Exhibit 7

NERC REQUIREMENTS

1. Applicability to Bulk Electric System Cyber Systems and Information

1.1 Pursuant to a directive from the North American Electric Reliability Corporation ("**NERC**"), PG&E has implemented policies and procedures for the protection of facilities, systems, assets and information that are critical to the operation or support of the Bulk Electric System ("**BES**"). PG&E identifies these facilities, systems, assets and information in accordance with its internal utility procedures.

1.2 If this Contract relates to BES Cyber Systems or BCSI, or their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) (as designated by PG&E), then Contractor must comply with the additional requirements described in this Exhibit 7. Contractor represents and warrants that it has consulted with PG&E to determine whether Exhibit 7 is applicable.

2. Definitions

2.1 The following terms are defined for use in this Exhibit:

2.1.1 "**Access**" means:

a) Unescorted access by any person to facilities, systems and functions that PG&E deems critical to the support of the Bulk Electric System ("**Critical Facilities and/or Critical Systems**"), including persons working within PG&E Critical Facilities and/or Critical Systems; and

b) Physical or electronic access by any person to BCSI, or administrative control over BCSI or systems containing BCSI. For the avoidance of doubt, disclosing BCSI to a person by any means constitutes Access to such information by that person.

2.1.2 "**BCSI**" means Bulk Electric System Cyber System Information in any form (whether printed or electronic) including data, files, and file attributes. BCSI is information about a BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as determined by PG&E. BCSI is typically classified by PG&E as "NERC CIP Confidential – BCSI" or "Restricted – BCSI," but not all BCSI data will be designated as such in all formats.

2.1.3 "**BES**" means Bulk Electric System.

2.1.4 "**BES Cyber Asset**" ("**BCA**") means a programmable electronic device, including the hardware, software, and data in the device, that if rendered unavailable, degraded, or misused, would within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, functions, applications, or equipment, and which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES.

2.1.5 "**BES Cyber System**" ("**BCS**") means a grouping of BCAs.

2.1.6 "**CIP**" means Critical Infrastructure Protection

2.1.7 "**Disclosed**" means any circumstance when the security, integrity, or confidentiality of any PG&E Information has been compromised, including, but not limited to incidents where (i) PG&E Information has been damaged, lost, corrupted, destroyed; (ii) a third party has gained control over access to PG&E Information (including as part of a ransomware attack); (iii) PG&E Information has been accessed, acquired, modified, or used by, or disclosed to, an unauthorized third-party by any person in an unauthorized manner, or for an unauthorized purpose.

2.1.8 "**FERC**" means the Federal Energy Regulatory Commission.

2.1.9 "**PRA**" means Personal Risk Assessment.

2.1.10 "**NERC**" means the North American Electric Reliability Corporation or its successor.

2.1.11 "**Security Incident**" means any circumstance when (i) Contractor knows or should have reason to believe that PG&E Information that is protected, hosted or stored by the Contractor has been Disclosed; (ii) Contractor knows or should have reason to believe that its act or omission has

compromised or may reasonably compromise the confidentiality or cybersecurity of PG&E Information or of the products and services provided to PG&E by Contractor or the physical, technical, administrative, or organizational safeguards protecting Contractor's or PG&E's systems responsible for protecting, storing or hosting PG&E Information; or (iii) Contractor receives any complaint, notice, or communication which relates directly or indirectly to (A) Contractor's handling and safeguarding of PG&E Information, Contractor's compliance with the data safeguards in the Agreement or any applicable law, (B) or regulation in connection with protection or safeguarding of the PG&E Information, or (C) the confidentiality or cybersecurity associated with the products or services provided to PG&E by the Contractor.

2.1.12 "**PG&E Information**" means, for the purposes of these terms and conditions, any and all information concerning PG&E, and its business in any form, including, without limitation, the products and services provided under this Agreement that is disclosed to otherwise learned by Contractor during the performance of this Agreement.

2.1.13 "**WECC**" means the Western Electricity Coordinating Council or its successor.

3. NERC CIP Security Obligations

3.1 Contractor shall comply with all cyber security policies, plans and procedures relating to the BES Cyber Systems and/or BCSI as directed by PG&E. As directed by PG&E, Contractor shall provide documentation and evidence demonstrating such compliance. This may include the conduct of periodic tests and audits as specified by PG&E from time to time. Contractor acknowledges that Contractor's failure to comply and demonstrate compliance may subject Contractor and/or PG&E to fines and other sanctions.

3.2 Before being granted Access, Contractor must satisfactorily complete PG&E's Vendor Security Review process. If Work is to be performed at Contractor locations, those locations must be approved by PG&E following completion of the Vendor Security Review Process. PG&E's approval does not limit its rights to conduct periodic audits and reviews as provided in the Contract.

3.3 Contractor shall ensure that (i) any BCSI that is obtained by Contractor is stored and Accessed only within the United States, (ii) BCSI is not copied, exported, transferred or otherwise transmitted outside the United States, and (iii) no third party (including without limitation any individual, corporation, government or governmental agency), system or environment located outside the United States obtains Access to BCSI through Contractor. Without limiting any other term of this Contract, a third party, system, or environment will be deemed to have Access to BCSI if Contractor shares BCSI with such third party, system, or environment in any manner, or if such third party uses access tokens, cards, credentials, or other means of authentication furnished to Contractor by PG&E to obtain, view, download, or copy BCSI.

3.4 Contractor shall ensure that any personnel requiring Access successfully complete background checks ("**Personnel Risk Assessments**" or "**PRAs**") and PG&E-mandated security training before they obtain Access, in accordance with the following requirements:

3.4.1 Contractor shall perform a background screening for each individual that includes each of the following criteria: (i) Social Security Number verification; (ii) City, County, State and Federal Criminal Check for felonies and misdemeanors over the past seven years (in up to three counties where the individual has lived in the past seven years); (iii) "Global Watch" (check of 19 Federal and International Terrorist Watch lists); and (iv) validation of current residence and confirmation of continuous residence at this site for a minimum of the most recent 6 months (confirmed by period of residence, employment, or education at a specific site) and validation of other locations where, during the seven years immediately prior to the date of the foregoing Federal Criminal Check, the individual has resided for six consecutive months or more.

3.4.2 After performing an acceptable background check, the Contractor shall provide PG&E's Human Resources Department with a copy of the complete Personnel Risk Assessment results at the time the Access request is submitted.

3.4.3 Contractor shall require that each individual complete an initial training and annual PG&E web-based training session on safety, information security, compliance with PG&E codes and procedures, including but not limited to CORP-0804 Cyber and Physical Security Awareness training (or alternative training as designated by PG&E).

3.4.4 After Contractor certifies to PG&E completion of the requirements set forth in paragraphs 3.4.1 through 3.4.3 above, PG&E will issue appropriate Access credentials. PG&E will deny Access to any individual for whom Contractor has not certified completion of the requirements set forth in such referenced paragraphs.

3.4.5 Every seven years, Contractor shall perform background screening as described herein for each individual on continuing assignment who has Access.

3.4.6 Contractor shall retain documentation supporting the Personnel Risk Assessment Attestation Form for each individual with Access for a minimum of seven years.

3.4.7 PG&E may audit Contractor's background screening methodology and substantiate the accuracy of Personnel Risk Assessment Attestation Forms for each individual. Contractor shall respond to any auditing requests and activities, including but not limited to data requests, within one business day. PG&E and/or WECC will set the frequency of auditing the Contractor's PRA process and supporting records.

3.5 After being granted access, Contractor agrees to notify PG&E at the sooner of close of business or 11:59 PM on the same day of any personnel departures or changes in roles of Contractor personnel who no longer require Access.

3.6 Unless otherwise indicated, Contractor agrees to notify PG&E of any Security Incidents within 24 hours of discovery.

3.7 Unless otherwise indicated, Contractor agrees to work with PG&E on a coordinated response to any Security Incidents as defined in this Exhibit.

3.8 Unless otherwise indicated, Contractor agrees to notify PG&E of any known vulnerabilities related to the products or services provided to PG&E within 1 business day of discovery of the vulnerability.

3.9 Unless otherwise indicated, Contractor agrees to work and cooperate with PG&E, to the satisfaction of PG&E, to develop mechanisms that verify the software integrity and authenticity of all software and patches provided by the Contractor for use in the BES Cyber Systems.

3.10 Unless otherwise indicated, Contractor agrees to adhere to PG&E's requirements for vendor-initiated Interactive Remote Access, as well as system-to-system remote access with a vendor.

3.11 In addition to its other indemnity obligations hereunder, Contractor shall indemnify and hold harmless PG&E for any fines, penalties or other sanctions assessed against PG&E (including but not limited to fines, penalties or sanctions assessed against PG&E by the WECC, NERC, or the FERC for a violation of any NERC reliability standard) caused by Contractor's failure to perform its obligations under this Contract.

3.12 If Contractor is providing, installing or configuring equipment or software to be used in a BES Cyber System, Contractor shall comply with NERC CIP 013 Addendum (www.pge.com/nerc-cip-013).