CIP-013 Addendum

NERC REQUIREMENTS

I. Applicability to Bulk Electric System Cyber Systems and Information

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**") and/or their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). PG&E identifies these facilities, systems, assets and information in accordance with its internal utility procedures.

If this Contract relates to BES Cyber Systems or BCSI (as designated by PG&E), or their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS),and is designated as in scope for CIP-013 requirements, then Contractor must comply with the additional requirements described in this Addendum.

II. Definitions

The following terms are defined for use in this Addendum:

"**Access**" means:

1) Electronic access by any individual connecting (i.e. IRA) to PG&E systems, functions and/or applications that PG&E deems critical to the support of BES (i.e. IRA)

2) Electronic access by a non-PG&E system to a PG&E system or systems, functions, and/or applications that PG&E deems critical to the support of the BES (i.e. system-to-system)

3) Unescorted physical access by any individual to facilities, systems and functions that PG&E deems critical to the support of the Bulk Electric System (BES)

4) Physical or electronic access by any individual to PG&E BES Cyber System Information (BCSI), or administrative control over BCSI or systems containing BCSI. For the avoidance of doubt, disclosing BCSI to an individual by any means constitutes access to such information by that individual.

"**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.

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, application, or equipment, and which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES.

BES Cyber System ("BCS") means a grouping of BES Cyber Assets

Bulk Electric System ("BES") means, unless modified by NERC documentation and processes, all transmission elements operating at 100 kV or higher and real power and reactive power resources connected at 100 kV or higher. Does not include facilities use in the local distribution of electric energy.

"**Contractor**" means organization or individual providing products or services to PG&E. For the avoidance of doubt, a Contractor can be either or both an organization or individual.

Critical Infrastructure Protection (“CIP”) means a set of regulatory standards developed by the North American Electric Reliability Corporation (“NERC”) to ensure the reduction of risks to the Bulk Electric System (“BES”)

“**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 PG&E Information has been damaged, lost, corrupted, destroyed; or 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.

Electric Reliability Organization (“ERO”) means NERC and the six (6) Regional Entities which enforce the NERC CIP security standards. For this Addendum, the ERO will include FERC.

Electronic Access Control or Monitoring Systems (“EACMS”) means any Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems

Federal Energy Regulatory Commission (“FERC”) means Federal agency granted the authority under the Federal Power Act (“FPA”) of 2005 and subsequent amendments to ensure the safe operation and reliability of the Bulk Electric System (“BES”).

Interactive Remote Access (“IRA”) means user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol

North American Reliability Corporation (“NERC”) means the agency (or its successor) which has the regulatory authority to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Electric System (“BES”). Regulatory authority granted to NERC by the Federal Energy Regulatory Commission (“FERC”).

Personnel Risk Assessment (“PRA”) means process and information on background checks for individuals requiring access to PG&E BES Cyber System (“BCS”) or BES Cyber System Information (“BCSI”).

“**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 or otherwise learned by Contractor during the performance of this Agreement.

PG&E Point of Contact (“**PG&E POC**”**)** means any organization at PG&E, and its designated representatives, whose functions and/or responsibilities necessitate direct engagement with the contractor

Physical Access Control Systems (“PACS”) means Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

“**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, B) Contractor’s compliance with the data safeguards in the Agreement or any applicable law 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..

"**Software**" means compiled code created or purchased by the Contractor and supplied to PG&E, source code created or purchased by the Contractor and supplied to PG&E, or software acquired using open source distribution and supplied to PG&E.

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

III. Conflict of Terms

In case of any conflict between the terms in the CIP-013 Addendum and the terms in the general conditions, the terms of the CIP-013 Addendum shall prevail.

IV. NERC CIP Security Obligations

A. Contractor shall implement and demonstrate to PG&E's satisfaction the implementation of a security framework and controls for the governance and protection of the Contractor's products and services supplied to PG&E.

B. Contractor shall comply with all cyber security policies, plans and procedures relating to the BES Cyber Systems and/or BCSI and/or their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) as directed by PG&E. As directed by PG&E, Contractor shall provide documentation and evidence demonstrating such compliance. This may include conducting periodic assessments, tests and audits as specified by PG&E. Contractor acknowledges that Contractor's failure to comply and demonstrate compliance may subject PG&E to regulatory enforcement actions including costs of handling the enforcement actions, penalties, fines and other sanctions for which PG&E will seek redress from Contractor.

C. 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.

D. Contractor shall ensure that any individual requiring Access successfully complete PRA background checks and PG&E-mandated security training before obtaining Access, in accordance with the following requirements:

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.

2) After performing an acceptable background check, the Contractor shall provide PG&E's Human Resources Department with a a copy of the complete Personnel Risk Assessment results at the time the Access request is submitted.0

3) Contractor shall require that each individual complete an initial training and timely complete annual PG&E web-based training sessions 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). Contractor shall direct that each individual complete the PG&E training program by CD or by hard copy format, if Contractor informs PG&E that web based training is not feasible. Satisfactory and timely completion of the training specified by PG&E is required for each Contractor to establish and maintain Access.

4) After Contractor certifies to PG&E completion of the requirements set forth in paragraphs D(1) through (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 paragraphs D(1) through (3) above.

5) No later than every seven years, Contractor shall perform background screening as described herein for each individual on continuing assignment who has Access to extend their Access.

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

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.

E. Contractor with Access to PG&E BCS or PG&E BCSI shall:

1) Implement policies and procedures to address and ensure the security of remote and onsite access to PG&E Information, BCSI, PG&E Systems and network, and PG&E property (an "Access Control Policy") that is consistent with the personnel management requirements of NIST Special Publication 800-53 Rev. 4 AC-2, PE-2, PS-4, and PS-5 (or other comparable industry standard) as may be amended and also meets the following requirements:

   a. In the course of furnishing products and services to PG&E under this agreement, Contractor shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Contractor Personnel") to access PG&E property, systems, or networks or PG&E Information, or BCSI, without PG&E's prior express written authorization. Such written authorization may subsequently be revoked by PG&E at any time at PG&E's sole discretion.

   b. Any Contractor Personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by PG&E.

   c. All PG&E authorized connectivity or attempted connectivity to PG&E's systems or networks shall be in conformity with PG&E's security policies as may be amended from time to time with notice to the Contractor.

   d. Contractor will regularly (at least quarterly) review and verify Contractor Personnel's continued need for access and level of access to PG&E Information (including BCSI), PG&E systems, networks, and property on a quarterly bases and will retain evidence for seven years from the date of each review.

   e. Contractor will immediately notify PG&E in writing (no later than the sooner of close of business or 11:59 PM on the same day as: the day of termination or change sent forth below) and will immediately take all steps necessary to remove Contractor Personnel's access to any PG&E Information, system, networks, or property when

      i. Any Contractor Personnel no longer requires such access,

      ii. Any Contractor personnel is terminated or suspended or his or her employment is otherwise ended,

      iii. Contractor reasonably believes any Contractor Personnel poses a threat to the safe working environment at or to any PG&E personnel or property, including to PG&E employees and customers,

      iv. Contractor discovers any material adverse changes to any Contractor Personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record, as well as any changes involving the loss of Contractor Personnel's U.S. work authorization.

      v. Any Contractor Personnel fails to maintain conduct in accordance with the qualifications set forth in PG&E's vendor code of conduct.

2) Contractor shall, as part of its Access Control Policy, take all steps reasonably necessary to immediately deny such Contractor Personnel electronic and physical access to PG&E Information as well as PG&E property, systems, or networks, including, but not limited to, removing and securing individual credentials access badges, RSA tokens, and laptops, as applicable, and will return to PG&E any PG&E-issued property including, but not limited to,

PG&E photo ID badge, keys, parking pass, documents, or laptop in the possession of such Contractor Personnel.

3) Complete the Access requirements indicated in Article IV.D of this Addendum.

4) Submit to monitoring of the Access and agree to suspension or termination of the Access on suspected unauthorized or potentially malicious activity as determined by PG&E.

5) Contractor shall ensure that: (i) no third party or third party system or environment (including, without limitation, that of any individual, corporation, subsidiary or affiliate of Contractor, subcontractor, government or governmental agency) obtains Access to BCSI through Contractor without the express written permission of PG&E; (ii) any BCSI that is obtained by Contractor is secured, stored and Accessed only within the United States, and (iii) BCSI is not copied, exported, transferred or otherwise transmitted outside the United States.. 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 can use access tokens, cards, credentials, or other means of authentication furnished to Contractor by PG&E to access, obtain, view, download, or copy BCSI.

F. Access no longer required:

1) Notify PG&E POC at the sooner of close of business or 11:59 PM on the same day of any departures or change in roles of Contractor personnel who no longer require Access.

2) Notification shall be submitted in electronic form to the PG&E POC for Access control and receipt of the notification verified by Contractor.

G. Before the connection of any Contractor Cyber Asset(s) to PG&E BCS or network related to the BCS, Contractor must:

1) Implement measures and processes designed to ensure malware protection is deployed to PG&E's satisfaction on Service Provider Cyber Assets connected to PG&E BCS and those Cyber Assets are maintained to the latest product versions, signatures, and/or configurations to protect against the latest threats.

2) Provide on request to PG&E, process documentation and evidence the Cyber Assets indicated in Article IV.G(1) are maintained.

H. Security Incident Reporting

1) Contractor shall develop and implement policies and procedures to address Security Incidents ("Response Plan") by mitigating the effects of Security Incidents; addressing and remediating the Security Incident occurrence; and implementing processes, controls or procedures to prevent the recurrence of Security Incidents in the future. Contractor shall provide PG&E access to inspect its Response Plan. The development and implementation of the Response Plan shall follow best practices that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 (or other comparable industry standard) as those standards may be amended.

2) Contractor agrees to notify PG&E Point-of-Contact immediately by telephone, and subsequently via electronic communication, whenever a Security Instance occurs. Subsequent notifications by Contractor shall be submitted in electronic form to PG&E Point of Contact and receipt of the notification shall be verified by Contractor.

This notice shall include the date and time of the Security Incident occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of (a) why the Security Incident occurred, if known (e.g. a precise description of the reason for the system failure), (b) the nature and amount of PG&E Information known or reasonably believed to have been Disclosed, and (c) the measures

being taken to address and remedy the occurrence to prevent the same or similar event from occurring in the future.

Contractor shall provide regular and prompt electronic updates of the notice to PG&E addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances. Contractor shall cooperate with PG&E in PG&E's efforts to determine the risk to the BES posed by the Security Incident, including providing additional information regarding the Security Incident upon request from PG&E.

I. Coordination of Incident Response:

1) Contractor shall develop and implement policies and procedures to address Security Incidents ("Response Plan") that address: the mitigation of harmful effects of Security Incidents, the remediation of Security Incident occurrences, and the prevention of recurrence of Security Incidents in the future.

2) Contractor shall provide PG&E access to inspect its Response Plan.

3) The development and implementation of the Response Plan shall follow best practices that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 (or other comparable industry standard) as those standards may be amended.

4) Within 10 DAYS of a Security Incident, Contractor shall develop and begin execution of a plan that reduces the likelihood of the same or similar Security Incident from occurring in the future consistent with the requirements of its Response plan, and shall communicate that plan to PG&E.

5) Within 10 DAYS of notifying PG&E of the Security Incident, Contractor shall, to the extent that PG&E may act, recommend actions to be taken by PG&E on PG&E-controlled systems to reduce the risk of recurrence of the same or similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Contractor shall coordinate with PG&E in developing those action plans and mitigating controls. Contractor will provide PG&E guidance and recommendations for long-term remediation of any cyber security risks posed to PG&E Information, equipment systems, and networks as well as any information necessary to assist PG&E in any recovery efforts undertaken by PG&E in response to the Security Incident.

6) In the event a Security Incident results in PG&E Information being Disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of PG&E under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by PG&E, except as required by applicable law or approved by PG&E in writing. PG&E will have sole control over the timing and method providing such notification.

7) In the event (a) Contractor's confidential information has been corrupted or destroyed or has been accessed, acquired, compromised, modified, used, or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose; (b) Contractor knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided by Contractor to an entity other than PG&E; or (c) Contractor receives any complaint, notice, or communication which relates directly or indirectly to (i) Contractor's handling of confidential information or Contractor's compliance with applicable law in connection with confidential information or (ii) the cybersecurity of the products and services provided by Contractor to an entity other than PG&E (Unrelated Security Incident), Contractor shall provide PG&E a confidential report describing, to the extent legally permissible, a detailed summary of the facts and circumstances of the Unrelated Security Incident, including a description of (1) why the Unrelated security Incident occurred (if known), (2) the nature of the confidential

information disclosed, and (3) the measures being taken to address and remedy the occurrence to prevent the same or similar event from occurring in the future.

J. Vulnerability Management:

1) Contractor shall implement a vulnerability detection and remediation program consistent with NIST Special Publication 800-53 Rev. 4 RA-5, SA-11, SI-2 (or comparable industry standard), as may be amended.

2) Contractor shall develop and implement policies and procedures to address the disclosure and remediation of Contractor of vulnerabilities and material defects related to the products and services provided to PG&E under this Agreement including the following:

   i. Prior to the delivery of the procured product or service, Contractor shall provide PG&E summary documentation of publicly disclosed vulnerabilities and material defects related to the procured product or services; the potential impact of such vulnerabilities and material defects, the status of Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

   ii. Prior to the delivery of any products and services to PG&E or any connection of electronic devices, assets or equipment to PG&E's electronic equipment, Contractor shall provide PG&E documentation regarding its patch management and vulnerability management/mitigation programs and update processes (including third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required to be connected to the assets of PG&E during the provision of products and services under this Agreement.

   iii. Unless otherwise approved by PG&E in writing, current or supported version of Contractor products and services shall not require the use of out-of-date, unsupported, or end-of-life versions of third-party components (e.g., Java, Flash, Web browser, etc.).

   iv. Contractor shall provide PG&E with summary documentation of vulnerabilities and material defects in the procured products or services within one (1) business day after such vulnerabilities and material defects become known to Contractor that could pose a threat to the BES Cyber Systems. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. The summary documentation shall include a description of each vulnerability and material defects and its potential impact, root cause, and recommended corrective actions, compensating security controls mitigations, and/or procedural workarounds.

   v. Contractor shall disclose to PG&E the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written documentation that all such backdoors created by Contractors have been permanently deleted or disabled.

   vi. In providing the products and services described in this agreement Contractor shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weakness within 14 days. If updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations and/or workarounds within 14 days of discovery of the critical vulnerability.

   vii. When third-party hardware, software (including open-source software), and firmware is provided by Contractor to PG&E, Contractor shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 days. If these third-party updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations and/or workarounds within 30 days).

3) Unless otherwise permitted by PG&E, Contractor-delivered solutions will be required to not reside on end-of-life operating systems, or any operating system that will go end-of-life, twenty-four (24) months from the date of installation.

4) Unless otherwise permitted by PG&E, Contractor solutions will support the latest versions of operating systems on which Contractor-provided software functions within twelve (12) months from official public release of that operating system version.

K. Software Integrity and Authenticity:

1) Contractor shall establish, document, and implement commercially reasonable risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under this Agreement. Contractor shall provide PG&E with documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, and instructions on how to request replacement parts.

2) Contractor shall specify to PG&E how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If PG&E deems that it is warranted, Contractor shall apply encryption to protect procured products throughout the delivery process.

a. If Contractor provides software or patches to PG&E, Contractor shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) information on the software and patches to enable PG&E to use the hash value as a checksum to independently verify the integrity of the software.

b. Contractor shall identify the country (or countries) of origin of the product procured and its components (including hardware, software, and firmware). Contractor will identify countries where the development, manufacturing, maintenance, and service for the product are provided. Contractor will notify PG&E of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur 180 days prior to initiating a change in the list of countries.

c. Contractor shall use trusted channels to ship procured products, such as U.S. registered mail.

d. Contractor shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

e. Contractor shall demonstrate chain-of-custody documentation for procured products as determined by PG&E in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

f. Where encryption is required, contractor shall:

i. Document how the cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system as specified by PG&E. This documentation shall include, but not be limited to the following:

1. The cryptographic methods (hash functions, symmetric key algorithms, asymmetric key algorithms), and primitives (e.g. Secure Hash Algorithm [SHA]-256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.

2. The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation

ii. Use only “approved” cryptographic methods as defined in the FIPS 140-2 Standard when enabling encryption on its products.

3) Contractor shall submit information to PG&E on the methods to verify the integrity and authenticity of any supplied Software.

L. System to System and Interactive Remote Access:

1) Contractor shall coordinate with PG&E on all remote access to PG&E's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by PG&E.

2) Contractors that, with express written permission of PG&E, directly (or through any of their affiliates, subcontractors, or service providers) connect to PG&E's systems or networks agree to the additional following protective measures:

i. Contractor will not access,and will not permit any other person or entity to access, PG&E's systems or networks without PG&E's authorization and any such actual or attempted access will be consistent with any such authorization.

ii. Contractor shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.

iii. Contractor shall ensure Contractor Personnel do not use any virtual private network or other device to simultaneously connect machines on any PG&E system or network to any machines on any Contractor or third-party system, without

1. Using only remote access method consistent with PG&E's remote access control policies,

2. Providing PG&E with the full name of each individual who uses such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and

3. Ensuring that any systems used by Contractor Personnel to remotely access any PG&E system or network will not simultaneously access the Internet or any third-party system or network while logged on to PG&E systems or networks.

Contractor shall ensure Contractor Personnel accessing PG&E networks are uniquely identified and that accounts are not shared between Contractor Personnel.

M. 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.