[DISCUSSION DRAFT]

108TH CONGRESS
1ST SESSION

H. R. _____

To amend the Securities Exchange Act of 1934 to require each publicly traded company to conduct an assessment of the company's computer information security.

IN THE HOUSE OF REPRESENTATIVES

Mr. PUTNAM introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Securities Exchange Act of 1934 to require each publicly traded company to conduct an assessment of the company's computer information security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Corporate Information Security Accountability Act of 2003''.

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to protect public safety, the economy, and shareholder's investments, by providing a basic framework for assessing the effectiveness of information security controls over information resources for publicly traded companies;

(2) to recognize the highly networked nature of corporate computer information systems and provide effective oversight of the related information security risks; and

(3) provide for the establishment, improvement, and continued maintenance of necessary controls to protect these privately maintained information systems.

SEC. 3. COMPUTER SECURITY ASSESSMENT REQUIRED.

Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) is amended by adding at the end the following new subsection:

''(m) COMPUTER INFORMATION SECURITY ASSESSMENT REQUIRED.—

''(1) IN GENERAL.—Each issuer (as such term is defined in section 2 of the Sarbanes-Oxley Act) shall include in the annual report submitted under this section, for each fiscal year that begins on or after one year after the date of enactment of this

subsection, a certification by an independent party that the issuer conducted an assessment during such fiscal year of the issuer's computer information security in accordance with standards prescribed by the Commission by rule.

''(2) STANDARDS.—The Commission shall prescribe standards for purposes of this subsection within 60 days after the date of enactment of this subsection. In prescribing such standards, the Commission shall—

''(A) establish criteria by which to determine the independence of the party to conduct the assessment;

''(B) establish standards for the assessment of the risks to the issuer's computer information that require the issuer—

''(i) to assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(ii) to determine the levels of information security appropriate to protect such information and information systems, to include at least the following:

''(I) critical information technology assets inventory;

''(II) annual risk assessment;

''(III) development of risk mitigation plan;

''(IV) development of incident response plan; and

''(V) development of business continuity plan;

''(iii) to implement policies and procedures to effectively reduce risks to an acceptable level; and

''(iv) to periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented.

''(3) PROTECTION OF INFORMATION.—The certification required by paragraph (1) shall not include specific proprietary information, and shall not contain any information identifying, directly or indirectly, any specific vulnerability of the issuer's computer information. Notwithstanding any other provision of law, the Commission shall not be compelled to disclose any information obtained by the Commission in any investigation of an issuer's compliance

with this section. Nothing in this paragraph shall authorize the Commission to withhold information from Congress, or prevent the Commission from complying with a request for information from any other Federal department or agency requesting information for purposes within the scope of its jurisdiction, or complying with an order of a court of the United States in an action brought by the United States or the Commission. For purposes of section 552 of title 5, United States Code, this paragraph shall be considered a statute described in subsection (b)(3)(B) of such section 552.

''(4) DEFINITIONS.—For purposes of this subsection:

''(A) COMPUTER INFORMATION SECURITY.—The term 'computer information security' means the systems, procedures, and devices used for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(i) integrity, by guarding against improper information modification or destruction, and ensuring information nonreproduction and authenticity;

"(ii) confidentiality, by preserving authorized restrictions on access and disclosure, and by protecting personal privacy and proprietary information; and

"(iii) availability, by ensuring timely and reliable access to and use of information.

"(B) INFORMATION SYSTEM.—The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.".