United States Government **Department of Energy**

Bonneville Power Administration

memorandum

DATE: 09/16/2020

REPLY TO ATTN OF: CGP

SUBJECT: BPI Interim Policy 2020-01 Cyber Security Risk CIP 013

TO: Lynnial Trusty – NSS – 4400

The purpose of this memorandum is to provide detailed guidance (referred to as the "Interim Policy") to the Bonneville Purchasing Instruction (BPI) clarifying the immediate impacts of the recent NERC issued Reliability Standard CIP-013 Cyber Security Supply Chain Risk Management. The purpose of CIP-013 is to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

The policy is effective October 1st, 2020 and will remain in place until December 31st, 2021, but may be extended if necessary to coincide with the promulgation of the next revision of the Bonneville Purchasing Instructions (BPI). This interim policy supersedes the BPI dated February 1st, 2020.

Contracting Officers should abide by all changes issued under this interim policy update. All solicitations and contracts issued after the effective date of this transmittal shall comply with the requirements of this update unless otherwise directed by the HCA.

SUMMARY OF CHANGES TO THE BPI:

TOPIC	REFERENCE	CHANGE	CLAUSE
Definition	BPI 15.8.1	Added a BES Cyber Assets (BCAs) definition	N/A
Policy	BPI 15.11.1	Added new policy regarding NERC issued Reliability Standard CIP-013	N/A
Policy	BPI 15.11.2	Added 15-19 policy to direct COs to include clause 15-19, Contractor Supply Chain Security Controls	N/A

Clause	BPI 15-19	Added a clause for Contractor-identified cyber security incidents related to the products or services provided to Bonneville that pose cyber security risk to Bonneville.	Contractor Supply Chain Security Controls (15-19) (OCT 2020)(15.11)
Prescription	BPI 15-18	Revised the prescription for clause 15-18 to add part (b). (b) Bonneville is contracting for products or services associated with BES Cyber Systems	N/A

The italicized font below indicates the type of change that has occurred.

{added a new BCA definition in section 15.8.1}

15.8.1 Definitions

BES Cyber Assets (BCAs) means a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk electric system.

{added a new 15.11.1 policy}

15.11 CONTRACTOR SUPPLY CHAIN SECURITY CONTROLS

15.11.1 Policy

Bonneville is subject to the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards. NERC issued Reliability Standard CIP-013 *Cyber Security Supply Chain Risk Management*. The purpose of CIP-013 is to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS). To assure Bonneville meets the requirements of CIP 013, contractors must notify Bonneville of any cyber security incidents, all known security vulnerabilities related to their products or services, and ensure the integrity and authenticity of their products or services. Whenever contracts are issued for

products or services associated with BCS, Homeland Security Clause 15-18 must also be included in the contract.

{added a new 15.11.2 policy}

15.11.2 Contract Clause

The CO shall include the clause 15-19, Contractor Supply Chain Security Controls, in all solicitations and contracts where the contractor will provide products or services associated with BES Cyber Systems.

{added a new 15.19 contract clause}

CONTRACTOR SUPPLY CHAIN SECURITY CONTROLS (15-19)
(OCT 2020)(15.11)

(a) The Contractor shall notify Bonneville in the event of and coordinate responses to Contractor-identified cyber security incidents related to the products or services provided to Bonneville that pose cyber security risk to Bonneville. Examples of such incidents could be, but are not limited to, disclosure of proprietary code repositories, private digital certificates, proprietary or personally-identifiable information (PII) of Bonneville, its employees, contractors, or partners, or compromise of Contractor user credentials related to products or services provided to Bonneville.

(b) The Contractor shall provide information to Bonneville of known security vulnerabilities related to their products or services in accordance with NERC CIP-013 R1.2.4. This information shall include a method of disclosing known vulnerabilities, both past and present, with a clear explanation of how these vulnerabilities are currently addressed, and a method Bonneville may use for obtaining security vulnerability fixes, patches, and configuration or mitigation activities. The information provided should be brief, yet comprehensively outline the Contractor's capability to address any security vulnerabilities. If no known vulnerabilities exist, this should be clearly stated as such along with the Contractor's intended process or mechanism to support Bonneville's ability to address any such security vulnerabilities that may be discovered in future.

(c) The Contractor shall ensure the integrity and authenticity (in accordance with NERC CIP-013 R1.2.5) of all software/firmware products, versions, and patches Bonneville may purchase from the Contractor.

(d) The Contractor shall comply with Bonneville policy *Managing Access and Access Revocation for NERC CIP Compliance* (430-2).

(e) The Contractor shall include this clause in all subcontracts.

{revised the prescription for clause 15-18 to add (b) as noted below}

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

(a) Bonneville is contracting for hardware, software, or services;
(b) Bonneville is contracting for products or services associated with BES Cyber Systems;
(c) A non-disclosure agreement has been included; or
(d) Any other instance where the requisitioner or CO determines it is necessary to protect
(e) Bonneville's interests.

NICHOLAS JENKINS

Digitally signed by NICHOLAS JENKINS
Date: 2020.09.16 15:39:38 -07'00'

Nicholas M. Jenkins
Head of the Contracting Activity
Bonneville Power Administration

cc:
McDonald, Tom– C-7
Frost, Christopher – CG-7
Kuhn, Shana – NS – 4400
DeLong, Matt – NSS – 4400
McMahon, Amber L (BPA) - NSSS-4400-2