



April 30, 2014

Ms. Elizabeth M. Murphy,
Secretary of Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File Number 4-673 Cybersecurity Roundtable

Dear Secretary Murphy,

BSA | The Software Alliance (“BSA”)¹ appreciates the opportunity to present its views in response to the U.S. Securities & Exchange Commission’s (“SEC”) request for comments on the Roundtable on Cybersecurity hosted on March 26, 2014. BSA is an association of world-class companies that invest billions of dollars annually to create innovative software solutions, which make enterprises more productive, competitive, and secure. These comments focus on the role of strong internal controls related to cybersecurity in preventing exposure to risks and protecting a company, its investors, and capital markets, generally. Discussions during the Roundtable focused on the risks companies face with respect to protecting their information technology systems from intrusion, unwarranted disclosure of customer information, and disruption and identified the need to evaluate the scope of a company’s disclosure obligations when communicating such risks to investors. An aspect of the discussion warranting further development is the importance of sound internal controls related to software assets as a first line of defense against cyber-attacks. In this regard, the SEC has already given notice to companies regarding its expectations that in 2014 they address the 2013 revisions to *The Internal Control – Integrated Framework*

¹ BSA is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world’s most innovative companies creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA’s members include: Adobe, Altium, Apple, ANSYS, Autodesk, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rockwell Automation, Rosetta Stone, Siemens PLM, Symantec, Tekla, The MathWorks, and Trend Micro.

("Revised Integrated Framework") of the Committee of Sponsoring Organizations ("COSO"). Included in the Revised Integrated Framework are procedures that provide a solid foundation for preventive measures regarding cybersecurity risks. These procedures deserve attention in any dialogue regarding a company's exposure to cyber risks. The SEC has long recognized the critical importance of sound internal controls over financial reporting. In the Revised Integrated Framework, additional focus was placed not only on controls applicable to financial reporting, but also compliance and operations. In the context of technology risks, the Revised Integrated Framework provides guidance on technology controls: "appropriate controls over changes to technology, which may involve requiring authorization of change requests, [and] verifying the entity's legal right to use technology in the manner in which it is being deployed." This new and important focus on technology controls is not well known and often overlooked by management and their service providers. Verifying legal use of software is a critical first-step in deterring cyber-attacks. Increasing education on internal controls and enhanced compliance will not only better inform investors, but also encourage companies to guarantee that these controls are in place and functioning as intended.

Acquisition and use of pirated and counterfeit software is a significant national and international problem. A 2014 study by the International Data Corporation ("IDC") found "that consumers and enterprises have a 33% chance of encountering malware when they obtain a pirated software package or buy a PC with pirated software on it."² This follows a 2013 IDC report which found that "42% of all PC software packages installed in the world in 2011 were pirated."³ The existence and availability of pirated and counterfeit software exposes corporate information technology networks to significant risks in many ways, for example:

- Unlicensed software eliminates the opportunity for security updates and patches from legitimate vendors when security breaches are identified. Notably, up to 43% of companies with fully licensed software routinely fail to install security updates.⁴
- Malware and viruses may be contained within pirated software itself or reside on the networks from which it is downloaded, thereby infecting the user's system during the download process.
- Many unauthorized, but seemingly legitimate, websites offering brand name utility software such as Acrobat Reader, Chrome, and Skype have been found to provide software with malware or viruses.⁵ Consequently, even good faith attempts to obtain legal software from seemingly legitimate sources may carry significant risks.

² *The Link between Pirated Software and Cybersecurity Breaches: How Malware in Pirated Software is Costing the World Billions*, IDC White Paper, Mar. 2014.

³ *The Dangerous World of Counterfeit and Pirated Software*, IDC White Paper, Mar. 2013.

⁴ IDC White Paper, 2014, *Ibid*.

⁵ *The Lowdown on Utility Downloads*, *Journal of Accountancy*, Nov. 2013.

- Exposure to cyber-attacks in the workplace has increased due to a new trend referred to as “bring your own device” or “BYOD.” As companies accommodate more and more access for employees’ personal devices on corporate networks, these networks are further exposed to malware or viruses, because employee devices are more likely to include unlicensed software.
- Illegally copying, distributing, and using copyright protected software significantly increase a company’s exposure to litigation, fines, and penalties.

In considering the need for appropriate disclosure by registrants related to cybersecurity risks, BSA encourages the SEC to first focus on reminding companies of the benefits of sound internal controls aimed at preventing cyber-attacks and good software asset management. Such controls should include at a minimum:

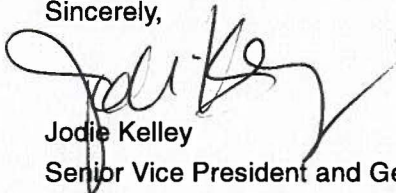
- Controls and procedures to ensure that software is only purchased from authorized vendors.
- Controls to ensure that software downloaded directly from the Internet, even free software, is not being downloaded by secondary market sites and only from reputable authorized vendors.
- Procedures to conduct periodic software inventories and to monitor compliance with the software licensing agreements.
- Procedures to limit a company’s exposure to malware and viruses brought into their systems by linkage of employee personal devices to corporate systems.

We believe recommending registrants to report on the status of their internal controls in the critical area of licensing and legal use of software will create a positive focus and raise the awareness of the need for sound software asset management policies and procedures. Focusing on these issues from an internal control perspective is a natural adjunct to existing SEC policies and procedures. Making sure that installed software is legitimate, and properly licensed during its use, is a first line of defense against cyber-attacks and the destructive costs to the company, shareholders and the marketplace.

BSA appreciates this opportunity to share its views on the importance of sound internal controls for information technology and how such controls foster improved protection for shareholders and the capital markets. Indeed, greater awareness of the benefits of improved compliance with software license agreements represent a necessary step towards reducing companies’ exposure to cyber-attacks.

We would be happy to discuss these comments further or to answer any questions.

Sincerely,



Jodie Kelley
Senior Vice President and General Counsel