May 3, 2022

By Electronic Mail
The Honorable Gary Gensler
The Honorable Hester M. Peirce
The Honorable Allison Herren Lee
The Honorable Caroline A. Crenshaw
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chair Gensler and Commissioners Peirce, Lee, and Crenshaw:

I am pleased to transmit to you a summary of the Public Company Accounting Oversight Board's (PCAOB) Office of Internal Oversight and Performance Assurance (IOPA) performance review, titled User Access Controls Over Non-Financial Systems Review. The Board formed IOPA to promote the confidence of Congress, the Securities and Exchange Commission, and the public in the integrity of PCAOB programs and operations. IOPA conducted this review in conformance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

IOPA undertook this review to evaluate the design and operating effectiveness of user access controls over non-financial systems. As the summary sets forth, IOPA found that, in general, user access to non-financial systems was well controlled, though the enterprise has historically lacked centralized policies and procedures, and the divisions and offices have created procedures independently. IOPA identified opportunities to improve controls in the areas of:

- Standardizing user access validation,
- Expanding communication of employee terminations, and
- Further securing access to certain third-party systems used by the Office of External Affairs.

The Board has reviewed IOPA's recommendations and management's responses thereto, and has approved the transmittal of the summary to you.

Please feel free to contact the Director of IOPA, Ryan Sack, at (202) 808-1574, or me if you have any questions or would like any additional information about the review.

Sincerely,

Erica Y. Williams

Erica Williams
Chair

Enclosure: User Access Controls over Non-Financial Systems Review (IOPA Review No. 21-PCAOB-03, January 2022)

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Internal Oversight and Performance Assurance

User Access Controls over Non-Financial Systems Review

IOPA Review No. 21-PCAOB-03

January 2022

Background

The Office of Internal Oversight and Performance Assurance (IOPA) conducted a review of the user access controls over non-financial systems during the fourth quarter of 2021. User access controls over systems that contain financial data are considered and reviewed, both internally and externally, as part of the PCAOB's internal controls over financial reporting program and its independently audited financial statements. However, systems that contain sensitive, non-financial data are not necessarily considered in this program. Divisions and offices within the PCAOB use a variety of applications, databases, and SharePoint sites and subsites (hereinafter collectively referred to as "systems") to accomplish their business objectives. These systems contain a wide range of data, with classification ranging from publicly available to sensitive.

We note that the majority of the non-financial systems authenticate (or verify) incoming users using Active Directory authentication (single sign-on) or conditional authentication (i.e., access is only available via a pre-registered or PCAOB-issued device, or over a PCAOB network, etc.). These authentication methods work as a compensating control or "failsafe" as users without access to the authentication method(s) are unable to reach the PCAOB systems that utilize them. In our evaluation, we assessed the risk of any test exceptions (i.e., where a user is deemed to have a high risk of unauthorized access to a system) after considering the protection provided by existing user-authentication methods.

Objective and Scope

The purpose of our review was to evaluate the design and operating effectiveness of user access controls over sensitive data residing within non-financial systems. The scope of our review covered procedures in place as of September 2021. Our review included testing a judgmental sample of various systems utilized by nine divisions/offices within the PCAOB. To accomplish our objective, we:

1. Reviewed and reconciled inventories of systems maintained by ODST and OERM.
2. Interviewed personnel from nine divisions/offices to assess the risk associated with access to systems and judgmentally selected systems to test.
3. Obtained selected user access lists and documentation of user access reviews.
4. Validated user access lists and reviewed for inappropriate users, including terminated employees.
5. Evaluated systems for appropriate segregation of duties in role-based user access.

We conducted our review in conformance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

Summary Results and Conclusion

Generally, we found that user access to non-financial systems was well controlled, though the enterprise has historically lacked centralized policies and procedures, and the division and offices have created procedures independently. Systems with more complexity, more sensitive data, and larger user volumes tended to have more robust and refined approaches to controlling user access, while systems that served smaller groups and contained less sensitive data tended to have more ad-hoc or informal controls in place.

During the course of our review, we identified opportunities to improve control over user access to non-financial systems. The brief table below summarizes and categorizes the audit observations on a risk scale[1].

Low Risk (1)	Moderate Risk (2)	Significant Risk (0)	Material Risk (0)

Our observations are briefly described below –

● ***Standardize Approach to User Access Validation –*** We noted that divisions and offices have implemented a variety of approaches to granting access for new users, maintaining related documentation, and conducting periodic user access reviews. While the timing and rigor of the processes employed generally correspond to the complexity of the individual systems, the retention of surrounding documentation is often ad hoc or informal.[2]

We recommend that the Chief Information Security Officer (CISO) finalize an emerging enterprise standard for system user access control ("access control policy,") addressing controls and documentation standards related to the addition of new users, changes to existing user access, and periodic user access review.

● ***Expand Communication of Employee Terminations –***We observed that certain system administrators were not included in the distribution of the Human Resource communications related to terminated employees and may not be aware that user access needs to be terminated.

We recommend that the CISO, in coordination with divisions/offices, identify appropriate system administrators to include in the HR termination email distribution. Also, we recommend the access control policy consider and establish any further controls that might assist system administrators in promptly terminating employee access and conducting meaningful user access reviews.[3]

● ***Secure Access to Certain Third-Party Systems Used by Office of External Affairs (OEA) -*** We found that access information related to certain third-party systems used by OEA was accessible by all employees in OEA on a shared Excel spreadsheet.

We recommend that OEA limit the access information to only users who have a business need to access such systems and consult with the CISO on any additional safeguards.

The CISO and the director of OEA provided responses indicating concurrence with our audit observations and a commitment to corrective actions that are responsive to our recommendations.

We thank all personnel who supported our review, both at the senior management and staff operating level, for their courtesy and cooperation throughout this assessment.

[1] See Appendix A for IOPA Risk Rating Legend.
[2] Complexity refers generally to the size of the system in terms of the total number of users, the existence of users from multiple divisions and offices, and the need for diversified assignment of users to compartmentalized data withing the system.
[3] For example, we noted a recent draft of the emerging User Access Control policy referred to a monthly terminations report that would be a helpful resource in the proper inactivation of terminated users and periodic user access reviews.

APPENDIX

Appendix A – Risk Classifications and Definitions

To provide the reader with further perspective of the degree of risk IOPA attributes to each audit observation, we have assigned color-coded risk ratings as explained in the legend below.

Degree of Risk and Priority of Action	
Material	The degree of risk is unacceptable and poses a significant level of financial, compliance or operational risk to the organization. As such, complete remediation is generally required within one month from the time of the finalized IOPA report.
Significant	The degree of risk is undesirable and poses a significant financial, compliance or operational risk to the organization. As such, complete remediation is generally required within three months from the time of the finalized IOPA report.
Moderate	The degree of risk is undesirable and poses a moderate financial, compliance or operational risk to the organization. As such, complete remediation is generally required within six months from the time of the finalized IOPA report.
Low	The degree of risk appears reasonable but there are opportunities to further reduce risk through improvements to existing policies, procedures, and/or operations. As such, management should take actions to reduce the risks to the organization.

IOPA used its professional judgement in determining the overall ratings presented in the Summary Results and Conclusion section of this report. The report is intended to provide management with information about the condition of risks and internal controls at a point in time.