Dragos NERC CIP-013 Addendum

This North American Electric Reliability Corporation (NERC) CIP-013 Addendum (this "Addendum") shall apply to the extent that Customer's access to or use of a specific Offering requires that Dragos access Bulk Electric System (BES) Cyber Assets and Critical Energy Infrastructure Information (CEII).

1. DEFINITIONS

Unless otherwise defined herein, each term defined in the Agreement shall have the same meaning in this Addendum. Unless otherwise specified, references to "Section" refer to the applicable Section of this Addendum.

(a) ***"BES Cyber Asset ('BCA')"*** is defined by NERC as a Cyber Asset that if rendered unavailable, degraded, or misused would, within fifteen (15) minutes of its required operation, misoperation, 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 reliability operation of the Bulk Electric System. Redundancy of affected Facilities, systems and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

(b) ***"BES Cyber Systems ('BCS')"*** is defined by NERC as one or more BES Cyber Assets logically grouped by a responsibility entity to perform one or more reliability tasks for a functional entity.

(c) ***"BES Cyber System Information ('BCSI')"*** is defined by NERC as information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BCSI does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter (ESP) names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems (PACS), and Electronic Access Control or Monitoring Systems (EACMS) that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collection of network addresses; and network topology of the BES Cyber System. BCSI is considered CEII.

(d) ***"Critical Energy Infrastructure Information ('CEII')"*** is defined by the Federal Energy Regulatory Commission (FERC) as specific engineering, vulnerability or detailed design information about proposed or existing critical infrastructure (physical or virtual) that (a) relates details about the production, generation, transmission or distribution of energy, (b) could be useful to a person planning an attack on critical infrastructure, (c) is exempt from mandatory disclosure under the Freedom of Information Act, and (d) gives strategic information beyond the location of the critical infrastructure. As used herein, Customer Data includes CEII.

(e) "***Disclosed***" means any circumstance when the security, integrity, or confidentiality of any Customer Data has been compromised, including but not limited to incidents where Customer Data has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for any unauthorized purpose.

(f) "***Security Incident***" means any circumstance when (i) Dragos knows that Customer Data hosted or stored by Dragos has been Disclosed; (ii) Dragos knows that an act or omission has

compromised or may reasonably compromise the cybersecurity of the Offerings provided to Customer by Dragos or the physical, technical, administrative, or organizational safeguards protecting Dragos' systems or (iii) Dragos receives a credible, validated complaint, notice, or communication which relates directly or indirectly to a Security Incident involving (A) Dragos' handling of Customer Data or Dragos' compliance with the data safeguards in the Agreement or applicable laws; in connection with Customer Data or (B) the cybersecurity of the Offerings.

2. NOTIFICATION OF VENDOR-IDENTIFIED SECURITY INCIDENTS

(a) Dragos agrees to notify Customer whenever it becomes aware of a confirmed Security Incident, but in no case later than forty-eight (48) hours of such awareness; a written notice shall also be sent by email to Dragos' primary business contact with Customer. The notice shall include the date and time of the Security Incident's 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 (e.g., a description of the reason for the system failure), (b) the amount of Customer Data known or reasonable believed to have been Disclosed, and (c) the measure being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

(b) Dragos shall provide written updates of the notice to Customer 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. Dragos shall reasonably cooperate with Customer in Customer's efforts to determine the risk posed by the Security Incident, including providing additional information regarding the Security Incident upon request from the Customer.

3. COORDINATION OF RESPONSES TO CYBERSECURITY INCIDENTS

(a) Response Plan. Dragos shall develop and implement a "Response Plan," which shall include policies and procedures to address Security Incidents. The Response Plan shall include appropriate provisions for mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence(s) to prevent the recurrence of similar Security Incidents in the future. Dragos shall provide upon written request Customer access to inspect Dragos' Response Plan, with any sensitive information (i.e. technical details, granular playbooks, etc.) redacted. The development and implementation of the Response Plan shall follow industry generally accepted practices.

(b) Immediately upon learning of a confirmed Security Incident related to the Offerings provided to Customer, Dragos shall implement its Response Plan and, within 48 hours of implementing its Response Plan, shall notify Customer in writing of that implementation as described above.

(c) Prevention of Recurrence. Within thirty (30) days of a Security Incident, Dragos shall develop and execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan, and shall communicate that plan to Customer. Dragos shall provide recommendations to Customer on actions that Customer may take to assist in the prevention of recurrence, as applicable or appropriate.

(d) Coordination of Incident Response with Customer. Within five (5) days of notifying Customer in writing of the Security Incident, Dragos shall recommend actions to be taken by Customer on Customer-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Dragos shall coordinate with Customer in developing those action plans and mitigating controls.

Dragos will provide Customer guidance, recommendations, and other necessary information for recovery efforts and long-term remediation and/or mitigation of cyber security risks posed to Customer Data, equipment, systems, and networks as well as any information necessary to assist Customer in relation to the Security Incident.

(e) Notification to Affected Parties.

i. Dragos will, at its sole cost and expense, assist and cooperate with Customer with respect to any investigation of a Security Incident, disclosures to affected parties, and other remedial measures as requested by Customer in connection with a Security Incident or required under any applicable laws related to a Security Incident.
ii. In the event a Security Incident results in Customer Data 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 Customer 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 Customer, except as required by applicable law or approved by Customer in writing. Customer will have sole control over the timing and method of providing such notification.

4. ACCESS CONTROL

(a) Development and Implementation of Access Control Policy. Dragos shall develop and implement policies and procedures to address the security of Dragos' remote and onsite access to Customer Data, Customer systems and networks, and Customer property (an "Access Control Policy") that is consistent with the personnel management requirements of industry generally accepted practices and also meets the additional requirements set forth in this Section 4.

(b) Customer Authority over Access. In the course of furnishing Offerings to Customer under the Agreement, Dragos shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Dragos Personnel") to access Customer's property, systems, or networks or Customer Data without Customer's prior express written authorization. Such written authorization may subsequently be revoked by Customer at any time in its sole discretion. Further, any Dragos personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Customer. All Customer-authorized connectivity or attempted connectivity to Customer's systems or networks shall be in conformity with Customer's security policies as may be amended from time to time with notice to Dragos.

(c) Dragos Review of Access. Dragos will review and verify Dragos Personnel's continued need for access and level of access to Customer Data and Customer systems, networks and property on a semi-annual basis and will retain evidence of the reviews for two years from the date of each review.

(d) Notification and Revocation. Dragos will immediately notify Customer in writing, but under no circumstances later than close of business on the next day as the day of termination or change set forth below (except for 4(d)(i), in which case Dragos will notify Customer within five business days), when:

i. any Dragos Personnel no longer requires such access in order to furnish the Offerings provided by Dragos under the Agreement,
ii. any Dragos Personnel is terminated or suspended or his or her employment is otherwise

ended,

iii. Dragos reasonably believes any Dragos Personnel poses a threat to the safe working environment at or to any Customer property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or Customer Data,

iv. there are any material adverse changes to any Dragos Personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record,

v. any Dragos Personnel loses his or her U.S. work authorization, or

vi. Dragos' provision of Offerings to Customer under the Agreement is either completed or terminated, so that Customer can discontinue electronic and/or physical access for such Dragos Personnel.

Dragos will take all steps reasonably necessary to immediately revoke such Dragos Personnel's electronic and physical access to Customer Data as well as Customer property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multifactor security tokens, and laptops, as applicable. Further, for such revoked Dragos Personnel, Dragos will return to Customer any Customer-issued property including, but not limited to, Customer photo ID badges, keys, parking passes, documents, or electronic equipment in the possession of such Dragos Personnel. Dragos will notify Customer once access to Customer Data as well as Customer property, systems, and networks has been removed.

5. DISCLOSURE AND REMEDIATION OF VULNERABILITIES

Disclosure and Remediation by Dragos. Dragos shall develop and implement policies and procedures to address the disclosure and remediation by Dragos of vulnerabilities and material defects related to the Offerings provided to Customer under the Agreement. Dragos' policies and procedures on addressing the disclosure and remediation of vulnerabilities and material defects is contained in the Dragos Product Security Assurance and Vulnerability Policy (the "Policy"). Dragos may update the Policy from time to time, provided that such updates shall not result in a material degradation of Dragos' responsibilities and commitments as set forth in the prior version of the Policy, or have a materially negative impact on Customer's use of the Offerings. Dragos shall keep the Policy posted and accessible to Customer on the Dragos' portal.

6. SOFTWARE AND PATCH INTEGRITY AND AUTHENTICITY

(a) Hardware, Firmware, Software and Patch Integrity and Authenticity.

i. Dragos shall establish, document, and implement risk management practices for supply chain delivery of hardware, Software (including patches), and firmware provided under the Agreement.

ii. Dragos shall specify how digital delivery for Offerings (*e.g.*, Software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If Customer deems that it is warranted, Dragos shall apply encryption technology to protect Offerings throughout the delivery process.

iii. If Dragos provides Software or patches to Customer, Dragos shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the Software and patches to enable Customer to use the hash value as a checksum to independently verify the integrity of the Software and patches.

iv. Dragos shall use or arrange for the use of trusted channels to ship Offerings, such as U.S.

registered mail and/or tamper-evident packaging for physical deliveries.

v. Dragos shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

vi. Dragos shall demonstrate chain-of-custody documentation for Offerings as determined by Customer in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

(b) Patching Governance.

i. Prior to the delivery of any Offerings to Customer or any connection of electronic devices, assets, or equipment to Customer's electronic equipment, upon request, Dragos shall provide documentation regarding the patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for Offerings, and any electronic device, asset, or equipment required by Dragos to be connected to the assets of Customer during the provision of Offerings under the Agreement. This documentation shall include information regarding:
    1. the resources and technical capabilities to sustain this program and process such as the method or recommendation for how the integrity of a patch is validated by Customer; and
    2. the approach and capability to remediate newly reported zero-day vulnerabilities for Dragos Offerings.

ii. Unless otherwise approved by the Customer in writing, the current or supported version of Offerings supplied by Dragos shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components (*e.g.*, Java, Flash, Web browser, etc.).

iii. Dragos shall verify and provide documentation that Offerings (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to Customer.

iv. In providing the Offerings described in the Agreement, Dragos shall provide or arrange for the provision of appropriate Software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for Dragos Offerings within 60 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within thirty (30) days. If updates cannot be made available by Dragos within these time periods, Dragos shall provide mitigations, methods of exploit detection, and/or workarounds within thirty (30) days.

v. When third-party hardware, software (including open-source software), and firmware is provided by Dragos to Customer, Dragos shall provide or arrange for the provision of appropriate hardware, Software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses, if applicable to the Customer's use of the third-party product in its system environment, within 60 days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Dragos' use of the third-party product in its system environment shall be provided within thirty (30) days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested, and made available by Dragos within these time periods, Dragos shall provide or arrange for the provision of recommended mitigations and/or workarounds within 30 days.

(c) Virus, Firmware and Malware.

i. Dragos will use reasonable efforts to investigate whether computer viruses or malware are present in any Software or patches before providing such Software or patches to Customer. To the extent Dragos is supplying third-party software or patches, Dragos will use

reasonable effort to ensure the third-party investigates whether computer viruses or malware are present in any Software or patches providing them to Customer or installing them on Customer's information networks, computer systems, and information systems.

ii. Dragos warrants that it has no knowledge of any computer viruses or malware coded or introduced into any Software or patches, and Dragos will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such Software or damaging information or functionality. To the extent Dragos is supplying third-party software or patches, Dragos will use reasonable efforts to ensure the third-party will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such Software or damaging information or functionality.

iii. If a virus or other malware is found to have been coded or otherwise introduced as a direct result of Dragos' breach of its obligations under the Agreement, Dragos shall upon written request by Customer and at its own cost:

1. Take all necessary remedial action and provide assistance to Customer to eliminate the virus or other malware throughout Customer's information networks, computer systems, and information systems; and
2. the virus or other malware causes a loss of operational efficiency or any loss of data. (use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

(d) <u>End of Life Operating Systems</u>

i. Dragos-delivered solutions will not be required to reside on end-of-life operating systems, or any operating system that will go end-of-life six (6) months from the date of installation.

ii. Dragos solutions will support the latest versions of operating systems on which Dragos-provided Software functions within twenty-four (24) months from official public release of that operating system version.

(e) <u>Cryptographic Requirements</u>

i. Dragos shall document how the cryptographic system supporting the Offerings under the Agreement protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to, the following:

1. The cryptographic methods (hash functions, symmetric key algorithms, or 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. Dragos will use only "approved" cryptographic methods as defined in the FIPS 140-2 Standard when enabling encryption on its Offerings.

iii. Dragos shall provide or arrange for the provision of an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

iv. Dragos shall ensure that:

1. The system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, as may be amended.

2. The key update method supports remote re-keying of all devices within one (1) year as part of normal system operations.
3. Emergency re-keying of all devices can be remotely performed within 30 days.

v. Dragos shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

7. REMOTE ACCESS CONTROLS

Dragos shall coordinate with Customer on all remote access to Customer'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 Customer.

(a). Controls for Remote Access. If Dragos directly, or through any of its affiliates, subcontractors, or service providers, connects to Customer's systems or networks, Dragos agree to the additional following protective measures:

i. Dragos will not access, and will not permit any other person or entity to access, Customer's systems or networks without Customer's written authorization and any such actual or attempted access will be consistent with any such written authorization.
ii. Dragos 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. Dragos shall ensure Dragos Personnel accessing Customer networks are uniquely identified and that accounts are not shared between Dragos Personnel.

8. DRAGOS CYBERSECURITY POLICY

(a) Dragos will provide Customer upon request Dragos' cybersecurity policy which shall be consistent with industry generally accepted practices. Dragos will implement and comply with its established cybersecurity policy.

(b) Any changes to Dragos' cybersecurity policy as applied to Offerings provided to Customer under the Agreement and Customer Data shall not materially decrease the protections afforded to Customer or Customer Data and any material changes shall be communicated to the Customer in writing by Dragos prior to implementation.

9. PROTECTION OF CEII AND BCSI

(a) Any Customer Data labeled as CEII or BCSI must be stored under the following conditions:

i. CEII or BCSI must be stored in a specific, identified data storage location(s);
ii. Designated storage location(s) shall be encrypted;
iii. Designated storage location(s) shall be managed in such a way that all personal with access can be identified individually and their access can be managed individually;
iv. Access to designated storage location(s) shall be granted through a formal, documented approval process and only after Dragos provides attestation that the individual has passed a seven-year background check (which includes identity verification) and receipt of training on the appropriate handling and containment of Customer Data;

v. A review shall be conducted on a calendar semi-annual basis to ensure that all individuals with access to designated storage location(s) have the appropriate records as specified in subsection (d) above and a continuing need for that access; and
vi. Access to designated storage location(s) shall be removed according to the Access Control restrictions written above after the individual's termination from Dragos.

(b) Dragos shall store evidence demonstrating compliance with the requirements in this Section 9, and such evidence shall be available to Customer upon prior written request, for a period up to two years.

10. RETURN OR DESTRUCTION OF CUSTOMER DATA

Upon completion of the delivery of the Offerings to be provided under the Agreement, or at any time upon Customer's request, Dragos will return to Customer all hardware and removable media provided by Customer containing Customer Data. Customer Data in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by Customer. Dragos' destruction or erasure of Customer Data pursuant to this Section shall be in compliance with industry standard practices (*e.g.*, Department of Defense 5220-22-M Standard, as may be amended).

11. AUDIT RIGHTS

Upon prior written request, Dragos shall provide to Customer the opportunity to review a copy of Dragos' independent audit report summaries that are part of a cyber security framework (e.g. ISO-27001, SOC2). Further, to the extent Dragos utilizes any third-party services or systems for performance of the Offerings, it shall be Dragos' responsibility to review the policies, procedures, evidence and independent audit report summaries that are party of such parties' cyber security framework (e.g. ISO-27001, SOC2) to ensure such third-parties are complying with the requirements set forth herein; to the extent Dragos' identifies any issues during such review, it shall notify Customer and work with the third-party on mitigating and remedying any deficiencies.

12. REGULATORY EXAMINATIONS

Dragos agrees that any regulator or other governmental entity with jurisdiction over Customer and its affiliates may request information from Customer related to the Agreement. Upon prior written request, Dragos shall promptly cooperate with and provide information reasonably necessary for Customer to comply with any such examination.