

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
OFFICE OF THE GENERAL COUNSEL



1111 Franklin Street, 8th Floor • Oakland, California 94607-5200 • (510) 987-9800 • FAX (510) 987-9757

Charles F. Robinson
VICE PRESIDENT AND GENERAL COUNSEL

March 4, 2008

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

Re: Sarbanes-Oxley and Adoption of Best Practices by UC –
Executive Summary of Attached Memorandum

Dear Members of the Board of Regents:

The attached memorandum responds to questions raised at the last Regents' meeting regarding University compliance with Sarbanes-Oxley ("SOX"). It includes a brief overview of all sections of the statute in Attachment 1 as well as a report of the best practices already adopted by UC and suggested next steps. The following is a short summary:

Section I identifies the provisions of SOX that apply to all persons, including corporate persons such as UC. These sections of SOX provide both civil and criminal penalties for retaliation against whistleblowers and for interference with an investigation – particularly intentional alteration or destruction of records.

Section II lists and summarizes the actions taken by UC to date to comply with best practices developed under SOX, which fall roughly into four categories:

1. Comprehensive revisions of the scope and conduct of Regents Committee on Audit business, including oversight of and communications with the external auditor, enhancement of internal controls certification, availability of appropriate financial expertise, and integration of risk management with development of annual internal and external audit plans;
2. Development of the Universitywide *Statement of Ethical Values and Standards of Ethical Conduct* as well as a suite of online training modules for employees to raise awareness of the *Statement* and *Standards* and conflict of interest requirements;
3. Continued development of the University's whistleblower policies and procedures which were in place prior to SOX as required by state statute; and

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

March 4, 2008

Page 2

4. Appointment of the University's new Senior Vice President – Compliance and Audit in September 2007.

The Federal Sentencing Guidelines discussed at the end of Section I and caselaw developed under SOX require a high level of board engagement and oversight of corporate compliance programs. Section III discusses the plans for presenting the Universitywide Compliance Program model to the Committee on Audit in March as well as a Board Resolution in May or June to ensure The Regents' continuing involvement in the process of this important program development.

We will continue to work closely together and with The Regents to identify and implement best practices in Governance and Compliance for UC.

Sincerely,



Charles F. Robinson
Vice President and General Counsel



Sheryl Vacca
Senior Vice President/
Chief Compliance and Audit Officer

Attn.

cc: Regents-Designate
Faculty Representatives
President Dynes
Provost Hume
Executive Vice President Lapp
Secretary and Chief of Staff Griffiths

173154.1

March 4, 2008

TO: The Regents of the University of California

FROM: Charles F. Robinson, Vice President and General Counsel
Sheryl Vacca, Senior Vice President-Chief Compliance and Audit Officer

RE: University of California – The Response to Sarbanes-Oxley

Dear Members of the Board of Regents:

At the January 2008 meeting, several Regents raised questions regarding University compliance with the federal Sarbanes-Oxley Act. Since the questions raise issues of law and compliance, the offices of the General Counsel and Compliance and Audit have decided to provide this response in a joint letter to the Board. We would be pleased to do a followup presentation or to answer questions.

Introduction

The Sarbanes-Oxley Act (“SOX”), signed into law on June 30, 2002 in response to a series of accounting, securities and corporate governance scandals, imposes significant disclosure and accountability requirements on publicly traded companies in the United States. Although it is sometimes stated that SOX does not apply to institutions of higher education, a few provisions of the law expressly do apply. In addition, SOX has resulted in raising standards and expectations of corporations and their boards, including nonprofits. In this letter and its attachments, you will find the following:

1. A brief overview of the statute (See Attachment 1)
2. A discussion of the sections that apply to the University
3. Identification of the steps the University has already taken to adopt best practices developed under SOX
4. Identification of the standards and specific expectations related to board members, and
5. Suggested next steps provided for your consideration.

I. SOX Whistleblower and Anti-Spoliation Provisions Applicable to UC

Protection of Whistleblowers from Retaliation

There are several SOX provisions that in various ways provide protection to whistleblowers from retaliation.¹ These provisions, which apply to all persons and entities, including UC, are essentially the same as those contained in the California state statute which had been applicable to the University for several years before SOX was passed. The California statute and the federal law provide for both civil and criminal penalties for intentional retaliation by individuals and corporations against whistleblowers.²

The University has in place a Whistleblower Policy as well as a Whistleblower Protection Policy. Implementation includes a website and a hotline for anonymous complaints as well as training to protect whistleblowers from retaliation and annual reminders to employees of the availability of these resources.³

Prohibitions against Destruction of Records or Impeding an Investigation

It is a violation of federal criminal law, punishable by a fine and/or imprisonment for up to 20 years, for any person to interfere with any “official proceeding” (such as an investigation) or to interfere with/retaliate against another person who cooperates with a “law enforcement officer.”⁴ Although the phrase “law enforcement officer” is not defined in SOX, the phrase is defined in an earlier section of the federal criminal code to ensure that it will be broadly construed.⁵ Thus, this provision protects all communications with representatives in the executive, judicial and legislative branches of the United States government, not just communications with organizations that are more readily associated with law enforcement activities, such as the FBI.

The Corporate and Criminal Fraud Accountability Act (Title VIII of Sarbanes-Oxley) also added two new sections to the federal criminal code specifying that alteration, concealment or destruction of records in an effort to influence or obstruct any investigation will lead to fines and imprisonment for up to 20 years or both.⁶

The sections of SOX discussed above apply to every person in the United States, whether or not they are affiliated with a publicly traded company. In addition, these code sections apply not just to individuals but also to the corporations for which those individuals work.

In the whistleblower context as well as in Human Resources and employment law training

¹ See, e.g. 18 U.S.C. §§ 1513, 1514A, 1515(1), and 1512(C)(2)

² Calif. Gov. Code §§ 8547.11 – 8547.12

³ <http://ucwhistleblower.ucop.edu/welcome.html>

⁴ 18 U.S.C. §1513; see also 18 U.S.C. § 1512(C)(2)

⁵ See, 18 U.S.C. § 1515(1)

⁶ 18 U.S.C. §§ 1519 and 1512(c)

programs, employees are advised that retaliation against individuals engaging in protected activity covered by a host of state and federal statutes is prohibited. Nonretaliation will be included as a part of basic compliance training as the University moves forward with its compliance program.

Federal Sentencing Guidelines

The Federal Sentencing Guidelines⁷ were substantially amended in November 2004 in response to SOX, including Chapter 8 which applies to nonprofit corporations, such as UC. Chapter 8 describes in detail the kind of factors a federal judge would take into account at the sentencing phase of a criminal trial, on the question whether the good faith efforts of the corporation to prevent, detect and correct illegal behavior by its employees could mitigate or reduce the sentence. Chapter 8 states the essential elements of a corporate compliance program which were presented to The Regents Committee on Audit by the Senior Vice President of Compliance and Audit, Sheryl Vacca, at its January 2008 meeting. (Attachment 2.) As we discuss in the final section of this letter, it is clear that these Guidelines as well as best practices call for significant knowledge and engagement on the part of governing boards in establishment and operation of the corporate compliance program.

II. University Actions to Adopt Sarbanes-Oxley Best Practices

Title III of SOX is entitled “Corporate Responsibility.” Sections 301 – 308 identify a number of required practices for boards of directors including establishment of an audit committee and a description of the responsibilities audit committees should have. The Regents began responding affirmatively to the best practices contained in SOX almost immediately and have continued on that course over time, as further best practices were developed. A little over two months after SOX became law, at its September 2002 Board meeting, The Regents Committee on Audit approved its first standard in conformance with the statutory best practices by prohibiting the outside auditor from performing any of the services prohibited under SOX. Upon presentation to the Board as a whole, the standard was adopted.⁸ It is described in more detail in the next section, #5.

Shortly thereafter, the University hired a consulting firm to undertake an analysis of the entire statute and to make recommendations for best practices that the University should consider. The consultant’s report was submitted to the Committee on Audit in March 2003. It was discussed in detail at the next meeting, and the University Auditor was directed to produce a set of management recommendations in response to the report.

In September 2003, the University Auditor proposed amendments to the Audit Committee charter along the lines recommended by a consulting firm and in conformance with provisions of

⁷ USSG, Ch. 8, Part B: Remediating Harm from Criminal Conduct and Effective Compliance and Ethics Program

⁸ <http://www.universityofcalifornia.edu/regents/minutes/2002/audit902.pdf>

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

March 4, 2008

Page 4

SOX. He also provided a matrix addressing SOX provisions, consultant recommendations, recommendations for higher education by the National Association of College and University Business Officers as well as UC management recommendations for adoption of best practices. Following discussion and direction by The Regents Committee on Audit, the Senior Vice President for Business and Finance advised the committee that the changes recommended by management would be implemented.

Periodic reports on progress were then made to the Board, most recently in May 2005, where the Board was advised that all the best practices recommendations in response to SOX had been implemented and put in place.⁹ The governance and best practices adopted are summarized below:

1. Audit Committee Expanded Oversight. The Committee on Audit charter was revised to reflect the expanded oversight and responsibility set out in the provisions of SOX.
2. Board Independence. A set of standards for determination of independence for Board members and a requirement that only independent Board members can be appointed to the Committee on Audit was considered by the Committee on Audit and the Committee on Regents Procedures in January 2005 and it was approved by the entire Board at that time. The standards exceed those required by the California Nonprofit Integrity Act of 2004, and meet SEC standards under SOX.
3. Financial Expertise. Selection and appointment of an expert advisor who meets the SEC standards of a financial expert was completed in July, 2005. Mr. Kent Vining, who has served ably for nearly three years as the financial expert advisor to the Committee on Audit, is now preparing to step down. The search for a replacement is currently under way. In addition, a Regents Item is in preparation for the March 2008 meeting that will revise the screening and appointment process, add an expert advisor in risk/corporate compliance and propose appropriate changes to the Committee on Audit charter as well as related governance documents.
4. Outside Auditor Retention. The independent or external auditor is no longer retained by management. The Committee on Audit now engages the independent auditor and has direct oversight responsibility.
5. Non-Audit Services. The Committee on Audit now must pre-approve all permissible non-audit services performed by auditors. Consistent with provisions of SOX, the external auditor is forbidden to provide the following services to the University: bookkeeping, financial information systems design and implementation, appraisal or valuation, actuarial work, internal audit outsourcing, management functions, broker/dealer, investment advisor or banking services, legal services and expert opinions.

⁹ <http://www.universityofcalifornia.edu/regents/regmeet/may05/904.pdf>

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

March 4, 2008

Page 5

6. Outside Auditor Evaluations. The Committee on Audit hears informal annual evaluations of the external auditor with active participation in a formal evaluation whenever reappointment is considered, currently every three years. Rotation of the lead and reviewing partners are also considered at that time with an expectation of rotation every five years, consistent with provisions of SOX. The lead and reviewing partners for UC were changed by the external auditor in 2007 and the Committee on Audit is currently formally evaluating the external auditor and assessing whether to undertake a competitive bidding process for the future services of an external auditor.
7. Management Conflict with Auditors. The Committee on Audit has authority to address and resolve disagreements between the external auditors and management. There have been none to date. Regents-only sessions are held between the external auditor and members of the Committee periodically to assure an adequate opportunity for reporting on disagreements or efforts to influence the auditors, should this occur.
8. Internal Controls Certification. Statements regarding responsibility for the internal control structure are now included in the Management Representation letters, where management certifies that all appropriate and relevant information has been disclosed to assist auditors in concluding that the financial statements conform to applicable auditing and accounting standards. The certification process now includes signatures by top-level management as well as those deeper in the management structure such as Vice Chancellors and Deans.
9. Required Communications. Statement of Auditing Standards No. 114 issued in 2006 superseded an earlier set of required communications by establishing standards and guidance for auditors on matters to be communicated to those charged with governance of the organization being audited. Since 2003, The Regents Committee on Audit has routinely been making additional time available for Regents Only communications with the outside auditor and continues to assure that channels for two-way communication are kept open.
10. Audit Plan Risk Assessment. Although Committee on Audit review and discussion of risk assessment and risk management is not required by SOX, it is required by the stock exchanges and thus has become a standard best practice in business. The UC Administration has adopted this requirement, by discussing each year with the chair of the Committee on Audit the Committee's principle risk concerns, so that they may be considered in development of each year's annual audit plan, and by including such consultation as a requirement in the Committee on Audit Charter. Additionally, risk management will provide periodic and annual reports to the Committee on Audit in FY 2008 – 09 to integrate the organization's risk reporting with compliance and audit.
11. Whistleblower Process. As previously noted, UC has a robust set of policies and procedures for whistleblower communications and for protection against retaliation that

complies with both state and federal statutory requirements. Consistent with best practices for protection of anonymity, the University has retained an outside vendor as its Hotline provider and followup case management tools are in place.

12. Ethics Training. A new systemwide code of ethics package, the *University of California Statement of Ethical Values and Standards of Ethical Conduct* was approved by The Board of Regents in May 2005. The President subsequently funded rollout of an online training program to introduce the ethics package to The Regents and all University employees. There have been periodic reports to the Committee on Audit regarding the status of ethics training with UC employees.
13. Chief Compliance and Audit Officer. The Regents appointed a new Senior Vice President of Compliance and Audit at its September 2007 meeting. (See below.)

III. Next Steps

Since 2002, there has been a great deal of discussion about extending the SOX provisions to the nonprofit sector, but to date none of the statutory or regulatory changes apply directly to UC (except as noted above in Section I). The state of California, for example, enacted the Nonprofit Integrity Act in 2004 and though it does apply to the UC Foundations, both higher education institutions and hospitals were specifically exempted from coverage.¹⁰ Nonetheless, the governance practices of the state statute were also adopted by The Regents in 2005, by an amendment to the independence requirements for service on the Committee on Audit.¹¹

The University of California has reason to be proud of the actions taken so far to comply with not only applicable provisions of SOX but also with many of the best business practices that have come to be the standard expected of large corporations, both publicly traded and nonprofit. More, however, can be done.

The provisions of the Federal Sentencing Guidelines, caselaw developed under Sarbanes-Oxley¹² and very recent statements by the Internal Revenue Service¹³ make clear the expectation that an organization's Compliance Program must include Governing Board accountability, oversight and engagement in the program process. To this end, SVP Vacca will provide information to both the Committee on Audit and to the Board to request adoption of a Board Resolution to approve

¹⁰ Cal. Bus. & Prof. Code § 17510.5; Cal. Gov. Code §§ 12581–12586, 12399, and 12599.1–12599.7.

¹¹ <http://www.universityofcalifornia.edu/regents/minutes/2005/regpro505.pdf>

¹² See, e.g., La. State Police Retirement System et al. v. Caremark [and individually named members of the board of Caremark] et al., 918 A.2d 1172, 2007 Del. Ch. LEXIS 27 (Del. Ch. Feb. 23, 2007)

¹³ <http://www.irs.gov/newsroom/article/0,,id=176722,00.html>

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

March 4, 2008

Page 7

the Universitywide Compliance Program at the July meeting. The Office of the General Counsel and the Office of the Senior Vice President – Compliance and Audit will work closely together and with The Regents to continue identifying and implementing best practices in Governance and Compliance for the University of California.

Sincerely,



Charles F. Robinson
Vice President and General Counsel



Sheryl Vacca
Senior Vice President/
Chief Compliance and Audit Officer

cc: Regents-Designate
Faculty Representatives
President Dynes
Provost Hume
Executive Vice President Lapp
Secretary and Chief of Staff Griffiths

ATTACHMENT 1

Brief Overview of the Provisions of the Sarbanes-Oxley Act of 2002

- Title I, Sections 101 – 109: establishes the Public Company Accounting Oversight Board, providing for registration and oversight of firms providing independent audit services to publicly traded companies.
- Title II, Sections 201 – 209: sets standards for maintenance of the outside auditor’s independence.
- Title III, Sections 301 – 308: addresses requirements for board audit committees, assigns responsibility for certification of financial statements, prohibits interference with audits by officers or directors and requires forfeiture of incentive compensation for the CEO and CFO where an accounting restatement is caused by misconduct. Requires attorneys to report serious violations up the ladder to the board.
- Title IV, Sections 401 – 409: requires enhanced financial disclosures including off-balance sheet transactions, holdings by directors, and assessments of internal controls, prohibits loans to directors/executives by the corporation. Sets baseline standards for codes of ethics and for qualification as a “financial expert,” requiring that every audit committee have at least one such expert.
- Title V, Section 501: establishes conflict of interest requirements for stock analysts.
- Title VI, Sections 601 – 604: identifies changes in SEC resources and authority, including a substantial allocation for Information Technology.
- Title VII, Sections 701 – 705: requires various studies and reports largely to assess the degree of noncompliance with SEC requirements prior to enactment of SOX.
- Title VIII, Sections 801 – 807: establishes criminal penalties for corporations, including nonprofits, for altering/destroying documents or otherwise interfering with an investigation and for retaliating against employees who blow the whistle or cooperate. Directs the United States Sentencing Commission to review and amend Federal Sentencing Guidelines for organizational criminal misconduct.
- Title IX, Sections 901 – 906: enhances criminal penalties for white collar crime.
- Title X, Section 1001: states the “sense of the Senate” that tax returns should be signed by the CEO.
- Title XI, Sections 1101 – 1107: amends various provisions of federal criminal statutes to enhance punishments for impeding official proceedings in any way, including spoliation of documents, for violating SEC laws and for retaliating against informants. Authorizes the SEC to prohibit persons from serving as officers or directors of publicly traded companies if their conduct demonstrates unfitness for such service.

ATTACHMENT 2

2005 Federal Sentencing Guidelines**Chapter 8 - PART B - REMEDYING HARM FROM CRIMINAL CONDUCT, AND EFFECTIVE COMPLIANCE AND ETHICS PROGRAM****§8B2.1. Effective Compliance and Ethics Program**

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (c)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

- (1) exercise due diligence to prevent and detect criminal conduct; and
- (2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

- (1) The organization shall establish standards and procedures to prevent and detect criminal conduct.
 - (2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.
 - (B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.
 - (C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.
- (3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.
 - (4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subdivision (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

Commentary

Application Notes:

1. Definitions.—For purposes of this guideline:

"Compliance and ethics program" means a program designed to prevent and detect criminal conduct.

"Governing authority" means the (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization.

"High-level personnel of the organization" and "substantial authority personnel" have the meaning given those terms in the Commentary to §8A1.2 (Application Instructions - Organizations).

"Standards and procedures" means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct.

2. Factors to Consider in Meeting Requirements of this Guideline.—

(A) In General.—Each of the requirements set forth in this guideline shall be met by an organization; however, in determining what specific actions are necessary to meet those requirements, factors that shall be considered include: (i) applicable industry practice or the standards called for by any applicable governmental regulation; (ii) the size of the organization; and (iii) similar misconduct.

(B) Applicable Governmental Regulation and Industry Practice.—An organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.

(C) The Size of the Organization.—

(i) *In General*.—The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization's standards and procedures, depend on the size of the organization.

(ii) *Large Organizations*.—A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization. As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.

(iii) *Small Organizations*.—In meeting the requirements of this guideline, small organizations shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations. However, a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems.

Examples of the informality and use of fewer resources with which a small organization may meet the requirements of this guideline include the following: (I) the governing authority's discharge of its responsibility for oversight of the compliance and ethics program by directly managing the organization's compliance and ethics efforts; (II) training employees through informal staff meetings, and monitoring through regular "walk-arounds" or continuous observation while managing the organization; (III) using available personnel, rather than employing separate staff, to carry out the compliance and ethics program; and (IV) modeling its own compliance and ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.

(D) *Recurrence of Similar Misconduct*.—Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of this guideline. For purposes of this subdivision, "similar misconduct" has the meaning given that term in the Commentary to §8A1.2 (Application Instructions - Organizations).

3. *Application of Subsection (b)(2)*.—High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program, shall perform their assigned duties consistent with the exercise of due diligence, and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

If the specific individual(s) assigned overall responsibility for the compliance and ethics program does not have day-to-day operational responsibility for the program, then the individual(s) with day-to-day operational responsibility for the program typically should, no less than annually, give the governing authority or an appropriate subgroup thereof information on the implementation and effectiveness of the compliance and ethics program.

4. *Application of Subsection (b)(3)*.—

(A) *Consistency with Other Law*.—Nothing in subsection (b)(3) is intended to require conduct inconsistent with any Federal, State, or local law, including any law governing employment or hiring practices.

(B) *Implementation*.—In implementing subsection (b)(3), the organization shall hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with the exercise of due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law under subsection (a). With respect to the hiring or promotion of such individuals, an organization shall consider the relatedness of the individual's illegal activities and other misconduct (i.e., other conduct inconsistent with an effective compliance and ethics program) to the specific responsibilities the individual is anticipated to be assigned and other factors such as: (i) the recency of the individual's illegal activities and other misconduct; and (ii) whether the individual has engaged in other such illegal activities and other such misconduct.

5. *Application of Subsection (b)(6).*—Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

6. *Application of Subsection (c).*—To meet the requirements of subsection (c), an organization shall:

(A) Assess periodically the risk that criminal conduct will occur, including assessing the following:

(i) The nature and seriousness of such criminal conduct.

(ii) The likelihood that certain criminal conduct may occur because of the nature of the organization's business. If, because of the nature of an organization's business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct. For example, an organization that, due to the nature of its business, employs sales personnel who have flexibility to set prices shall establish standards and procedures designed to prevent and detect price-fixing. An organization that, due to the nature of its business, employs sales personnel who have flexibility to represent the material characteristics of a product shall establish standards and procedures designed to prevent and detect fraud.

(iii) The prior history of the organization. The prior history of an organization may indicate types of criminal conduct that it shall take actions to prevent and detect.

(B) Prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b), in order to focus on preventing and detecting the criminal conduct identified under subdivision (A) of this note as most serious, and most likely, to occur.

(C) Modify, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) to reduce the risk of criminal conduct identified under subdivision (A) of this note as most serious, and most likely, to occur.

Background: This section sets forth the requirements for an effective compliance and ethics program. This section responds to section 805(a)(2)(5) of the Sarbanes-Oxley Act of 2002, Public Law 107-204, which directed the Commission to review and amend, as appropriate, the guidelines and related policy statements to ensure that the guidelines that apply to organizations in this chapter "are sufficient to deter and punish organizational criminal misconduct."

The requirements set forth in this guideline are intended to achieve reasonable prevention and detection of criminal conduct for which the organization would be vicariously liable. The prior diligence of an organization in seeking to prevent and detect criminal conduct has a direct bearing on the appropriate penalties and probation terms for the organization if it is convicted and sentenced for a criminal offense.

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).