APPENDIX A

FORM 8-K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

B. Events to be Reported and Time for Filing of Reports.

1. A report on this form is required to be filed or furnished, as applicable, upon the occurrence of any one or more of the events specified in the items in Sections 1 -through 6 and 9 of this form. Unless otherwise specified, a report is to be filed or furnished within four business days after occurrence of the event. If the event occurs on a Saturday, Sunday or holiday on which the Commission is not open for business, then the four business day period shall begin to run on, and include, the first business day thereafter. A registrant either furnishing a report on this form under Item 7.01 (Regulation FD Disclosure) or electing to file a report on this form under Item 8.01 (Other Events) solely to satisfy its obligations under Regulation FD (17 CFR 243.100 and 243.101) must furnish such report or make such filing, as applicable, in accordance with the requirements of Rule 100(a) of Regulation FD (17 CFR 243.100(a)), including the deadline for furnishing or filing such report. A report pursuant to Item 5.08 is to be filed within four business days after the registrant determines the anticipated meeting date. A report pursuant to Item 1.05 is to be filed within four business days after the registrant determines that it has experienced a material cybersecurity incident.

* * * * *

G. Use of this Form by Asset-Backed Issuers.

* * * * *

1. * * *

(a) Item 1.05, Cybersecurity Incidents;

(b) Item 2.01, Completion of Acquisition or Disposition of Assets;

(~~b~~c) Item 2.02, Results of Operations and Financial Condition;

(~~c~~d) Item 2.03, Creation of a Direct Financial Obligation or an Obligation under an Off-Balance Sheet Arrangement of a Registrant;

(~~d~~e) Item 2.05, Costs Associated with Exit or Disposal Activities;

(~~e~~f) Item 2.06, Material Impairments;

(~~f~~g) Item 3.01, Notice of Delisting or Failure to Satisfy a Continued Listing Rule or Standard; Transfer of Listing;

(~~g~~h) Item 3.02, Unregistered Sales of Equity Securities;

(~~h~~i) Item 4.01, Changes in Registrant's Certifying Accountant;

(~~i~~j) Item 4.02, Non-Reliance on Previously Issued Financial Statements or a Related Audit Report or Completed Interim Review;

(~~j~~k) Item 5.01, Changes in Control of Registrant;

(~~k~~l) Item 5.02, Departure of Directors or Principal Officers; Election of Directors; Appointment of Principal Officers;

(~~l~~m) Item 5.04, Temporary Suspension of Trading Under Registrant's Employee Benefit Plans; and

(~~m~~n) Item 5.05, Amendments to the Registrant's Code of Ethics, or Waiver of a Provision of the Code of Ethics.

* * * * *

INFORMATION TO BE INCLUDED IN THE REPORT

Section 1 – Registrant's Business and Operations

* * * * *

Item 1.05 Material Cybersecurity Incidents.

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, 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.

(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's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident.

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] 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.

* * * * *

FORM 10-K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

J. Use of this Form by Asset-Backed Issuers.

* * * * *

(1) * * *

(b) Item 1A~~.~~, Risk Factors and Item 1C, Cybersecurity;

* * * * *

PART I

* * * * *

Item 1C. Cybersecurity.

Furnish the information required by Item 106 of Regulation S-K (§ 229.106 of this chapter).

REGULATION S-K

Subpart 229.1—General

§229.106 (Item 106) Cybersecurity.

(a) *Definitions*. For purposes of this section:

Cybersecurity incident means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Cybersecurity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Information systems means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

(b) *Risk management and strategy*. (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

(i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;

(ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

(iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.

(c) *Governance*. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

(i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

(ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

(iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Instruction 1 to Item 106(c): In the case of a foreign private issuer with a two-tier board of directors, for purposes of paragraph (c) of this section, the term "board of directors" means the supervisory or non-management board. In the case of a foreign private issuer meeting the requirements of §240.10A-3(c)(3) of this chapter, for purposes of paragraph (c) of this Item, the term "board of directors" means the issuer's board of auditors (or similar body) or statutory auditors, as applicable.

Instruction 2 to Item 106(c): Relevant expertise of management in Item 106(c)(2)(i) may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

(d) *Structured Data Requirement*. 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.

* * * * *

229.601 (Item 601) Exhibits

* * * * *

(b) * * *

(101) * * *

(i) * * *

(C) * * *

(1) Only when ~~the~~:

(i) The Form 8-K contains audited annual financial statements that are a revised version of financial statements that previously were filed with the Commission and that have been revised pursuant to applicable accounting standards to reflect the effects of certain subsequent events, including a

discontinued operation, a change in reportable segments or a change in accounting principle. In such case, the Interactive Data File will be required only as to such revised financial statements regardless of whether the Form 8-K contains other financial statements; or

(ii) The Form 8-K includes disclosure required to be provided in an Interactive Data File pursuant to Item 1.05(b) of Form 8-K; and

* * * * *