13650 Dulles Technology Dr. Suite 500
Herndon, VA 20171-4601

T +1 703.480.8510
F +1 703.480.8440

September 15, 2006

Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090
Attn: Nancy M. Morris
Secretary

Re: File Number S7-11-06

Gentlemen:

Cybertrust appreciates the opportunity to comment to the Securities and Exchange Commission (SEC) regarding Concept Release 34-54122. As the leading independent global information security company, Cybertrust represents more than 1,600 clients worldwide across industries, including financial services, telecommunications, retail, pharmaceutical, government, energy and utilities, and computer services industries. Of our commercial customers, many are publicly traded companies, and therefore subject to the provisions of the Public Company Accounting Reform and Investor Protection Act of 2002, commonly referred to as Sarbanes-Oxley or SOX.

As the Commission prepares its Section 404 guidance for filers, it has the opportunity to clarify a host of lingering compliance issues for accelerated filers, as well as ease the compliance burden for small and micro-caps. Since 2003, the costs associated with pre-audit consulting and remediation activities, in addition to audit fees, have been exorbitant. Some accelerated filers have had the resources to absorb these costs, and many have acknowledged that as their compliance activity matures, they have seen costs decrease slightly. Small and micro-caps, however, are only beginning their compliance activities; historically, implementation projects and first-year filings are the most burdensome. Most of these organizations do not have the resources to readily absorb these costs and continue to do business profitably.

At the hearing on May 10, the Commission expressed its reluctance to provide regulatory relief through additional rulemaking, or create a carve-out for small business. Cybertrust agrees that a carve-out based on revenue or market capitalization would be essentially arbitrary, and that in keeping with the spirit of the law, all publicly traded companies must be held to a uniform standard of corporate governance in order to protect investors.

Cybertrust therefore urges the Commission to relieve the regulatory burden on small and micro-caps through guidance, and at the same time, allow accelerated filers to streamline their compliance management activities. Non-binding implementation and management guidance can create strata for filers of various sizes, and associated levels of performance, without arbitrarily favoring or being punitive toward one or more classes of public company.

Cybertrust has reviewed the Concept Release, and considered those questions that relate specifically to IT General Controls. In response to those specific questions raised in the Concept Release:

> Question 1: Would additional guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting be useful? If so, would additional guidance be useful to all reporting companies subject to the Section 404 requirements, or only to a sub-group of companies? What are the potential limitations to developing guidance that can be applied by most or all reporting companies subject to Section 404 requirements?

Response: On May 16, 2005, the Public Company Accounting Oversight Board (PCAOB) issued guidance on Section 404. Although widely read by filers, there was very little that a filer could practically apply from that document when trying to implement, manage and monitor its control measures. This was due to the fact that this guidance was created for the benefit of the profession, as clarification for Audit Standard No.2 for auditors, to use when evaluating a company's internal control structure.

Filers would benefit from guidance designed to address management's challenges when designing the internal control structure, managing and monitoring individual controls, and most particularly, demonstrating that controls in place are functioning effectively. The guidance must be comprehensive, and address all reporting companies subject to Section 404 requirements; using the experiences of the accelerated filers in creating illustrative examples in the guidance also has the potential to benefit those companies just beginning their compliance activity.

> Question 3: Should additional guidance be limited to articulation of broad principles or should it be more detailed?

Response: The guidance issued by the Commission must be more detailed. One of the major problems experienced by the accelerated filers was the interpretation of the broad principles articulated in Section 404 itself, the COSO framework, Audit Standard No. 2, the May 16 guidance, and even CobiT. All these documents are subject to interpretation, both by the public companies that must implement as well as the public accounting firms retained to evaluate compliance of an organization. It was this interpretation, particularly on the part of the public accounting firms, that was the cause of dramatic expenditures in the first two years of reporting for the accelerated filers.

There have literally been hundreds of "horror stories" from accelerated filers required to document and/or implement thousands of key controls, or make dramatic changes to a working internal control structure, based on the demands of their accounting firms. Many filers feel that they do not have reasonable grounds for appeal or push back on these demands, which very often seem arbitrary because of the way in which broad principles have been interpreted by an individual consultant or auditor.

The Commission has a real opportunity to turn the relationship between the filers and their accounting partners from adversarial to cooperative by clearly establishing boundaries for internal controls and clearly establishing categories for key controls, as well as allowing the management of public companies to establish reasonable levels of risk tolerance within their internal control framework. Detailed guidance that defines the parameters in which management and the profession may work would benefit accelerated and non-accelerated filers alike.

> Question 4: Are there additional topics, beyond what is addressed in this Concept Release, that the Commission should consider issuing guidance on? If so, what are those topics?

Response: The primary issue the Commission must consider when it issues guidance is the role of IT General Controls in the internal control structure. Cybertrust urges the Commission to consider including the following in its guidance:

> a) Clarify the role of Information Technology (IT)
>
> Section 404 has actually allowed IT to take its rightful place in the organization's internal control structure, and make information security a recognized part of corporate governance. It has been generally understood by filers and the profession that IT is to be included in 404 compliance activities, but the extent to which IT can contribute to significant deficiency and/or material weakness in the organization's overall internal control structure is largely undefined.
>
> In its guidance, the Commission must clearly establish the role of IT in terms of the internal control structure, and clearly delineate a "target environment," a subset of the organization's entire corporate computing environment, that includes the systems, services, devices, and personnel that create, process, store, and destroy the financial data and financial reporting. Without clear definition, appropriate levels of controls and spending in the IT environment have been determined by the profession, in many cases without mercy. Filers have no solid foundation to push back when the public accounting partner demands superfluous effort or redundant testing for assessment. The Commission, rather than the profession, should clearly define the role of IT, the scope of the target environment, and the controls relevant to Section 404 compliance.
>
> b) Charge the National Institutes of Standards and Technology (NIST) with creating an information security standard

In addition to clarifying the role of IT, the Commission must consider solidifying information security within the target environment. This is yet another area that has been left to the discretion of the profession, and has been responsible for significant costs to the filer. The Commission should consider charging NIST with creating an information security standard for the target environment. There is precedent; at the direction of the Department of Health and Human Services (HHS), NIST created SP 800-66, an information security standard for covered entities required to implement the Security Rule under the Health Information Portability and Accountability Act (HIPAA). There are dozens of information security documents in NIST's Special Publication 800 series; designing a standard or guidance for Section 404 would not only benefit small caps and foreign filers just beginning their compliance activities, but also allow accelerated filers to streamline their compliance work and thereby reduce costs.

c) Allow for a Statement of Risk Tolerance

The Commission should provide to filers (particularly small and micro-caps) a means for arbitration and/or appeal when public accounting partner demands become draconian. Allow management to assert its level of risk tolerance – the recognition that:

i. information security is an inexact science
ii. certain exposures are a fact of life in the interconnected eBusiness world
iii. a valid risk assessment has been performed, and
iv. management recognizes certain areas of risk within its IT environment, mitigated against those risks to the extent reasonably feasible, and is prepared to conduct business within certain parameters of risk

This could be as simple as allowing management to include a documented statement of risk tolerance in the 302 and 404 filings.

Currently, management has no grounds for appeal or push back when the accounting firms and consultancies demand excessive control measures and spending in order to achieve a nebulous compliance target. By clarifying the role of IT in the internal control structure, creating an information security standard, and allowing management to document its risk tolerance, the Commission, rather than the profession, can set a realistic compliance goal. This will allow management and its accounting partner to work within certain proscribed boundaries, which will serve to reduce both confusion and expense, and make the relationship less adversarial and more cooperative.

Question 5: Would additional guidance in the format of a Commission rule be preferable to interpretive guidance? Why or why not?

Response: For the reasons stated in the response to Question 3, interpretive guidance would be far more beneficial to the filing community than a Commission rule. Rules, by their very nature, are subject to

interpretation; only interpretive guidance can provide the clarification necessary to relieve the regulatory burden on filers.

> Question 8: Why have the majority of companies that have completed an assessment, domestic and foreign, selected the COSO framework rather than one of the other frameworks available, such as the Turnbull Report? Is it due to a lack of awareness, knowledge, training, pressure from auditors, or some other reason? Would companies benefit from the development of additional frameworks?

The COSO framework is the predominant framework used by the accelerated filers because of its acceptance in the United States. Although other frameworks, such as the Turnbull Report, were deemed acceptable by both the Commission and the PCAOB, the general feeling amongst the filers was that the public accounting firms were most familiar and comfortable with COSO. Simply put, the use of another framework, albeit acceptable, begged the question from the auditor – why did the filer choose another framework instead of COSO? It was generally understood that foreign filers were free to use in-country frameworks, and not required to adopt COSO, in order to fulfill Section 404 requirements; COSO has simply become *de facto* in the United States.

That being said, both the COSO Internal Controls Framework of 1999 and the COSO ERAM of 2004 are excellent documents. There has been no adverse reaction within the community of filers indicating that COSO is unduly burdensome or onerous. Both documents can scale to accommodate organizations of various sizes. There is no need to spend time and resources creating additional frameworks. Filers have access to high-level conceptual documentation in abundance – the Commission should focus its attention at implementation-level guidance for the filers.

> Question 9: Should the guidance incorporate the May 16, 2005, "Staff Statement on Management's Report on Internal Control Over Financial Reporting"? Should any portions of the May 16, 2005 guidance be modified or eliminated? Are there additional topics that the guidance should address that were not addressed by that statement? For example, are there any topics in the staff's "Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports Frequently Asked Questions (revised October 6, 2004)" that should be incorporated into any guidance the Commission might issue?

Response: Certainly, the comments on the 'Information Technology Internal Controls' should be revisited. Staff comments indicate that "because Section 404 is not a one size fits all approach," they were unable "to provide a list of the exact general IT controls that should be included in an assessment for Section 404 purposes". This puts the burden on management to define a target environment, choose an information security framework appropriate to meet the requirements of COSO, apply the relevant to control measures from the framework to the self-defined target, test and evaluate those controls, and present the results of

testing to the public accounting partner. In situations where the accounting firm (or consultancy) finds this work insufficient, management has no choice but to then meet the additional requirements as defined by the partner.

In its guidance, the Commission must establish a baseline for the target environment and testing methods (see the response to Question 4). The Commission should also consider the creation of an information security standard for Section 404 compliance, or the endorsement or adoption of an information security framework (see the response to Question 30). In the absence of definition or clarification from the Commission, the profession is in the position of establishing the compliance requirements for Section 404.

> Question 10: We also seek input on the appropriate role of outside auditors in connection with the management assessment required by Section 404(a) of Sarbanes-Oxley, and on the manner in which outside auditors provide the attestation required by Section 404(b). Should possible alternatives to the current approach be considered and if so, what? Would these alternatives provide investors with similar benefits without the same level of cost? How would these alternatives work?

Response: The Commission should work with the PCAOB in order to clarify the extent to which the public accounting firms can rely on the work of others, particularly with regard to the testing and evaluation of the IT General Controls. Many filers have working information security programs or routine processes in place in the live production environment, including the target environment, which houses financial data and produces financial reporting. When filers work with reputable security firms, it is redundant in terms of effort and expense to have public accounting firms repeat testing and evaluation; the firms, however, indicate that they must perform all testing themselves because of the liability associated with opinion and assertions.

At the roundtable on May 10, 2006, the PCAOB indicated that it intended to clarify its position on allowing the profession to rely on the work of others for certain routine testing and evaluation of the internal control structure. Cybertrust urges both the Commission and the PCAOB to allow the profession to use the work of reputable information security firms for the testing and evaluation of the IT General Controls, and to clearly state this in guidance for the benefit of the profession and the filers.

Although the Federal Government cannot endorse an individual company or industry segment, the Commission and the PCOAB can consider creating criteria that an information security firm should meet in order to be considered “reputable” or appropriate to perform evaluations on the IT General Controls in a manner consistent with the requirements of Section 404. It need not be as extensive as a certification and accreditation program, but merely the establishment of a simple baseline or core set of capabilities that must be met in order to perform work at a level that is acceptable to the profession. This will allow filers to reduce both the costs and efforts associated with redundant and duplicative testing and evaluation of the IT General Controls.

> Question 14: In areas where companies identified significant start-up efforts in the first year, (e.g., documentation of the design of controls and remediation of deficiencies) will the COSO guidance for smaller public companies adequately assist companies that have not yet complied with Section 404 to efficiently and effectively conduct a risk assessment and identify controls that address the risks? Are there areas that have not yet been addressed or need further emphasis?

Response: The COSO guidance will indeed be helpful for small and micro-caps in establishing an internal control framework and conducting a risk assessment. In terms of implementation, however, smaller companies will need specific guidance when identifying controls appropriate to address the risks identified through assessment, and to monitor and manage the controls in place in the live production environment over time. These organizations, in particular, will benefit from any clarification of the role of IT (as noted in the responses to Questions 3 and 4) and specific interpretive guidance issued by the Commission.

> Question 20: Would guidance on how management's assessment can be based on evidence other than that derived from separate evaluation-type testing of controls, such as on-going monitoring activities, be useful? What are some of the sources of evidence that companies find most useful in ongoing monitoring of control effectiveness? Would guidance be useful about how management's daily interaction with controls can be used to support its assessment?

Response: This is an area in which the PCAOB can allow the profession to rely on the work of others, specifically security firms and consultancies, particularly with regard to the IT General Controls. Many filers work with security firms or consultancies that perform routine testing and evaluation of the corporate computing environment. The public accounting partner should feel comfortable in relying on the results of testing and evaluation performed by reputable information security specialists (see the response to Question 10). The Commission should urge the PCAOB to consider that if management can provide demonstrable evidence of a good faith compliance effort that includes an information security program that continuously manages and/or monitors the target environment and maintains an effective information security posture, redundant testing by the accounting firm itself should be unnecessary.

> Question 21: What considerations are appropriate to ensure that the guidance is responsive to the special characteristics of entity-level controls and management at smaller public companies? What type of guidance would be useful to small public companies with regard to those areas?

Response: For entity-level controls, particularly the IT General Controls, the more detailed the guidance, the better (see the responses to Questions 3, 4, and 10). Detailed guidance will be particularly useful to the small and micro-caps and foreign filers, which are just beginning their compliance activities. Although staff comments indicated a certain reticence to providing detailed guidance at the level of the IT environment and associated testing, inaction in this area by the Commission means continued definition of these critical

issues by the profession. This often puts filers at a disadvantage, and maintains an adversarial, rather than cooperative, relationship between the filer and the public accounting partner.

> Question 22: In situations where management determines that separate evaluation-type testing is necessary, what type of additional guidance to assist management in varying the nature and extent of the evaluation procedures supporting its assessment would be helpful? Would guidance be useful on how risk, materiality, attributes of the controls themselves, and other factors play a role in the judgments about when to use separate evaluations versus relying on ongoing monitoring activities?

This issue is particularly germane to the IT General Controls. Vulnerabilities can exist in the IT environment that do not represent real risk to the target environment encompassing financial reporting, or a significant deficiency or material weakness in the internal control structure. As part of its guidance, the Commission should consider establishing parameters for testing within the target environment. This can take the form of proscribed procedures or illustrative examples. Rather than including extensive procedures in the guidance, should the Commission choose to have a standards body develop information security requirements for Section 404 compliance, testing procedures can be included in those requirements. Short of that, the Commission can consider making a request of the ITGI to create a testing procedures document to accompany the second edition of the ”IT Control Objectives for Sarbanes-Oxley” document (see the response to Question 30).

> Question 23: Would guidance be useful on the timing of management testing of controls and the need to update evidence and conclusions from prior testing to the assessment “as of” date?

Response: Many of the accelerated filers relied on Statement of Accounting Standards No. 70 (SAS 70) “testing” to evaluate the IT General Controls. Such point-in-time audits are insufficient to effectively evaluate the effectiveness of controls in IT environment on an ongoing basis. Organizations should have in place an information security program that monitors the controls in place over time, in order to establish and maintain an effective security posture. Information security programs can compensate for routine changes to the corporate computing environment as well as changes in technology and the general threat landscape.

In its guidance, the Commission should encourage organizations to demonstrate to the public accounting partner that the testing of IT controls is routine and current. Demonstrable evidence of compliance should include electronic testing of IT controls takes place at least quarterly, as well as an annual inspection of the physical environment and review of relevant documentation including information security policies and procedures.

> Question 25: Would guidance be helpful regarding the definitions of the terms “material weakness” and “significant deficiency”? If so, please explain any issues that should be addressed in the guidance.

Response: Filers currently rely on the profession to define “deficiency”, “significant deficiency”, and “material weakness”; these definitions can vary, in both scope and meaning, between public accounting firms. In its guidance, the Commission should establish formal, universal definitions for these terms. The Commission should also consider clarifying these terms when they extend to controls outside of formal accounting practices and procedures. Specifically, the Commission should define “significant deficiency” and “material weakness” as they relate to the IT General Controls. As stated in the response to Question 22, not all vulnerabilities in the target environment represent deficiencies in terms of the internal control structure. Not all IT vulnerabilities represent real risk to the corporate computing environment. The Commission should state in its guidance, by establishing formal parameters or providing illustrative examples, the extent to which IT vulnerabilities can contribute to findings of significant deficiency or material weakness in the internal control structure.

> Question 29: Is guidance needed to help companies determine which IT general controls should be tested? How are companies determining which IT general controls could impact IT application controls directly related to the preparation of financial statements?

Response: To date, the determination of the IT general controls to be tested in a given filer’s environment has been a delicate negotiation between the filer and the public accounting partner, with the advantage clearly in favor of the accounting firm. There has been no clear definition of relevant controls, no consensus on the scope of the target environment that produces the financials as a subset of the entire corporate computing environment, and no uniformity in testing methodology. This has contributed greatly to the exorbitant costs of Section 404 compliance for the accelerated filers, and is a source of concern for small and micro-caps.

In its guidance, the Commission must define the basis of the target environment, limiting the scope (to the extent reasonably possible) to the systems, services, devices, and personnel that create, process, store and destroy the financial data and financial reporting. In its guidance, the Commission must encourage filers to appropriately isolate the target environment from the overall corporate computing environment, and provide the accounting firm with documentation and topographical evidence to support appropriate isolation. For purposes of Section 404 compliance, testing and evaluation can be limited to the target, unless there is clear evidence of deficiency or material weakness in the target that originates from external sources.

> Question 30: Has management generally been utilizing proprietary IT frameworks as a guide in conducting the IT portion of their assessments? If so, which frameworks? Which components of those frameworks have been particularly useful? Which components of those frameworks go beyond the objectives of reliable financial reporting?

Response: The most commonly used IT framework used to support Section 404 compliance has been the Control Objectives for Information and Related Technology (CobiT). CobiT is associated with the COSO

framework for Internal Controls, and is a globally recognized management standard with detailed information security requirements. Although CobiT is an excellent framework, only the largest corporations manage to this standard on a regular basis. It is widely viewed as suitable to organizations that adopt other management standards such as Six Sigma or Balanced Scorecard, but is also seen as overkill for many small companies. Nevertheless, as an open framework, the control clauses specific to IT can be adopted by organizations of all sizes.

CobiT is written as a set of broad management principles, which require interpretation to be successfully applied to a corporate computing environment. Many organizations use IT security standards to interpret CobiT, the most prevalent being the ISO 17799 Information Technology Security Techniques – Code of Practice for Information Security Management. ISO 17799 is the predominant global information security standard, and is generally accepted as a practical and achievable approach to information security management.

The IT Governance Institute (ITGI) has provided *de facto* guidance to filers in its document "IT Control Objectives for Sarbanes-Oxley"; the second edition, which uses CobiT v.4, is now available in exposure draft. Many filers have used this as a reference document for compliance implementation activities, but there is no statistical information available regarding its acceptance by the profession. This document, however, has realistically been the only direction and assistance created for the benefit of filers.

Should the Commission choose not to have information security requirements for Section 404 developed by an industry work group or standards body, it should consider the adoption or endorsement of the second edition of the ITGI document. Formal recognition by the Commission and/or the PCAOB would provide the assurance to filers that they have a solid rationale for the IT general controls that will meet with the approval of the profession.

> Question 34: Is guidance needed about documentation for information technology controls? If so, is guidance needed for both documentation of the controls and documentation of the testing for the assessment?

Response: In its guidance, the Commission must address documentation for both controls and testing. This is another area where filers are dependent upon the profession for guidance and direction in developing their control narrative. No universal or standardized interpretation exists for such documentation, and the discretion of the audit firms once again puts filers at a disadvantage when control regimes are arbitrarily burdensome.

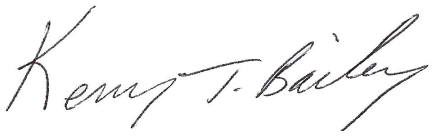
In the response to Question 29, Cybertrust urges the Commission to create a standardized scope defining the target environment (for IT) around the financial data. As it defines the scope, the Commission should include documentation requirements for all associated controls, and documentation requirements for related

testing. The Commission, rather than the profession, should define what constitutes demonstrable evidence of a good faith effort to comply with Section 404.

Again, Cybertrust thanks the Commission for this opportunity to express an opinion on the concept release and subsequent guidance for filers. It is Cybertrust's sincere belief that the accelerated filers have already seen tangible improvement in corporate governance and the accuracy of financial reporting; in addition, information security is now recognized as an integral part of the corporate governance structure, and that has the potential to positively impact corporate performance across the enterprise. The willingness of the Commission to create guidance specifically for filers will almost certainly clarify the outstanding compliance issues for the accelerated filers and reduce the implementation burden for small- and micro-caps as well as foreign filers.

If there are any questions regarding these comments, please contact me at (703) 480-8200.

Sincerely,



Kerry Bailey
Senior Vice President
Global Operations