management information.

Deemed Export: The releasing or otherwise transferring "technology" or source code (but not object code) to a foreign person within the United States. Any release of "technology" or source code to a foreign person in the United States is deemed an export to the foreign person's most recent country of citizenship or permanent residency.

Export: An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner. The export of an item that will transit through a country or countries to a foreign destination is deemed to be an export to that destination. Items include - equipment, materials, proprietary software, information (CEII, CI, CUI), data and technology.

Foreign Corporations: Any corporation that is not incorporated in the United States. This is further defined as any company, contractor or subcontractor organized or existing under the laws of a country other than the United States.

Foreign Nationals: Foreign nationals do not possess permanent legal residence within the United States. Foreign nationals include foreign institutions or governments and foreign corporations that were not incorporated in the United States.

Intangible Export: Means technical information transmitted through electronic media (e.g. telephone, electronic mail and World Wide Web).

Information Technology (IT): Is any equipment, system or sub-system (hardware, software, contract or service) that creates, maintains, stores, accesses, shares, adds or changes Bonneville Data or information that is used by federal employees, contract staff, managed services, or vendors in support of hardware or software to be accessed or used by Bonneville or operated on behalf of Bonneville.

Operational Technology (OT): Is a subset of IT software, hardware, or service whose function is to directly control or support the operation, maintenance, or monitoring of the electrical grid and that satisfies the following; (1) Accesses or contains memory or storage (2) Has logical access.

Physical Security: Means those measures used to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and documents; to safeguard them against espionage, sabotage, damage, and theft; and to reduce the exposure to threats, which could result in a disruption or denial of service.

Re-export: An actual shipment or transmission of an item from one Foreign Country to another Foreign Country, including the sending or taking of an item to or from such countries in any manner. Items include - equipment, materials, proprietary software, information (CEII, CI, CUI), data and technology.

Security Incident: Means intended or actual harm or injury to an employee, contractor or visitor, Government or personal property, or unauthorized access, use, sabotage, theft or vandalism of Government or personal property.

Sensitive Foreign Nation. 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/Nations 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 Nation 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 Nation list.

State Sponsor of Terrorism: A country designated by the U.S. Secretary of State as a State Sponsor of Terrorism. Countries designated by the U.S. Secretary of State as a State Sponsor of Terrorism are listed in: Appendix 15, Attachment 15-2, Export Control and Home Security Links.

Technology: Means both technical equipment, technical data and technical assistance and includes both Information Technology and Operational Technology.

Temporary Export: The transmission, shipping, carrying of equipment, materials, items, proprietary software, or protected information which is under physical control of a foreign national in some manner, which is returned to the U.S. or the country of origin after a specified period of time. Items being repaired or on loan in another country.

15.10 Homeland Security

15.10.2 Designation and Policy

- (a) It is Bonneville policy to protect the agency facilities, Critical Energy Infrastructure Information (CEII) and Critical Information (CI).
- (b) The U.S. Department of Homeland Security designates Bonneville as part of the critical national infrastructure. Information concerning the physical and technical infrastructure of Bonneville's existing and future power or transmission operations or information systems, which may be represented in data, drawings, notes, or oral presentations is deemed information critical to maintaining national security. This information shall not be exported tangibly or intangibly to countries on the Sensitive Foreign Nations list or to any country designated as a State Sponsor of Terrorism by the U.S. Department of State. Any intended Export of this information must have the prior written approval of Bonneville's Export Control Office and Bonneville Cyber Security and be in accordance with all laws of the United States. Breach of this section shall be reported immediately to Bonneville's Export Control Office and Bonneville Cyber Security.

15.10.3 Contract Clause

COs shall include the clause 15-18, Homeland Security in solicitations and contracts when –

- (a) Bonneville is contracting for services, information technology, operational technology, or other hardware, software, maintenance, or support; or
- (b) The contractor may require access to any data, critical energy infrastructure information, or critical information for the performance of the work; or
- (c) An export, deemed export or temporary export may occur; or
- (d) A re-export may occur; or
- (e) A non-disclosure agreement has been included; or
- (f) Any other instance where the requisitioner, COR or CO determines it is necessary to protect Bonneville's interests.

35.2.177 Clause 15-18, Homeland Security. As prescribed in 15.10.3, insert the following clause in solicitations and contracts:

Clause 15-18, HOMELAND SECURITY (OCT 2023)

- (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 Nation or by Sensitive Foreign Nation National. Additionally, no portion of the Contractors services, software, maintenance or support shall be subcontracted for performance in a Sensitive Foreign Nation or by Sensitive Foreign Nation 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 determine if the foreign country is a Sensitive Foreign Nation 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.
- (f) Notification of security incident. The contractor shall immediately notify Bonneville's Office of the Chief Information Officer (OCIO) Chief Information Security Officer (CISO) of any security incident and cooperate with Bonneville in investigating and resolving the security incident. In the event of a security incident, the contractor shall notify the CISO by telephone and ask for a Cyber Security Officer.

15.11 Export Control

U.S. Export Control Regulations apply to the export, temporary export, deemed export or re-export of Bonneville equipment, materials, items, proprietary software, information (including CEII, CI and CUI), data, or technology to foreign nationals or foreign corporations whether within or outside the U.S. The intent of the export control regulations is to safeguard national and economic security. The transmission, shipping, or carrying of any Bonneville equipment, materials, items, proprietary software, information, data, or technology to a foreign national or foreign corporation outside the U.S. is an export. The transmission, shipping, or carrying of any Bonneville equipment, materials, items, proprietary software, information, data, or technology to a foreign national that takes place – within the U.S. is considered to be an Export to the foreign national's country, and is classed as a "deemed export".

15.11.1 Policy

- (a) The transmission, shipping, or carrying of any Bonneville equipment, materials, items, proprietary software, information (Including CEII, CI and CUI), data or technology to foreign corporation's or foreign national's (non-U.S citizens) must be approved by the: (1) Bonneville Office of Personnel and Information Security pursuant to Bonneville Policy 430-1, and (2) Bonneville Export Control Office pursuant to Bonneville Policy 430-3, prior to the issuance of a solicitation or a contract award.

- (b) The transmission, shipping, or carrying of any Bonneville equipment, materials, items, proprietary software, information (including CEII, CI and CUI), data or technology to sensitive foreign nations or nationals of a country designated by the U.S. Secretary of State as a State Sponsor of Terrorism, within or outside the U.S is not permitted, unless authorized in writing on a case by case basis by the Export Control Office and the HCA.

15.11.2 Procedure

- (a) Requisitioners and CORs shall, (1) identify and mark, and (2) notify the CO and the Export Control Office of any solicitation or contract requirements that include the provision, transmission, shipping, or carrying of any Bonneville equipment, materials, items, proprietary software, information (including CEII, CI and CUI), data or technology.
- (b) CO's shall advise the Export Control Office of any intended solicitation recipient that is a foreign corporation or foreign national when the factors identified in 15.11.2(a) are included in the requirements.
- (c) The Export Control Office will review the factors identified in 15.11.2(a) and the details of the foreign corporation or foreign national being sent the solicitation or awarded the contract(s) and advise the CO of one or more of the following:
 - (1) No exceptions to the US Export Control Regulations are noted,
 - (2) The requirements, statement of work or statement of objectives do not meet the Export Control Office requirements or US Export Control Regulations,
 - (3) The solicitation recipients or contract awardee do not meet the Export Control Office requirements or US export control regulations, or
 - (4) A certificate of export or an end-user agreement is required.
- (d) Bonneville's Office of Personnel and Information Security and, Bonneville's Export Control Office shall approve, in advance, all foreign nationals, whether located within or outside the U.S. who may, as a part of a solicitation or in the performance of a contract:
 - (1) Receive Bonneville critical energy infrastructure information, critical information, or controlled unclassified information
 - (2) Receive Bonneville equipment, materials, items, proprietary software, information, data or technology;Either; as a part of a solicitation or in the performance of a contract.
- (e) The Bonneville Office of Personnel and Information Security and Bonneville's Export Control Office shall determine if there is a risk of a deemed export or the need for an export license.

15.11.3 Solicitation Provisions

- (a) The CO shall include the Provision 15-20, Export Control, when the solicitation is being issued to US Contractors or US Nationals and one or more of the following criteria exists:
 - (1) The requisitioner, COR, or CO identifies or determines that the solicitation includes or may require the disclosure of any criteria listed in 15.11.2(a), or
 - (2) An intangible export may occur or an export license, export end user agreement, or other export documentation may be required, or
 - (3) A non-disclosure agreement has been included, or

- (4) Any other instance where the requisitioner, COR or CO determines it is necessary to protect Bonneville's interests.
- (b) The CO shall include the Provision 15-21 Re-export Control when the solicitation is being issued to foreign corporation or foreign nationals when one or more of the criteria listed in 15.11.1 (1), (2), (3) and (4) exists and the solicitation is being issued to a foreign corporation or foreign national.

Provision 15-20. Export Control (OCT 2023)

The U.S. Department of Homeland Security designates Bonneville as part of the critical national infrastructure. Offeror shall not export or temporary export any Bonneville proprietary software, critical energy infrastructure information, critical information or controlled unclassified information, or other protected information, data or technology, contained in this solicitation to a foreign corporation or foreign national without the CO's prior written approval.

Provision 15-21. Re-export Control (OCT 2023)

The U.S. Department of Homeland Security designates Bonneville as part of the critical national infrastructure. Offeror shall not re-export any Bonneville proprietary software, critical energy infrastructure information, critical information or controlled unclassified or other protected information, data or technology, included in this solicitation to another foreign corporation or foreign national for the purposes of preparing and submitting offers, without the CO's prior written approval.

15.11.3 Contract Clauses

- (a) The CO shall include the Clause 15-22, Export Control, in solicitations and contracts when:
 - (1) The requisitioner, COR or CO identifies or determines that the contract includes or may require the disclosure of any criteria listed in 15.11.2(a), or
 - (2) An Intangible Export may occur or an export license, export end user agreement, or other export documentation may be required, or
 - (3) A non-disclosure agreement has been included, or
 - (4) Any other instance where the requisitioner, COR or CO determines it is necessary to protect Bonneville's interests.
- (b) The CO shall include the Clause 15-23 Re-export Control, when one or more of the criteria listed in 15.11.1 (1), (2), (3) and (4) exists and the solicitation is being issued to a foreign corporation or foreign national.

Clause 15-22. Export Control (OCT 2023)

The U.S. Department of Homeland Security designates Bonneville as part of the critical national infrastructure. Contractor shall not export, or temporary export any Bonneville proprietary software, critical energy infrastructure information, critical information or controlled unclassified or other protected information, data or technology to a foreign corporation or foreign national without the CO's prior written approval.

Clause 15-23 Re-export Control (OCT 2023)

The U.S. Department of Homeland Security designates Bonneville as part of the critical national infrastructure. Contractor shall not re-export any BPA proprietary software, critical energy infrastructure information, critical information or controlled unclassified or other protected information, data or technology to a foreign corporation or foreign national without the CO's prior written approval.

15.12 Restrictions 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 nation 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 and OT, or other research, design, development, and support and/or maintenance services, with entities located within the countries identified on the sensitive foreign nation 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 may not be within any country identified on the sensitive foreign nation list, or a country designated by the U.S. Secretary of State as a state sponsor of terrorism.

15.12.2 Procedure

The Bonneville Export Control Office and Bonneville's Office of Cyber Security shall determine if there is a risk associated with contracting for IT and OT research, design, development, and support and/or maintenance services by foreign corporations or foreign nationals not physically located outside the United States. Additionally, any outsourcing of such services shall be approved by the Cyber Security and the Export Control Office. COs shall consult BPA Policy 432-1 Physical Security for guidance. In the event HCA issues a waiver for such services to be performed in a country listed as a sensitive foreign nation, the CO shall include in the official file any waivers given by the HCA and the Export Control Office allowing such services to be performed in those countries.

15.12.3 Contract Clause

The CO shall include the clause 15-18, Homeland Security, and Clause 15-22 Export Control, in solicitations and contracts when:

- (a) Bonneville is contracting IT and OT research, design, development, and support and/or maintenance services; or
- (b) The contractor may require access to any data, CEII, CI, and CUI, for the performance of the work; or
- (c) An export, deemed export or temporary export may occur; or
- (d) A re-export may occur; or
- (e) A non-disclosure agreement has been included; or
- (f) Any other instance where the requisitioner, COR or CO determines it is necessary to protect Bonneville's interests.

17.0 Patents, Copyright and Data.

17.6.2 Nondisclosure – Safeguarding of Information

Performance under a Bonneville contract may require disclosure of either contractor proprietary information, or Bonneville information, including critical energy infrastructure information (CEII), critical information (CI), or controlled unclassified information (CUI) as defined in subsection 15.10.1. Proprietary information is a broad category that includes trade secrets and technical Data as well as financial information. A trade secret is information, not generally known, that has economic value and is protected from disclosure by its owner. A trade secret may be a formula, pattern, method, process, or technique. Trade secret protection is frequently used to protect computer software. Contractors often utilize trade secret law to protect their software under a trial use or evaluation agreement by signing a nondisclosure agreement with the potential licensee.

17.6.2.1 Policy

The timing of information disclosure and who is making the disclosure determines the documentation necessary to protect the information. Bonneville can protect contractor information, in both the solicitation stage of the procurement and during the performance of a contract, subject to the requirements of the Freedom of Information Act and other statutory authority, through the inclusion of a nondisclosure clause in the contract. Disclosure of Bonneville information, including CEII, CI and CUI requires a stand-alone Nondisclosure Agreement drafted and approved by OGC. See subpart 11.6. Any disclosure of Bonneville information, including CEII, CI and CUI to a foreign national or foreign corporation shall be in accordance with sections 15.10, 15.11 and 15.12.

17.6.2.3.1 Procedure

- (a) COs and their designees shall not disclose to any outside source, including IT businesses, corporate survey firms, consultants, publications, potential offerors, or current contractors, any information pertaining to Bonneville IT system architecture, platforms, operating systems, specific software applications, hardware, or any portion of the general Bonneville IT environment, except as authorized by the requisitioner acting under the CIO's policy guidance, and then only as necessary to acquire goods and services required to satisfy the IT need.
- (b) Should the CO and requisitioner determine there is an appropriate rationale to disclose such information to offerors and/or contractors, CO's shall consult with OGC prior to any disclosure for guidance on appropriate markings, nondisclosure agreements and procedures.
- (c) The CO shall refer to Bonneville Policy 433-1 for guidance and policy on safeguarding Confidential Unclassified Information.
- (d) IT and OT procurements which require disclosure of information pertaining to Bonneville system architecture, platforms, operating systems, specific software applications, hardware, or any portion of the general Bonneville environment must adhere to the disclosure requirements as set forth in 17.6.2. Procurements which require disclosure of Bonneville critical information or Data should be referred to OGC for preparation of a nondisclosure agreement as set forth in subpart 11.6. Additionally, any publication of IT or OT requirements must comply with subpart 11.3.

Export Control

BPI Appendix 15

Issued by the Head of Contracting Activity
Bonneville Power Administration





1	EXPORT CONTROL REQUIREMENTS AND PROCEDURES	2
1.1	Export control.....	2
1.2	Coverage	2
1.3	Standards	2
1.4	Exclusions	2
2	EXPORT CONTROL AND HOMELAND SECURITY LINKS	2
2.1	Links	2
	Attachment 15-1. Export Control Procedures and Requirements	3
	Attachment 15-2. Export Control and Homeland Security Links.	4

1 EXPORT CONTROL REQUIREMENTS AND PROCEDURES

1.1 EXPORT CONTROL

Bonneville Purchasing Instructions (BPI) Appendix 15 provides the Bonneville Acquisition Workforce (AWF) with additional information on requirements and procedures, necessary to comply with Bonneville Power Administration's Export Control Program policy 430-3, procedure 430-3-1 and Executive and Department orders and policy updates related to cyber, data and information risk management.

1.2 COVERAGE

The export control requirements and procedures provided in this Appendix are to be followed by Contracting Officers, Contracting Officer Representatives, requisitioners, business unit requesters, the Export Control Office and any individuals engaged in the development or administration of contracting requirements (statements or work, statement of objective, standards, specifications, changes to etc.).

1.3 STANDARDS

The requirements and procedures provided in Attachment 15-A shall be followed for all solicitations, contract awards, contract administration and closeout that include/may require the disclosure of the criteria identified in the first column of diagram 15-A.

1.4 EXCLUSIONS

The requirements and procedures of this Appendix do not apply to:

- (a) Financial Assistance (Grants or Cooperative Agreements); or
- (b) Contracts and subcontracts with Indian Tribes under the Indian Self Determination and Education Assistance Act (the exclusion would not apply to a procurement contract or subcontract under the BPI to an Indian-owned or tribally-owned business entity); or
- (c) Contracts not subject to the Bonneville Purchasing Instructions (BPI).

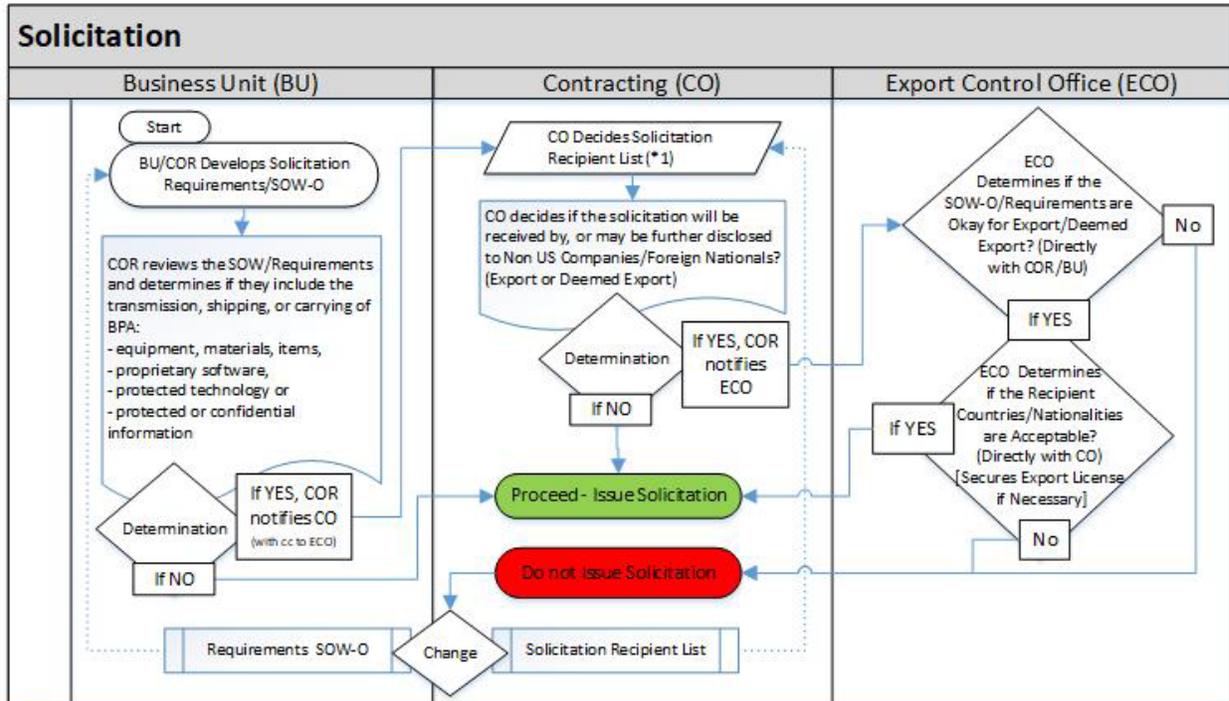
2 EXPORT CONTROL AND HOMELAND SECURITY LINKS

2.1 LINKS

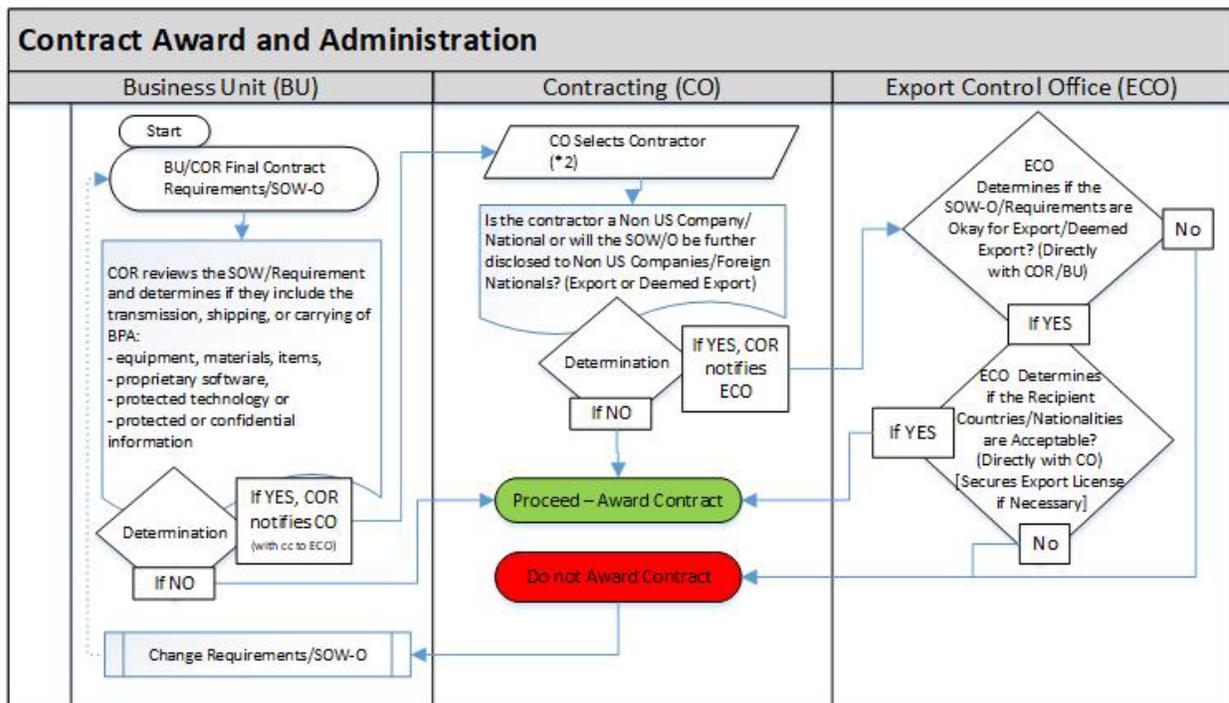
The Bonneville Purchasing Instructions (BPI) Appendix 15-B provides links to:

- (a) Sensitive Foreign Nations
- (b) State Sponsors of Terrorism

Attachment 15-1. Export Control Procedures and Requirements



* 1. Generally – in consultation with the business unit.



* 2. Subcontractors Identified as necessary.

Attachment 15-2. Export Control and Homeland Security Links.

Sensitive Foreign Nation:

(C) 8 SEC J_Appendix D - Sensitive Foreign Nations Control.pdf (energy.gov)

https://www.energy.gov/sites/default/files/migrated/nnsa/2017/11/f45/%28C%29%208%20SEC%20J_Appendix%20D%20-%20Sensitive%20Foreign%20Nations%20Control.pdf

State Sponsor of Terrorism:

<https://www.state.gov/state-sponsors-of-terrorism/>