PCAOB
Public Company Accounting Oversight Board

1666 K Street, N.W.
Washington, DC 20006
Telephone: (202) 207-9100
Facsimile: (202) 862-8430
www.pcaobus.org

November 13, 2007

The Honorable Christopher Cox
Chairman
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chairman Cox:

I am pleased to transmit to you a summary of the Public Company Accounting Oversight Board's most recent performance review, conducted by the Board's Office of Internal Oversight and Performance Assurance. The Board formed IOPA to provide the Board, the Securities and Exchange Commission, and others assurance that the PCAOB is achieving the objectives of Title I of the Sarbanes-Oxley Act in an effective manner. IOPA conducts its reviews in conformance with Government Auditing Standards issued by the Comptroller General of the United States.

This report summary discusses security policies and procedures the Board has in place to protect the PCAOB's information, assets, and personnel. Given the strategic importance of these issues, IOPA conducted the review to determine whether the PCAOB had defined and was meeting its business requirements for security.

The Board intends to publish the attached summary on the PCAOB's Web site on or about November 20, 2007. You and your staff should feel free to contact me or the Director of IOPA, Peter Schleck (202-207-9115), if you have any questions or would like any additional information about the review.

Sincerely,

Mark W. Olson
Chairman

cc: The Honorable Paul S. Atkins
The Honorable Annette L. Nazareth
The Honorable Kathleen L. Casey

PCAOB
Public Company Accounting Oversight Board

1666 K Street, N.W.
Washington, DC 20006
Telephone: (202) 207-9100
Facsimile: (202) 862-8430
www.pcaobus.org

PERFORMANCE REVIEW

THE PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD'S SECURITY POLICIES AND PROCEDURES (IOPA-2007-002)

INTERNAL OVERSIGHT AND PERFORMANCE ASSURANCE
November 13, 2007

Objective

One of the strategic goals of the Public Company Accounting Oversight Board (PCAOB) is to operate in a manner that recognizes the Board's public mission and responsibility to exercise careful stewardship over its resources. As articulated in the Board's strategic plan, an action intended to help achieve this goal is the development of a framework for identifying and monitoring operational and reputation risks to the organization. Such a framework should include, in our judgment, a comprehensive approach to ensuring that information and assets entrusted to the PCAOB are adequately protected from theft, other loss, or misuse. Likewise, an effective risk framework would also consider the safety and well-being of PCAOB employees.

Given the strategic importance of these issues, Internal Oversight and Performance Assurance (IOPA) conducted a review[1/] to determine whether the PCAOB has defined and is meeting its business requirements for security. For purposes of this review, we defined security broadly, to include information security, physical security, and the protection of employees.

Background

Title 1 of the Sarbanes-Oxley Act of 2002, which established the PCAOB, contains a number of explicit references to the protection of information. For example:

[1/] This is a public summary of the report. The full report, prepared in accordance with Government Auditing Standards, has been issued to the Board. The full report includes a detailed discussion of the review objective, scope, and methodology.

PERFORMANCE REVIEW

- 102(e) requires the protection of proprietary information contained in registration applications;

- 104(f) discusses protecting confidential information provided by accounting firms in response to inspection reports;

- 104(g)(2) discusses protecting criticisms or defects in quality control systems at accounting firms if those criticisms or defects are addressed within 12 months of the inspection report; and,

- 105(b)(5)(A) addresses confidentiality of documents and information prepared or received by the Board in connection with inspection and enforcement activities.

Although Title 1 does not explicitly address physical security, a number of references discuss the Board's powers, authorities, and responsibilities to do all things necessary for or incidental to operations and administration.

Based on these provisions of the Act, as well as language in PCAOB's bylaws, rules, and ethics code, it is clear that the PCAOB has the responsibility to protect confidential information and the authority to establish other security considerations, policies, or processes deemed necessary or appropriate to conduct its operations and meet its responsibilities.

Standards and Benchmarks

The International Organization for Standardization (ISO) has published ISO 17799, describing it as a comprehensive set of controls comprising best practices in information security. The standard gives recommendations on information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organizations. It is intended to provide a common basis for developing organizational security standards and effective security management practices. The standard is organized in 10 different sections:

- Security policy
- System access control
- Computer and operations management
- System development and maintenance

PERFORMANCE REVIEW

- Physical and environmental security
- Compliance
- Personnel security
- Security organization
- Asset classification and control
- Business continuity management

The ISO standard is referenced in a policy document generated by the PCAOB's OIT. Moreover, the former Chief Information Officer (CIO) told us that ISO 17799 is the key information security standard. In his view, the standard provides a management methodology that can be scaled, as appropriate, to fit a given organization.

The National Institute of Standards and Technology (NIST) also publishes recommended security controls for federal information systems. Although these standards are intended primarily for agencies of the federal government, a mapping between NIST and ISO standards demonstrates that similar terminology is used and that most individual security controls are addressed by both standards-issuing organizations.

As part of our review, IOPA interviewed security professionals at the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA).[2/] Our purpose in doing so was to explore and benchmark best practices employed by regulatory entities charged with protecting information that may be similar or analogous to that which the PCAOB must safeguard. We also discussed the protection of facilities, other assets, and employees with representatives of these organizations. Officials at both SEC and FINRA cited NIST standards. FINRA's security professionals also described ISO 17799 as a "backdrop" for that organization's overall security program.

Security Initiatives at the PCAOB

Security responsibilities within the PCAOB are vested with the Office of Information Technology (OIT) and the Facilities Office (Facilities) within the Office of

---

[2/] At the time of our fieldwork, the FINRA officials we spoke to were part of FINRA's predecessor organization, the National Association of Securities Dealers.

PERFORMANCE REVIEW

Administration. Both of these offices report to the Interim Chief Administrative Officer (CAO).

Since inception, the PCAOB has established a number of measures to ensure the security of its information, facilities, and employees. Such measures included:

- Drafting of a number of policy-type documents. OIT, Facilities, and Inspections have all developed written procedures covering various aspects of security. OIT, for example, drafted proposed PCAOB-wide policies for acceptable use of information technology and data classification. OIT also developed procedures for handling the loss of laptops and other security-related incidents.

  Similarly, Facilities developed documented procedures for issuing identification badges and securing PCAOB work spaces. In addition, at the time of IOPA's review, Inspections had drafted an incident management plan for the benefit of its inspectors traveling on official business in foreign countries.

- Staffing various information- and physical-security related positions. As of August 2007, OIT had 8 employees in security-related positions (out of a total staff of 70 as of August 2007), including security operations engineers, network engineers, and applications security engineers. In addition, Facilities was seeking to fill a physical security manager position that had been vacant for several months.[3/]

- Implementing numerous information technology security processes and protocols. Such protocols include network password protection, vulnerability scanning, virus detection and prevention, and multi-layered firewalls. In 2006, OIT also deployed a new remote access system to enhance security.

- Ensuring that such physical security measures as smart badges and video monitoring are used to help ensure the safety of employees and the protection of assets. At Headquarters and field locations we visited, we also noted that additional controls were in place in areas where sensitive information was stored, used, or processed.

[3/] At the time of our review, the Facilities Director maintained responsibility for physical security.

PERFORMANCE REVIEW

- Continuing work on other related initiatives, including an emergency communications protocol and security awareness training.

Results of Review

While the security practices we observed were generally consistent with the cited industry standards and with approaches adopted by the other regulatory entities IOPA consulted, the PCAOB's overall approach to security needed to be more effectively communicated. We observed inconsistencies regarding the status and enforcement of written policies and procedures; a lack of clarity, in some instances, as to roles and responsibilities; and a need for better communication of the organization's security strategy. Resolution of the inconsistencies we noted may help to ensure an effective security program. As such, IOPA made recommendations to the Interim CAO intended to help facilitate related communication and coordination.

In responding to a draft of this report, the Interim CAO agreed that PCAOB security-related activities could and should be better coordinated, that more information and training should be provided to staff, and that security policies should be updated. With regard to IOPA recommendations, the Interim CAO specifically committed to:

- Scheduling a Board discussion of the PCAOB's security program;
- Summarizing the security framework in a format that can be referenced by all employees;
- Overseeing a review of current security policies and procedures; and
- Dedicating a portion of the PCAOB's intranet-based electronic exchange to security matters.

The Interim CAO also stressed that the PCAOB is committed to providing a secure work environment for all staff. She noted that the essential elements of an effective security framework – a framework that meets statutory requirements and is consistent with widely-used operations risk management practices – are in place. In her comments, the Interim CAO summarized the PCAOB's physical security protections, as well as its information technology and network security infrastructure.