Item 1.05 Material Cybersecurity ~~incidents~~Incidents.

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, ~~disclose the following information to the extent known to the registrant at the time of filing:~~describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.

~~(1) When the incident was discovered and whether it is ongoing;~~

~~(2) A brief description of the nature and scope of the incident;~~

~~(3) Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;~~

~~(4) The effect of the incident on the registrant's operations; and~~

~~(5) Whether the registrant has remediated or is currently remediating the incident.~~

(b) A registrant shall provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

(c) Notwithstanding General Instruction B.1. to Form 8-K, if the United States Attorney General determines that disclosure required by paragraph (a) of this Item 1.05 poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, the registrant may delay providing the disclosure required by this Item 1.05 for a time period specified by the Attorney General, up to 30 days following the date when the disclosure required by this Item 1.05 was otherwise required to be provided. Disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order.

(d) Notwithstanding General Instruction B.1. to Form 8-K, if a registrant that is subject to 47 CFR 64.2011 is required to delay disclosing a data breach pursuant to such rule, it may delay providing the disclosure required by this Item 1.05 for such period that is applicable under 47 CFR 64.2011(b)(1) and in no event for more than seven business days after notification required under such provision has been made, so long as the registrant notifies the Commission in correspondence submitted to the EDGAR system no later than the date when the disclosure required by this Item 1.05 was otherwise required to be provided.

Instructions to Item 1.05.

1. A ~~registrant shall make a~~registrant's materiality determination regarding a cybersecurity incident ~~as soon as reasonably practicable~~must be made without unreasonable delay after discovery of the incident.

~~2. Disclosure of any material changes or updates to information disclosed pursuant to this Item 1.05 is required pursuant to §229.106(d) [Item 106(d) of Regulation S-K] in the registrant's quarterly report filed with the Commission on Form 10-Q (17 CFR 249.308a) or annual report filed with the Commission on Form 10-K (17 CFR 249.310) for the period (the registrant's fourth fiscal quarter in the case of an annual report) in which the change, addition, or update occurred.~~

2. To the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under this Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

3. The definition of the term "cybersecurity incident" in §229.106(a) [Item 106(a) of Regulation S-K] ~~shall apply~~applies to this Item.

4. A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.