January 16, 2004

Office of the Secretary
PCAOB
1666 K Street, N.W.
Washington, D.C. 20006-2803.

Also submitted via e-mail to comments@pcaobus.org

Re: Public Company Accounting and Oversight Board (PCAOB)
Proposed Auditing Standard On Audit Documentation And Proposed Amendment To Interim Auditing Standards.
PCAOB Release No. 2003-023
November 21, 2003
PCAOB Rulemaking
Docket Matter No. 012

Dear Sirs:

Thank you for the opportunity to comment on the PCAOB's Proposed Auditing Standard referred to above. We have read the PCAOB's Briefing Paper on the Proposed Auditing Standard, the PCAOB's Audit Documentation Roundtable (September 29, 2003), and the proposed standard. We applaud the PCAOB's efforts to fulfill their mission in implementing the Sarbanes-Oxley Act of 2002, and believe the proposed standard will improve the practice of auditing and the quality of audits. In my opinion, the standard is an improvement over SAS 96, the current professional standard governing audit documentation, because it is more clearly written and states in no uncertain terms the auditor's obligation for documentation of the work performed.

We agree with the PCAOB's adopting the substance of the Government Accounting Office's (GAO) documentation standard for government and other audits conducted according to generally accepted auditing standards (GAGAS), which state that "audit documentation should contain sufficient information to enable an experienced auditor who has had no previous connection with the audit to ascertain, from the audit documentation, the evidence that supports the auditor's significant judgments and conclusions." as well as the California statute on audit documentation, which creates a rebuttable presumption that the failure to document work performed indicates that the work was not performed.

In regard to the rebuttable presumption, some of the panelists in the September 29, 2003 roundtable were of the opinion that verbal explanation should be allowed if audit documentation failed to provide evidence that the work was performed or support the conclusions reached. We strongly disagreed with these panelists because allowing verbal explanation to support the conclusion will open the door for abuse if the auditors are allowed to not document their work but verbally claim after the fact that they did do the work.

My area of expertise is internal control, information technology (IT), and information security (InfoSec), and the remainder of my comments will address the relevant portions of the proposed standard affected by IT and InfoSec. In particular, We will address issues regarding:

- Maintaining audit documentation;
- Who prepared, reviewed, or changed audit documentation;
- The date audit documentation was prepared, reviewed, or changed;
- Retaining audit documentation;
- Subsequent changes to audit documentation.

The basic assumption of my comments is that today's audit documentation is almost entirely digital rather than hardcopy paper, and audit documentation in pen (or pencil) and paper is prepared by a very small minority of auditors of small issuers. Audit documentation is currently created and maintained digitally with audit documentation software, desktop software, and other computer applications. The movement from hardcopy paper to digital is nearly universal in almost all companies and audit firms. When reviewers or regulators review hardcopy audit binders they are only looking at "views" of digital data[1], which may have been fraudulently created especially for them with the intent to deceive. The transition from pen, ink, and paper to digital has turned important elements of the audit documentation paradigm on its head, such as the integrity of such documentation, the ability to determine who created it, and the ability to determine when it was created. It is important that the PCAOB and the auditing standards recognize this profound shift. The balance of my comments will first discuss some background information and then address specific issues in the proposed standard related to digital audit documentation and the need for information security controls over it.

BACKGROUND

Today, ninety-three percent of all business records are estimated to be in digital forms[2] and "almost all 'source data' now generated by enterprises is electronic or digital in nature and not physical. A University of California study conducted in 2000 has shown that 99.993% of the 3 billion gigabytes of data generated worldwide is computer generated. It is also clear that almost all enterprise source data for operations, accounting, audit, financial reporting and other purposes are digital, and have no paper and ink parentage."[3]

Since audit documentation is composed of business records and since auditors almost universally use computers to document and store evidence of their work, it stands to reason that a similar percentage of audit documentation is digital. Maintaining records means keeping the records in existence and preserving them. Since audit documentation

[1] Paul, G, H. Kesterson II, C. Merrill, and B. Nearon. "Views of Digital Data," Treatise on Digital Evidence. American Bar Association Information Security Committee, forthcoming.
[2] Lange, M. 2003. "Electronic Evidence & The Sarbanes-Oxley Act of 2003." *Kroll On Track*. http://www.krollontrack.com/LawLibrary/Articles/sarbanes.pdf.
[3] Nearon, B., J. Stanley, S. Teppler, and J. Burton. "Life After Sarbanes-Oxley: The Merger Of Security And Accountability." Working Paper. December 2003.

is most likely maintained with information technology, to maintain its existence and preserve it would require adequate information technology controls. Information technology controls in this context means information security controls. Specifically, as it applies to audit documentation, the relevant information security controls are:

- Controls to unambiguously determine *who* created, changed, or reviewed audit documentation.
- Controls to unambiguously determine *when* the audit documentation was created, changed or reviewed.
- Controls over *availability*.[4]
- Controls over *integrity* of the audit documentation and changes to it; integrity meaning the audit documentation remains intact and unchanged since the final set of audit documentation is assembled for retention. (Ordinarily, which should not be more than 45 days after the auditor grants permission to use the auditor's report,)[5] or if changes are made there are controls over such changes.[6])

SPECIFIC COMMENTS

Content of Audit Documentation

¶ 4 "Audit documentation ordinarily consists of memoranda, correspondence, schedules, and other documents created or obtained in connection with the engagement and may be in the form of paper, electronic files, or other media."

The audit standards need to recognize that audit documentation is most likely in the form of electronic files, that original paper audit documentation is a rare exception, and that paper audit documentation is most likely only one of many possible "views" of the original underlying digital audit documentation. The underlying digital data used to assemble the "views" of audit documentation is an ordered assembly of 0s and 1s and is unobservable to the human eye. As stored in memory or storage the 0s and 1s of a valid audit document appear indistinguishable from a fraudulent document, a digital photo, or a digital music file. Layers of software are used to construct the "views" of the audit documentation and software in common desktop computers used by auditors may consist of millions of lines of computer code and ten of thousands of files. Without information security controls over the operating system, programs, and files that create and display "views" the integrity of audit documentation being viewed is suspect.

¶ 5. "Audit documentation must contain sufficient information to enable an experienced auditor, having no previous connection with the engagement:

[4] PCAOB Proposed Auditing Standard On Audit Documentation And Proposed Amendment To Interim Auditing Standards. PCAOB Release No. 2003-023. Id. ¶ 13. Audit documentation must be retained for seven years from the date of completion of the engagement, as indicated by the date of the auditor's report, unless a longer period is required by law.
[5] Id. ¶ 14
[6] Id. ¶ 15

a. To understand the nature, timing, extent, and results of the procedures performed, evidence obtained, and conclusions reached, and
b. To determine *who performed the work* and *the date such work was completed* as well as *the person who reviewed the work* and *the date of such review*."

My comments for ¶ 5 focus on determining the "who" – who performed and reviewed the work, and the "when" – the date the work was performed and reviewed. This is not a trivial issue when it comes to digital documents, because without appropriate information security controls over digital audit documentation the "who" and "when" are not determinable with reasonable certainty.

Determining Who Prepared and Reviewed the Audit Documentation

Prior to the migration from ink (or pencil) and paper audit documentation to digital audit documentation, the "who" was determined by the auditor and reviewer evidencing their work by initialing or signing the documents. Forgeries of another person's initials or signature created in pen and ink are quite often obvious to untrained people and advances in forensic technology has made such forgeries easily detected by experts. Digital audit documentation is often signed-off by electronically initialing documents, and in some instances may legally bind the signer;[7] however, without appropriate information security controls, such electronic initialing offers no certainty as to the identity of the signer. It is a trivial exercise to forge another's electronic initials and without appropriate information security controls it is virtually impossible even for an expert to detect such a forgery. Therefore, without appropriate information security controls it is not possible to determine with reasonable certainty who prepared or reviewed digital audit documentation.

The forgery of an auditor's or reviewer's initials without detection is a very real possibility given the ease of doing this. Audit firms involved in accounting malpractice lawsuits, failed audits, litigation, and government enforcement actions have a powerful incentive to commit such forgeries and, as stated above, without appropriate information security controls such forgeries are not easily detected.

Therefore, we recommend that the auditing standard include a requirement that sign-off by auditors or reviewers of digital audit documentation be executed using Public Key Infrastructure (PKI) and digital signatures or equivalent technology.[8] Presently, PKI is a mature proven technology that can be cost effective when implemented for large groups of users. The "Big 4" accounting firms could certainly afford such a technology when spread across their large employee base. For smaller firms, professional accounting associations or even the PCAOB could offer their members digital signatures at a nominal charge. The use of PKI and digital signatures or equivalent technology would limit forgery of auditor and reviewer sign-off and allow users of digital audit

[7] *See*, Electronic Signatures In Global And National Commerce" 15 U.S.C. Sec 7000

[8] A useful reference work dealing comprehensively with PKI and PKI legal applications is ABA Information Security Committee, *Digital Signature Guidelines* (2001), <available at http://abanet.org/scitech/ec/isc/>. For a recent report dealing with PKI use in the U.S. Federal Government, see GAO, *Information Security – Status of Public Key Infrastructure Activities at Major Federal Departments and Agencies <available at. http://www.gao.gov/new.items/d04157.pdf.>*

documentation to determine with reasonable certainty the identities of the preparer and reviewer.

Determining When the Audit Documentation Was Prepared and Reviewed

When audit documentation was prepared in pen and paper, the auditor manually and contemporaneously inscribed the date the work was done or reviewed. If this were done after-the-fact within a reasonable amount of time, a fraudulent date would be almost impossible to detect even with advanced forensic techniques. It would take special forensic investigative techniques to detect such a fraud.

Today, the auditor or reviewer often dates digital audit documentation by manually entering a date on a digital audit document, or the entry of the date may be automatically made by audit documentation software using the computer system's time clock. Like the discussion of the "who", audit firms involved in accounting malpractice, litigation or government enforcement action have a powerful incentive to make it appear that work that was not done during the audit was actually done during the audit. It is a trivial exercise to manually backdate a digital document or reset the system time clock and it requires no special skills. This is not just a hypothetical, theoretical, or remote risk, considering that there have been several accounting frauds perpetrated in this manner. For example, see the SEC cases of Sensormatic,[9] Mortell,[10] and Newman[11] where management reset the system time clock to move income from a subsequent period to the audit period. Without controls over the system time clock in a like manner an audit firm that did not perform or review audit work prior to the release of the audit report could create audit documentation after-the-fact and backdate it. Without information security controls over the system time clock on computers used to prepare digital audit

[9] "In the Matter of Thomas H. Pike, Securities Exchange Act of 1934," Release No. 39793. (Mar. 25, 1998) ("At the end of each quarter, Sensormatic turned back the computer clock that dated and recorded shipments. Based on these computer-generated documents reflecting shipments, Sensormatic then prematurely recognized revenue on shipments made past the end of the quarter.") David Priebe. "Corporate Governance Reform and Electronic Documents." Forthcoming in *The American Bar Association Information Security Committee's Treatise on Digital Evidence*.

[10] *Securities & Exch. Comm'n v. Mortell*, No. 1:02 CV 01090 (RW) ¶ 32 (D.D.C. 2002). (http://www.sec.gov/litigation/complaints/complr17542.htmt. ("Under [a defendant's] supervision, PCN's shipping department reset the computer clock that dated certain shipping records and generated shipping documents bearing false shipping dates. The documents indicated that certain products were shipped by year-end 1996, when they were actually shipped during the first few days of 1997.") David Priebe. Forthcoming in The American Bar Association Information Security Committee's Treatise on Digital Evidence.

[11] *Securities & Exch. Comm'n v. Newman*, No. SA CV-00-948-GLT (Eex) C.D. Cal. Nov. 5, 2001. http://www.sec.gov/litigation/litreleases/lr17250.htm. (Summary judgment granted against officer in case alleging that officer ordered "resetting the date on Sirena's computer clock to March 30 or March 31. Manipulation of the computer clock allowed April shipments to be recorded as March revenue because the computer clock controlled the date that was printed on the company's invoices. The computer system also automatically recorded revenue earned as of the date of the invoice. In this way, [the defendants] held the March 1999 quarter open until April 12, 1999."). David Priebe. Cited in "Corporate Governance Reform and Electronic Documents." Forthcoming in The American Bar Association Information Security Committee's Treatise on Digital Evidence.xx

documentation, back-dating of audit documentation would be trivial to accomplish even by novices and difficult to detect by experts.

Therefore, We recommend that the auditing standards include a requirement that there be information security controls over the system's time generating device (the system time clock) on computers that are used to generate audit documentation so that the date the audit documentation was prepared or reviewed could be determined with reasonable certainty.

Determining the Content Integrity of the Audit Documentation from Time of Creation through Review

Information is an enterprise's most valuable asset, and this asset is now electronically generated as source data. Without some time reference and content anchor, however, digital records, as well as paper records originating therefrom, have little or no real substantive value if the binary data (organized sets of zeroes and ones) cannot be authenticated for the content it purports to provide auditors. During the life-cycle of data content, therefore, we propose that an identity independent trusted timestamping process be required to authenticate electronic content relevant to this proposed standard.

All financial and other business transactions, communications, and business records are ultimately time based and time dependent. Time plays a critical part in the everyday processes and operations of the business world, and accordingly in the generation, management and retention of documents used in connection with the audit process.

In the old days, physical records were recorded, and some time references (i.e., a raised impression and/or ink stamp, or other mark) would be affixed to a paper and ink physical record. If the record or the timestamp were tampered with, or forged after the fact, a wide array of forensic tools could be used to ascertain the genuineness of either the record or the notation of the time it was created.

Paper based forensics, which once provided sufficient means for determining the provenance of paper and ink source documents, is now woefully inadequate to the task of authentication.

There exists, therefore, a significant new issue and vulnerability arising from the aforementioned migration of source data to digital or electronic format. The issue is one of content authentication, i.e., relating to a strong binding of the "when" and the "what." The vulnerability is the system clock of the covered entity, and it's susceptibility to tampering by insiders. Content integrity authentication processes can operate irrespective of and must operate independent of any identity based authentication schema.

An unscrupulous insider can modify, substitute or destroy existing data and by resetting the system clock to an earlier time, can cover their tracks, completely and without any way to "audit" back to ascertain what is real, and what is not.

Accordingly, it is clear that with the onset of electronic data as source records for business and government enterprise, there has arisen a vulnerability unique to electronic data that has not yet been addressed, and that is the issue of time-based data manipulation. Witness the unfolding Parmalat scandal, in which the CEO, the CFO, with the alleged complicity of auditors, used time-based digital data manipulation to create a forged document purporting to substantiate the existence of more than 4 billion dollars in a Bank of America account. In late 2003 a former audit partner from Ernst & Young was charged by the SEC with criminally destroying and altering audit workpapers related to a federal examination of NextCard, a former online credit card company that is being liquidated in a 400 million dollar bankruptcy. The charge stated that the auditors accessed workpapers contained in an archive and revised them. The revised versions were saved, and original workpapers were deleted. To ensure that the computer did not record the revisions as "after the fact" the team reset the internal clock on their computer to make an earlier date appear. Similar tactics were used by the auditors and attorneys involved in the Enron scandal.

The problem with such time-based digital data manipulation is that it is most often employed by "trusted insiders" such as CEO's CFO's and auditors, and not discovered until the cow has long since left the barn. For instance, if a trusted time-stamping schema had been required for use by auditors for Parmalat, the source of the forged document would have immediately exposed the fraud. Routine scans of time-stamped digitized information used in the audit process would uncover, on an immediate basis, and data tampering by insiders.

Cases of such insider initiated time-based data manipulation are increasingly being uncovered in the US due to greater scrutiny on corporate governance and it is our opinion that the spirit and intent of Sarbanes-Oxley, as well as the rules promulgated thereunder, should encompass the adoption of processes for "new age" technologies that protect against "old-time" fraud. Act and the realization that electronic data that are comprised of zeroes and ones, and are not physical in nature are really very easily manipulated. No auditor, CEO, or technology expert can read binary data and interpret them as a spreadsheet, an email or database table element.

System clocks are essentially untrusted time sources, and what are generally considered "time-stamps" are human-manipulatable data strings. If the organization that creates or manages the audit data can also alter the system clock, the data is untrustworthy. Where insider control over network time exists, the capability for digital data fraud exists. In the United States, other data-protection oriented laws (Gramm-Leach-Bliley and HIPAA) both require that data integrity be maintained on a continuing basis and be protected from internal as well as external attack.

This weakness in the data generating process may result in a material misrepresentation sufficient to call into question the certification of authenticity, and place both the certifier as well as the auditor in peril. Further, this vulnerability could affect the admissibility and weight of the data as digital evidence.

The solution to this relatively new, largely undetectable, but growing problem is independent trusted time-stamping technologies. Indeed, the issue has been well recognized in the United States by the American National Standards Institute (ANSI) that formulates security standards for the financial services industry and is working on the new American National Standard X9.95 Trusted Time Stamps.

Trusted time-stamping removes the risk of undetectable data tampering, manipulation, alteration or deletion by "trusted" insiders, and so removes twin vulnerabilities; insider exploitation of the lack of sufficient controls and legal challenges to data authenticity. It also provides an enterprise with the benefit of transparency and immediate fraud detection in the data and data audit trails that it does generate.

The risk inherent in not adopting a digital data trusted timestamping requirement is not that fraud will escape undetected. Detected it will be, but only after the fact, i.e., after the money has disappeared, and in all likelihood after any possibility of recapture, reversal, or meaningful restitution to investors. The costs of implementation of this technology are far outweighed by the forward-looking protection afforded investors in public companies. The investing public simply should not be exposed to another round Parmalat, Enron, Rite-Aid, Sirena, NextCard frauds resulting from time-based data manipulation, and we believe that the intent and spirit of both Sarbanes-Oxley as well as the rules promulgated by this Board mandate the prevention of such occurrences in the future.

We therefore recommend that the auditing standards be drafted to include a requirement that digital information that may be used in connection with the audit process be time-stamped using a trusted-timestamp schema.

Retention of Audit Documentation

¶ 13. "Audit documentation must be retained for seven years from the date of completion of the engagement, as indicated by the date of the auditor's report,[12] unless a longer period of time is required by law."

Audit documentation that was created in pen and ink on paper was relatively easy to retain. It was bound, identified on the covers, indexed, boxed, and stored in secure file rooms or by record storage providers. In such form, audit documentation was easily located, retrieved, and available for reading by those that needed it. An individual physical work paper could be easily destroyed, but it would take great effort or a catastrophic event, such as a fire, natural disaster, or act of terrorism to destroy a whole set of work papers.

Retention of digital audit documentation is almost completely different than retention of hardcopy documents. First, the storage media itself, whether it is magnetic tape, compact disc, or hard-drive, is subject to minor physical damage and deterioration that could

[12] PCOAB Footnote 3. If a report is not issued in connection with an engagement, then the date of completion of the engagement would be the date that fieldwork was substantially completed.

render the media completely unreadable. Second, digital documents are often stored in specific technology formats that only work with specific software, specific versions of software, and specific hardware. Computer software and hardware is subject to Moore's Law, a generally accepted theory, which posits that computer processing power doubles every two years. Moore's law has held for the last fifty years and is expected to hold for the foreseeable future. The effect of Moore's law is that software and hardware are often obsolete within two years of purchase. Given the retention requirement of the proposed standard, it is likely that much of the digital audit documentation created today will be unreadable by software and hardware in use seven years hence, or even less.

Therefore, with respect to the easily damaged nature of the media used to store digital records, we recommend that the auditing standards require that audit firms to maintain at least two copies of digital audit documentation. With respect to the obsolesce of computer technology, we also recommend that when audit firms upgrade their software and hardware used to prepare audit documentation they be required to maintain compatible software and hardware capable of reading the original digital audit documentation for the required retention period.

Integrity of the Audit Documentation (Changes to Audit Documentation)

¶ 14 "A complete and final set of audit documentation must be assembled for retention within a reasonable period of time following the first time the auditor grants permission to use the auditor's report in connection with the issuance of the company's financial statements."

¶ 15 "Audit documentation must not be deleted or discarded; however, information may be added, including an explanation of its relevance, as long as the information identifies the date the information was added; by whom it was added; and the reason for adding it."

When audit documentation was in pen, ink (or pencil) and paper form, it would be difficult to insert whole workpapers within a set of workpapers after-the-fact due to the indexing system. Such insertions would be obvious unless great care was taken. Likewise deletions would also be obvious leaving gaps in the indexing system and hanging work paper references that led nowhere.

With digital audit documentation, the insertion, deletion, or change of workpapers after-the-fact is a trivial exercise with slight chance of detection without appropriate information security controls. Changing a digital audit document or deleting it entirely is as easy as point and click. Software such as Evidence Eliminator[13] makes the job even easier and more effective. As indicated previously, audit firms subject to litigation or government enforcement action have a powerful incentive to commit such fraud. The fact that it is easy and there is little chance of getting caught makes the fraud more likely.

Therefore, with respect to the integrity of the audit documentation to reasonably ensure that changes made after 45 days are detected, we recommend that the auditing standards

[13] Evidence eliminator is a software product to assist a PC user in wiping files from their computer and purports to defeat forensic software. See http://www.evidence-eliminator.com/

require that digital audit documentation be sealed with a combination of PKI and digital signature technology and secure computer time stamping technology. Such technologies would make it difficult to alter audit documentation after-the-fact without detection and provide reasonable assurance that the audit documentation has been unchanged from the date it was finalized and digitally sealed.

The above comments are ours personally and have not been approved by our Firms, nor should they be attributed to it. We would be glad to further discuss the proposed auditing standard and answer questions regarding my comments and may be reached at 973-871-4035.

Respectively submitted,

Bruce H. Nearon, CPA
Director of Information Technology Security Auditing
J.H. Cohn LLP
10 Sylvan Way
Parsippany, NJ 07054

Steven Teppler, Esq. CEO
TimeCertain LLC
5715 Firestone Ct.
Sarasota, FL 34238

Charles R. Merrill, Esq.
McCarter & English LLP
Four Gateway Center
100 Mulberry Street
Newark, NJ 07102-4096