Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4905

SIIA

COMMENTS OF THE

SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

on the Notice of Inquiry Issued by the Department of Commerce on April 23, 2010

"Information Privacy and Innovation in the Internet Economy"

Submitted June 14, 2010

On behalf of the members of the Software & Information Industry Association ("SIIA"), we appreciate the opportunity to respond to the Notice of Inquiry ("NOI") published by the Department of Commerce ("DOC") on April 23, 2010, requesting public comment on the impact of the current privacy laws in the United States and around the world on the pace of innovation in the information economy.

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet.[1] SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

For over a decade, SIIA has worked with policy makers at the Federal and state levels in the United States, and also with policy makers in Europe, Canada and other regions, to examine the implications and operations of privacy and related laws. This has included work with the relevant Federal agencies implementing existing privacy and security regulations and policies (notably, the FTC's approach on unfair trade practices, as well as implementation of Gramm-Leach-Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), and the Health IT Act; state policy makers (particularly as the myriad of state laws on privacy and data security have evolved); as well as foreign governments, notably Canada and the European Union ("EU").

---

[1] Our website can be found at: www.siia.net

Tel: +1.202.289.7442
Fax: +1.202.289.7097

www.siia.net

PRELIMINARY OBSERVATIONS

SIIA appreciates the request for stakeholder input into the questions posed by the Department's Internet Policy Task Force.

To state the obvious, treatises could be and have been written on the topics posed in the NOI. SIIA's comments do not attempt to address each and every one of the questions posed; rather, we focus on those that are especially relevant to the mission, experience and expertise of the Department.

Thus, it is appropriate to start with the last question: 'How can the Commerce Department help address issues raised by this Notice of Inquiry?'

For at least the last ten years, since the release of the *Framework for Global Electronic Commerce*, the Department has been positioned to engage not only within the Federal interagency process, but also with our major international trading partners, on the key issues and decisions affecting electronic commerce and doing business online. For these and other reasons, it was no accident that then-President Clinton directed then-Secretary of Commerce William Daley to "work with the FTC and other agencies, consumer advocates, industry, and our trading partners to develop new approaches to extend the proud tradition of consumer protection into cyberspace."[2]

Underlying the Department's role was a fundamental truth that the qualities of the new 'digital' economy advanced by the Internet – "flexibility, innovation, creativity, enterprise"[3] – were producing historic economic growth and jobs. At the time, Vice President Gore envisioned that "by the year 2010, we can triple the number of people who can support their families because they can reach world markets through the Internet."[4] The reality of the impact of the Internet on our economy has far exceeded this vision.

As the convergence of software and information ("S&I") have combined to transform the way that users (individual consumers, government, business end users, and enterprises) access news and information, deliver products and services, and operate, the S&I industries have become strong drivers of the U.S. and global economies, and they are also driving the digital revolution across virtually all sectors of the economy. Well-known firms as well as new, emerging startups — many of which are members of SIIA — create transformative products and services at the leading edge of innovation.

By any measure, the substantial economic impact of the S&I industries demonstrates the critical role that these industries play – despite vast economy uncertainty in real

---

[2] Remarks by the President and the Vice President at Electronic Commerce Event, White House Office of the Press Secretary, November 30, 1998, available at: http://govinfo.library.unt.edu/npr/library/speeches/rmkselec.html.

[3] Ibid.

[4] Ibid.

estate, financial services and manufacturing -- in a vibrant and dynamic U.S. and global economy.[5] The S&I industries have been over the last decade and remain today among the fastest growing and most important for creating jobs and propelling continued U.S. economic growth. For instance, in 2005, S&I industry growth was up nearly 11 percent, compared with 3.2 percent for the economy as a whole, while software and information generated $564 billion in revenue. Also notably, the newspaper, periodical, book and database publishing industry segments sold nearly $7 billion through overseas affiliates in 2005, up by 24 percent from 2000.

The Internet economy today far surpasses Vice President Gore's prediction, with the economic benefits of the commercial Internet eclipsing the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.[6] "And if e-commerce continues to grow annually *half as fast* as it grew between 2005 and 2010, then by 2020 global e-commerce will reach $24.2 trillion, and will add roughly $3.8 trillion annually to the global economy – more than the total GDP of Germany."[7]

As elaborated further below, the Department of Commerce – taking into account its mission, experience and expertise – should focus in the context of this NOI on the following both within the Executive Branch Interagency process and with international trading partners on the following:

- Technology and the Internet economy remain the engine of growth for the U.S. economy, producing relative high wage and high value jobs in an increasingly globally competitive marketplace.

- Cross-border flows of consumer and user data are essential to preserving the competitiveness of U.S. workers and US enterprises, and the Department should work to ensure that data protection laws do not impose barriers to trade.

- The myriad of state and Federal regimes on data protection and data security impose increasingly confusing and conflicting requirements.

- Implementation of state and Federal data privacy, data breach and data security laws have unintended consequences for consumer harm and innovation, and require close scrutiny.

- An expansive definition of what constitutes "personally identifiable information" undermines important efforts to build confidence on the Internet and produce innovative products and services

---

[5] *Software and Information: Driving the Global Knowledge Economy,* SIIA, January 2008, pg. 11, available at: http://www.siia.net/estore/globecon-08.pdf.

[6] Atkinson, et al, *The Internet Economy 25 Years After .com: Transforming Commerce & Life*, Information Technology & Innovation Foundation, March 2010, pg. 43, available at:

[7] Ibid (emphasis added).

- The notice and choice model remains essential in the global, online environment. Critical sources of public information promote confidence in the Internet economy.

CROSS-BORDER FLOWS OF CONSUMER AND USER DATA ARE ESSENTIAL TO PRESERVING THE COMPETITIVENESS OF U.S. WORKERS AND US ENTERPRISES, AND THE DEPARTMENT SHOULD WORK TO ENSURE THAT DATA PROTECTION LAWS DO NOT IMPOSE BARRIERS TO TRADE.

The NOI correctly recognizes that a variety of domestic and foreign laws govern how companies collect, use and share data about individuals. In addition, an increasing array of domestic and foreign laws address the security, retention and even accuracy of such information. This web of laws affects individuals in a variety of contexts: as individual consumers, as employees, and as persons doing business publicly.

This is occurring as US enterprises that are at the heart of the digital and Internet economy increasingly look outward from their U.S. bases to find new customers, enter new markets, and reap the benefits of delivering online services and products without having the costs of traditional 'brick-and-mortar' localization imposed, which may mitigate the opportunity risks.[8] This is true not just for larger enterprises, also for many smaller and medium sized enterprises, which SIIA's research indicates are having larger proportions of their revenues derive from outside North America.[9]

From our vantage, the risks are not only regulatory compliance costs and contradictions, as suggested in the NOI. It is also the direct risk that, under the rubric of data protection, data security and data retention laws, governments will impose barriers to commerce on the Internet that undermine the US Internet economy and our nation's jobs.

At minimum, the Department should be especially vigilant to this risk, factor this risk into its engagement with trading partners in both a multilateral and bilateral context and continue its on-going efforts to facilitate cross-border mechanisms, as well as seek appropriate common arrangements that further this objective.

---

[8] The Task Force should recall that central to Free Trade Agreements negotiated by the US, starting with Chile and Singapore, is a strategic definition of "digital product" that is not inherently tied to either a goods or services trade law framework and does not prejudice a product's classification. By broadly defining "digital product" to include computer programs, text, video, images, sound recordings and other products that are digitally encoded, regardless of whether they are fixed on a carrier medium or transmitted electronically, the FTAs seek a flexible, but practical approach to ensuring that goods and services that combine elements of any of these items are not discriminated against. In other words, no matter how a product may be classified, these Agreements provide for non-discriminatory treatment and promote broader free trade in such products. ***The FTAs also expand market access commitments in Computer and Related Services and ensure that establishment in either country is explicitly not required for the provision of services.***

[9] See *Software and Information: Driving the Global Knowledge Economy*, discussion beginning on pg. 31.

For example, the Department's role in negotiating and implementing the US-EU Safe Harbor agreement stands as a hallmark of DOC leadership and expertise. For many members of SIIA, and other US enterprises with customers and operations in the European Union ("EU"), the Safe Harbor agreement is an essential mechanism to foster cross-border information flows and satisfy different jurisdictional regimes. In addition, the work of the USG, in partnership with US industry, has been important to provide for model contracts to satisfy EU requirements in order that personal data can flow from a Data Controller established in the EU to a Data Controller established outside the EU.[10]

In addition, efforts by the Department, working with interagency colleagues, to provide for key principles, such as those found in APEC. It will be essential, e.g., that the Department support efforts to further the success of the 2008 APEC Ministerial that affirmed the "Digital Prosperity Checklist" and recognized the need to "Promote the development and operation of data privacy frameworks that maximize both privacy protection and the continuity of cross-border information flows consistent with the 2004 APEC Privacy Framework."[11] SIIA encourages the USG to consider the opportunities afforded by efforts such as the Trans-Pacific Partnership to further these goals. In addition, the USG should explore meaningful engagements with non-EU trading partners on how to foster cross-border flow of personal data without the context of the EU Data Protection Directive.

As the Task Force carries out its work in the area of securing personal date, it will be essential to emphasize, based on global principles and the US "Safeguards Rule" the need for on-going data security plans in a manner that promotes predictability and certainty for consumers, consumer protection authorities and businesses. This is not only good policy and practice. This approach also challenges other government that may seek to micromanage technical implementation of data security obligations.

SIIA summarizes the following principles based on international principles,[12] experts[13] and existing regimes, particular the U.S. "Safeguards Rule"[14] which are all appropriate regardless of the size of the entity.

As a fundamental matter, the companies and entities that own or license sensitive personal information should develop a written information security plan that describes their program to protect such information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity

---

[10] See http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.
[11] See note on the work of the APEC Electronic Commerce Steering Group, available at: http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.
[12] Organization for Economic Cooperation and Development (OECD), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (December 2005) ("OECD Guidelines"), found at: http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.
[13] "Final Report of the Advisory Committee on Online Access and Security" (May 15, 2000) ("Advisory Committee Final Report"), found at: http://www.ftc.gov/acoas/papers/finalreport.htm#III.
[14] Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title V of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. ' 6801 *et seq.*.

of the information it handles.[15] Stated another way, the promotion of on-going security plans should avoid micromanaging the details of the plans, since effective security plans will be based on risk and threat analysis, and implementation details that are unique to each entity's situation, taking into account a variety of factors that overt regulation cannot foresee or be flexible enough to adapt to in a rapid manner.

As a general matter, the experience to date suggests that each plan should include the following items, tailored to each entity's risk analysis and situation:

- designate one or more employees to coordinate its information security program;[16]
- identify and assess the risks to customer information in each relevant area of the company's operation (including, in particular) four areas that are particularly important to information security: employee management and training; information systems; detecting and managing system failures; and on-going evaluation of the effectiveness of the current safeguards for controlling these risks;[17]
- design and implement a safeguards program, and regularly monitor and test it;[18]
- select service providers that can maintain appropriate safeguards, making sure that contracts with such service providers require them to maintain safeguards, and oversee their handling of customer information;[19] and

---

[15] See, e.g., "Safeguards Rule." See, also, "OECD Guidelines", p. 12 ("Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system."); "Advisory Committee Final Report", Sec. 3.4.4. ("...adopt security procedures (including managerial procedures) that are 'appropriate under the circumstances.' 'Appropriateness' would be defined through reliance on a case-by-case adjudication to provide context-specific determinations.")

[16] "Safeguards Rule", 16 C.F.R. 314.3(a).

[17] "Safeguards Rule", 16 C.F.R. 314.3(b). See, also, "OECD Guidelines" ("Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.")

[18] "Safeguards Rule", 16 C.F.R. 314.3(c). See, also, "OECD Guidelines" ("Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.")

[19] "Safeguards Rule", 16 C.F.R. 314.3(d).

- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[20]

To emphasize the experience of our industry to date: These requirements are designed to be flexible, appropriate to an entity's own circumstances and updated on an on-going basis. In addition, companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network. These principles urge that rather than promoting an overtly micromanaged legal regime, national or regional frameworks should obligate entities or companies to assess and address the risks to information in all areas of their operations and implement security plans accordingly.

THE MYRIAD OF STATE AND FEDERAL REGIMES ON DATA PROTECTION, DATA SECURITY AND DATA BREACH IMPOSE INCREASINGLY DIFFICULT AND CONFLICTING REQUIREMENTS

The NOI correctly notes that most states have data breach laws (46 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information) or other laws addressing the privacy of information in the private sector. However, the sources that the NOI relies on[21] in fact underestimate the web of state laws that touch on the NOI inquiry. For example, our research indicates that at *least* 9 states have enacted prescriptive security requirements (or amended their data breach laws to achieve the equivalent goal) affecting what would be 'covered information' in the Draft.[22]

The fragmentation of laws and regulations at the state level makes it nearly impossible to provide consumers with consistent notice and choice, as well as undermine efforts to mount an effective offense against pernicious uses of data (including security breaches).

The NOI, however, focuses narrowly on the question of what hurdles enterprises face in complying with different *state* laws. This lens is increasingly not the singular or significant one. Rather, the issue of enterprise compliance with the federal framework within the maze of state laws is dominating compliance and business efforts by enterprises of all sizes. As recognized in the NOI, the approach of federal statutes is sectoral; in contrast, state privacy and date breach laws, on the whole, proscribe obligations generally on treatment of an individual's data. Yet, except in limited areas,

---

[20] "Safeguards Rule", 16 C.F.R. 314(e).

[21] The NOI references the list of state data breach and data privacy laws collected by The National Conference of State Legislatures, Telecommunications and Information Technology, available at: http://www.ncsl.org/Default.aspx?TabID=756&tabs=951,71,539#539.

[22] As of January 1, 2010, it appears that the following states have enacted security obligations: Arkansas, California, Maryland, Massachusetts, Nevada, Rhode Island, Oregon, Texas and Utah.

federal law does not pre-empt to the Federal government this sphere of influence. A key area where conflicts are arising is in the area of data breach requirements,[23] as well as the securing of health care information,[24] where HHS "Guidance"[25] is inconsistent with the provisions of data security laws in Massachusetts and Nevada, to cite two specific instances.

IMPLEMENTATION OF STATE AND FEDERAL DATA BREACH AND DATA SECURITY LAWS HAVE UNINTENDED CONSEQUENCES FOR CONSUMER HARM AND INNOVATION, AND REQUIRE CLOSE CRUTINY

In the arena of data protection, the implementation and impact of data breach laws is drawing increasing scrutiny. This is due to a number of factors, including media reports of large data breaches involving personal information and the growing challenge of identity theft. The need for such focus today is not merely related to implementation of good information practices. Rather, entities managing and collecting data face a growing array of "cybercrooks who are continually arming themselves with innovative tools and methods of attack."[26] These criminals "no longer want notoriety—they want financial gain" and their "criminally motivated attacks have more impact on businesses and their customers than the previous generation of digital vandalism and reckless hacking."[27]

In this context, SIIA offers some background that we believe is useful to examine the relationship between data security breaches and the incidence of identity theft.

Amidst the dramatic news stories of data breaches (most notably the massive breach experienced by TJX Corporation, where the public record indicates that a large number of fraudulent accounts were created as a result), several reports have documented that the instances of identity theft have, on the whole, been limited. One of the challenges is that many of the studies over time have not used consistent definitions of breach, and many do not use legal definitions in defining their parameters.[28]

---

[23] See http://www.siia.net/index.php?option=com_docman&task=doc_download&gid=2279&Itemid=48.

[24] See See comments to HHS on their proposed Guidance, available at: http://www.siia.net/index.php?option=com_docman&task=doc_download&Itemid=318&gid=1626.

[25] "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009".

[26] "Hackers open new front in payment card data thefts," *Computerworld*, April 15, 2008, available at: http://www.infoworld.com/article/08/04/15/Hackers-open-new-front-in-payment-card-data-thefts_1.html.

[27] Technical Brief: Symantec Security Response: *Handling Today's Tough Security Threats*, 2006, available at: http://www.symantec.com/content/en/us/enterprise/collateral/tech_briefs/11310863_HTTST_tb.pdf.

[28] See, e.g., the methodology used by the ID Theft Resource Center. The Center compiles an on-going list of publicly reported breaches. The Center's website indicates that "Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security and driver's license numbers and uses

A close examination of several of the most publicized breaches illustrates the point. For example, in March 2005, a laptop with personal information on 98,369 graduate students or graduate-school applicants was stolen from the University of California at Berkeley. However, not a single case of stolen identity related to the incident was ever reported. "The laptop was recovered in September, and police believe that the thief was interested only in the computer, not in the information in its files."[29] In other cases, "it is unclear whether any breach had taken place, [although] there was the possibility that the information was accessed by unauthorized people."[30] In one recent study, it was found that "data breaches were responsible for just 6 percent of all known cases of identity theft, compared to 30 percent from incidents like losing one's wallet. The study also showed that less than 1 percent of all individuals whose data was lost later became victims of ID theft."[31]

In July 2007, the U.S. Government Accountability Office (GAO) released a report[32] examining (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. The report represents one of the more thorough investigations on the subject, examining 570 data breaches that were reported in the news media from January 2005 through December 2006. (This period did not include the TJX case, the largest up to that date).[33]

The report suggests that breaches of sensitive personal information "have occurred frequently" and under widely varying circumstances, but concludes that:

- Evidence of actual identity theft resulting from the breaches is limited. "Available data and interviews with researchers, law enforcement officials and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts," the report states.

---

it for their own personal gain." However, the compilation provided by the Center includes many incidences that appear to not meet this particular definition.

[29] "Separating myth from reality in ID theft", CNET News.com, October 24, 2005, Found at: http://news.com.com/Separating+myth+from+reality+in+ID+theft/2100-1029_3-5907165.html.

[30] Michael, Turner, *Towards A Rational Personal Data Breach Notification Regime,* Information Policy Institute (June 2006), p. 8.

[31] "Survey: Data Breaches Yield Few ID Thefts", Computerworld, September 15, 2006. Found at: http://www.infoworld.com/article/06/09/15/HNidtheft_1.html.

[32] The report was requested by members of the U.S. House Financial Services Committee (Cong. Spencer Bachus, Mike Castle, Darlene Holey, Steve LaTourette, and Dennis Moore), all of whom were co-sponsors of the bill reported by the House Financial Services Committee in the 109th Congress. The full report can be read at: http://www.gao.gov/new.items/d07737.pdf.

[33] The breaches studies involved personal data, including financial data, that could be used to commit identity theft or other related harm. GAO excluded breaches involving other types of sensitive data, such as medical records or proprietary business information.

- Of the 24 largest reported breaches between 2000 and 2005, the GAO found three of the breaches resulted in fraud on existing accounts; specifically, the cases involving CardSystems, DSW and CD Universe, a case stretching back to December 1999. There was evidence in the ChoicePoint case indicating the creation of fraudulent accounts. For 18 of the breaches studied, no clear evidence was uncovered linking them with identity theft. For the remaining two breaches, there was insufficient evidence to make a connection with identity theft.

- "Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges," the report states. The GAO said that consumers notified of a breach could take steps to reduce the risk of identity theft, such as monitoring credit card and bank accounts.

- "At the same time," the GAO said, "breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals," the GAO said. "Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether."

- "... care is needed in defining appropriate criteria for incidents that merit notification. Should [the U.S.] Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk," the GAO said in its report.

In fact, based on this report, and a close examination of reports compiled by entities such as the ID Theft Resource Center, it appears that many breaches pose no real threat to the personal information of individuals and that the requirement for public notification should be carefully crafted.

One other point deserves elaboration. Based on the U.S. experience, a significant number of breaches reported involve government agencies (including U.S. States and the military). In 2009, government agencies accounted for 35.6 % of records breached, according to one source,[34] behind those experienced in the general business category, which was high last year due to the well-publicized Heartland Systems Breach.[35]

We therefore urge that policy recognize the key role that government agencies play in promoting more effective security practices and effectuate steps that minimize the likelihood of data breaches by public authorities:

---

[34] See "2009 Data Breach Stats" published by the Identity Theft Resource Center.
[35] Of the 132,000,000 records reported breached by the ITRC in 2009, at least 130,00,000 were attributed to this one breach.

As of this writing, 46 states (plus the District of Columbia, Puerto Rico and the Virgin Islands) as well as the FTC (under the Health IT Act and through actions under its existing authority[36] for failure to maintain or disclose security practices[37]) and Department of Health and Human Services ("HHS") are implementing data breach regimes.

The following lessons, in our view, are emerging from the implementation of these regimes:

Establish a meaningful threshold for notification to affected individuals. To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when the security of sensitive personal information has been breached in a manner that creates a ***significant risk*** of identity theft. This is the recommendation of consumer protection authorities such as the FTC, for example.[38]

---

[36] E.g., primarily Section 5 of the FTC Act for deceptive and unfair trade practices. See, also, Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA).

[37] To date, the FTC has brought 29 actions against companies that failed to protect consumers' personal information *See, e.g.,* See *Dave & Busters, Inc.,* FTC File No. 082-3153 (June 8, 2010); *See United States v. Rental Research Svcs.,* No. 09 CV 524 (D. Minn. Mar. 5, 2009); *Federal Trade Commission v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of CVS Caremark Corporation*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment); *In the Matter of Genica Corp.*, File No. 082 3113 (Feb. 5, 2009) (accepted for public comment); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[38] In testimony before the U.S. Congress, then-Chairman Deborah Majoras of the FTC stated the view of regulators that: " ... companies ... notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft. Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. ... the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required." Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the

A meaningful threshold predicated on a "significant risk" standard is essential to avoid overnotification of consumers. As then-Chairman of the FTC Deborah Majoras stated in Congressional testimony:

> "The challenge is to require notices *only* when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, ***notices may be more common than would be useful***. As a result, ***consumers may become numb*** to them and fail to spot or act on those risks that truly are significant. In addition, ***notices can impose costs on consumers and on businesses,*** including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally."[39]

In April 2007, the Identity Theft Task Force established by U.S. President Bush,[40] and co-chaired by FTC Chairman Majoras and then-Attorney General Alberto Gonzales and comprised of 17 federal agencies with the mission of developing a comprehensive national strategy to combat identity theft, reached the same conclusion: that a national standard should be established to require private sector entities to safeguard the personal data they compile and maintain and "to provide notice to consumers when a breach occurs that poses a significant risk of identity theft."[41]

The establishment of a meaningful threshold is essential as there may be direct and harmful unintended consequences that may be associated with broad notification. For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and "phishing" attacks when bad actors hear through the media about notifications.

The concern is based on the fact that consumers are being preyed upon by bad actors following massive notifications. In January 2006, the New York State Consumer Protection Board (CPB) advised that scam artists were trying to cash in on the national paranoia over identity theft by luring victims with a phony warning that they may already

---

United States Senate (June 16, 2005), p. 7. Found at: http://www.ftc.gov/os/2005/06/050616databreaches.pdf. (Hereinafter referred to as "Majoras Testimony."

[39] Majoras Testimony at p. 10. (emphasis added)

[40] Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

[41] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), *available at* http.//www.idtheft.gov, p. 4.

be the victims of identity theft.[42] The FTC was compelled to caution U.S. veterans in 2006 "to be extra careful of scams following the recent data breach at the Department of Veterans' Affairs (VA)," noting that "[i]n the past, fraudsters have used events like this to try to scam people into divulging their personal information by e-mail and over the phone."[43]

Such scams follow a simple, but serious pattern: Users may receive emails purporting to come from their credit card company or bank, referencing recent news reports of "breaches", asking them to enter their details and account numbers for the purposes of fraud protection or to reactivate their account. Often emails may even claim a fraud has been committed against the user's account and against the backdrop of a widely reported data breach, many users will assume that news is legitimate.[44]

Careful coordination with enforcement authorities is essential to mitigate harm to consumers in the event of a breach. Based on the practical experience that where a breach occurs it is essential to act rapidly to prevent the subsequent harmful affects, a categorical requirement such as this may be inappropriate, and potentially counterproductive.

The decision as to whether or not individual notification is required in the event of a breach must be based on an analysis of the level of risk of harm on a case-by-case basis. This is absolutely essential, due to the fact that public notification of data breaches is a complex issue with signifiant implications for organization and individuals as well as law enforcement, data protection, and consumer protection authorities.

Where a breach occurs, and there may be a significant risk of identify theft, entities experiencing the breach will need to work in a time-sensitive manner with relevant law enforcement authorities who are empowered to combat computer hacking, consumer fraud and related crimes. It is essential that these vital steps are not impeded by requirements that are not as time sensitive. Moreover, it essential that coordination be required among government authorities.

Define carefully the kind of personally identifiable information that is covered by notification requirements. Central to an effective framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personal information" be the basis for determining whether any notification occurs.[45] Two very important points:

---

[42] See "Phishing Fraudsters Prey on Identity Theft Fears," January 13, 2006, found at: http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html.

[43] "FTC Warns Veterans to Delete Unsolicited E-mails;*Scams via E-mail and Telephone Often Follow Data Breaches*," (June 2, 2006), found at: http://www.ftc.gov/opa/2006/06/fyi0632.htm.

[44] See "Will MasterCard breach breed new wave of phishing?", 21 June 2005. Found at: http://software.silicon.com/security/0,39024655,39131331,00.htm.

[45] In general, sensitive personal information that, if breached, should be subject to notification, should include first and last name in combination with any of the following: (A) Government issued identification number used to facilitate social welfare benefits or the equivalent; or (B) Financial account number or

- It should not include a breach involving elements that are widely used in commerce to facilitate transactions.

- It also makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches on information that is already widely available and in the public domain.[46]

Avoid mandating specific technologies, while encouraging the adoption of good practices. SIIA would urge, as part of a coherent national framework, technology-neutral incentives for businesses to take appropriate and effective steps to safeguard sensitive data. A number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction. To single out one method to secure data in legislation, such as encryption, suggests, if not an outright mandate, then a *de facto* exclusive means to avoid notification, creating a false sense of security. Singling out one methodology would not be in the overall best interests of the security marketplace, since it may reduce the development and use of diverse and innovative security tools. SIIA strongly recommends that "securing the information by a method that renders the data elements unreadable or unusable" is recognized in policy.

Where 3rd parties manage data, and notification is required, avoid consumer confusion. In cases where a 3rd party manages "sensitive personal information" of consumers for entities that own or possess sensitive personal information, notification requirements should be constructed to avoid consumer confusion. The best way to achieve this end is to obligate the third party to notify the entity that owns or licenses the data – i.e., the entity that has the relationship with the person whose sensitive personal information may have been breached. The entity that owns or licenses the sensitive personal information should, in turn, notify the end user or consumer. Otherwise, individuals are unlikely to recognize the source of the notice and thus unlikely to act in a manner to protect themselves, which is the object of notification regimes.

As a final note on this point, SIIA urges the Task Force to focus its attention on a trend where NIST guidance – which was developed for use by federal agencies, and may not be to be evaluated against – is being included in legally binding obligations on private sector entities under Federal data breach regimes. Earlier this year, SIIA wrote to NIST Director Patrick Gallagher[47] expressing deep concern that "the incorporation of the NIST technical guidance and standards by HHS into a mandatory rule not only factually misstates many of their key elements, it also risks degradation of key non-binding

---

credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual's account.

[46] It is noted that the vast majority of U.S. states that have enacted data security breach notification laws (35 of the 39 to date) have included an exception for public record information.

[47] A copy of the letter is found in Attachment A.

technical work that NIST engages in and which is of tremendous value to our industry." It is essential that NIST remain a first class world laboratory. Steps such as those taken by HHS in its "Guidance" risk making NIST a 4th class regulator.

AN EXPANSIVE DEFINITION OF WHAT CONSTITUTES "PERSONALLY IDENTIFIABLE INFORMATION" UNDERMINES IMPORTANT EFFORTS TO BUILD CONFIDENCE ON THE INTERNET AND PRODUCE INNOVATIVE PRODUCTS AND SERVICES

SIIA appreciates that the topic of non-personally identified information is one that is the focus of rich discussion in a variety of venues. Yet, despite the robust discussion underway, there appears to be a trend to expand the scope of privacy and data protection regimes to include *non-personally* identifiable information about individual users, whether they are consumers or business associates, i.e., without regard to the context of the collection, use or disclosure of individual data. This makes compliance not only challenging, but raises serious questions about the balance of achieving meaningful privacy protections with providing essential services and innovation solutions that enhance consumers.

Nowhere is this debate more evident than over Internet protocol addresses. We note, however, that to date no data protection authority or judicial body, to the best of our knowledge, has determined that such an identifier is personally identifiable without examining *the specific context in which an IP address is used*; indeed, data protection authorities and judicial bodies have avoided categorical conclusions in this regard.

The inclusion of IP address in the definition of "personally identifiable information" also fails to recognize that it is a standard data point and absolutely necessary to deliver Web pages and content. It is not personally identifiable, as such.

Moreover, the collection, use and disclosure of Internet Protocol address data, which travels with virtually all Internet communications, is essential to the prevention, investigation and combating of all forms of online misconduct. It is particularly important to preserve the ability to collect and use Internet Protocol address data in cooperative efforts to reduce the unacceptably high levels of trademark and copyright infringement, cybercrime, denial of service attacks, and other illegal and harmful activities online. And it would be difficult, perhaps completely unnecessary – and potentially counterproductive -- to provide notice and consent to Internet users, as has been suggested in some quarters, that their publicly available IP address information may be collected for these purposes.

It has asserted that developments in the EU support the argument that IP addresses are to be considered PII. Despite press reports of high profile statements by leading data

protection authorities,[48] a closer scrutiny belies the broad assertion that IP addresses are categorically considered PII in the EU. The actual discussion of the issue revolves around the purpose and manner in which IP addresses may be associated with *other* information that is not collected from the consumer. In the recent high profile case, *Promusicae v. Telefónica,*[49] the European Court of Justice (ECJ) examined the question whether the Internet Service Provider (ISP) Telefónica should be "ordered to disclose the identities and physical addresses of certain persons who it provided with internet access services, *whose IP addresses and data and time of connection were known*"[50] in the context of a civil investigation that included a request for contact information about individuals using the KaZaA file exchange (peer-to-peer) program to exchange pirated sound recordings. Significantly, the ECJ did not conclude that IP addresses were *inherently* PII as such, because the names and addresses, which did constitute PII, were previously known and linked.[51]

SIIA urges the Task Force, the Department and the Administration to work to make sure that the long-standing availability of this information be explicitly preserved in order to detect and remedy instances of malicious and illegal conduct, including cybercrimes and intellectual property infringement.

THE NOTICE AND CHOICE MODEL REMAINS ESSENTIAL IN THE GLOBAL, ONLINE ENVIRONMENT. CRITICAL SOURCES OF PUBLIC AVAILABLE INFORMATION PROMOTE CONFIDENCE IN THE INTERNET ECONOMY

The NOI inquires whether the notice and choice approach to consumer data privacy is still a useful model.

In short, yes, it remains essential, particularly in the global online environment where entities driving the digital and Internet economy operate across borders and in different jurisdictions. As previously noted, there is a trend to expand the scope of privacy and data protection regimes to include *non-personally* identifiable information about individual users, whether they are consumers or business associates, i.e., without regard to the context of the collection, use or disclosure of individual data. Thus, especially in a business-to-business context, whether dealing with recognized PII or non-PII of business customers, it is essential that the contours of those commercial relationships be able to be managed effectively through a notice and choice model.

---

[48] *See, e.g.*, "European Regulators Mull Protecting IP Addresses," Information Week, January 23, 2008 06:00 AM, found at: http://www.informationweek.com/internet/showArticle.jhtml?articleID=205916731.

[49] C-275.06, 29 January 2008.

[50] Ibid at para. 30 (emphasis added).

[51] See, also, *EMI Records v Eircom Ltd* [2010 IEHC 108], finding that such uses fully compatible with Irish data protection law. Available at: http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d88408025770700350 82f?OpenDocument

The NOI inquires whether a "use-based model for commercial data privacy" could be a basis for defining data protection obligations.[52] SIIA has studied the cited document on a preliminary basis, and will discuss it further with members in light of our experience with US and global data protection, data breach, data security and data retention regimes. As an initial reaction, the paper holds some useful insights into well-established fair information practices. However, it is not clear how this would be a substitute for notice and choice, in light of the well-developed frameworks that predicate data protection on this model. In addition, it is not clear how the approach put forward could be reconciled with non-US regimes, which are based on different assumptions than fair information practices.

Regardless of the model – notice and choice, use-based, or other underlying principle – it is essential that the Task Force, the Department and the Administration work to preserve the use and disclosure of individual data that "enhance the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy," as stated in the NOI.

A few illustrative examples are provided below.

Whois Domain Name Registration Data. As the Task Force is well aware, domain name registration information has been publicly accessible through "Whois" since the earliest days of the domain name system, even predating the World Wide Web.

Access to Whois data is critical to dealing with instances of phishing, distribution of malware, network attacks, and online frauds of all kinds; it is also essential to the investigation and mitigation of copyright piracy and trademark misuse over the Internet. Virtually every Internet user benefits from public accessible Whois, as public access to Whois data is essential to knowing the entity one is doing business with via the Internet.

This policy is recognized not only in the NTIA policy governing the ccTLD .us. It is also recognized in the Affirmation of Commitments that the Department concluded with ICANN last September.[53] It should also be noted that the leadership of the Energy & Commerce Committee – including Chairman Waxman, Chairman Boucher and Chairman Emeritus Dingell – wrote to Secretary Locke[54] last summer with the same vision: that ICANN would remain perpetually accountable to the public via an instrument that should:

---

[52] The NOI cites as one example of a use-based model the paper published by the Business Forum for Consumer Privacy ``A Use and Obligations Approach to Protecting Privacy: A Discussion Document," Dec. 7, 2009, http:/ /www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf.

[53] Moreover, it is essential that the Department not only work to preserve public access to such Whois data, but strengthen its oversight to improve the accuracy, reliability and timeliness of data found in the Whois service.

[54] August 4, 2009, available at: http://www.boucher.house.gov/images/icann%20letter.pdf.

"Ensure that ICANN will adopt measure to maintain timely and public access to accurate and complete Whois information, including registrant, technical, billing, and administrative contact information that is critical to the tracking of malicious websites and domain names."

It is incumbent on the Task Force, Department and Administration to make sure that this policy is also preserved vis-à-vis our global government partners, some of whom have taken the position that publicly accessible Whois is incompatible with the privacy laws of some countries. The positions of these governments threaten to cloud the transparency needed for the digital and Internet economy.

IP Address Information. To reiterate our concerns stated above, the discussion about what constitutes 'personally identifiable information' remains a central challenge to the implementation of data protection regimes domestically and globally.

In the context of this discussion, the collection, use and disclosure of IP addresses is extremely important to combating cyber crimes, online fraud, denial of service attacks, copyright piracy, trademark infringement, and other forms of harms to consumers misconduct carried out online.

It is essential that the Task Force, the Department and the Administration engage actively on these issues, both in the development of U.S. privacy law and policy, and in consultations with our trading partners, to ensure that that the "personal data" rubric is not counterproductively extended to impede responsible use of IP address data to detect and deal with instances of online conduct and crimes.

ATTACHMENT A

Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

March 5, 2010

The Honorable Patrick D. Gallagher, Director
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 1000
Gaithersburg, MD 20899-1000

Dear Dr. Gallagher:

On behalf of the members of the Software & Information Industry Association (SIIA), I am writing to bring to your attention our concerns with the misapplication of NIST technical guidance and technical standards by the Department of Health and Human Services (HHS) last year when it published guidance on technologies to secure personal health information.[1] As we explain below, the incorporation of the NIST technical guidance and standards by HHS into a mandatory rule not only factually misstates many of their key elements, it also risks degradation of key non-binding technical work that NIST engages in and which is of tremendous value to our industry.

A legal safe harbor is designed to encourage good practices, not merely to avoid notification. As such, the Interim Final Rule Guidance does not achieve the purposes of the Safe Harbor by relying on inapplicable NIST documentations and processes, many of which cannot be technically adhered to in the manner asserted in the Interim Final Rule Guidance.

We respectfully request that NIST, along with your colleagues at the Department of Commerce, work with others in the Administration's interagency team implementing the Health IT portions of the American Recovery and Reinvestment Act of 2009 (the "stimulus Act") to address these inaccuracies and misapplication of NIST documents. With HHS likely to update its guidance, and a report to Congress on the health data security provisions of the stimulus bill possibly underway, we also urge the interagency review of the guidance before any report is provided by HHS as required by law.

---

[1] Section 13402 of the American Recovery and Reinvestment Act of 2009 required the Secretary of Health and Human Services (HHS), within 60 days of its enactment, to issue "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements".

Despite HHS issuing the guidance within that time frame, the substance of the Guidance proved extremely problematic. SIIA commented at two specific stages of the HHS rulemaking process, outlining the concerns were share today. At no stage did HHS address the substance of these comments. And the guidance, as published by HHS remains essentially unchanged and of deep concern.

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

CONCERNS WITH THE GUIDANCE

SIIA raised this substantive issue in our prior comments, but HHS did not specifically address it in its analysis.[2]

First, the Interim Final Rule Guidance conditions a legal safe harbor on compliance with documents and processes of the National Institute of Standards and Technologies (NIST) that were not intended to be used in this manner.[3] We strongly urge that any reference to NIST in the Guidance be removed to the degree that it implies that the legal basis of the 'safe harbor' reflected in the Guidance is predicated entirely on implementation of the NIST publications and validation procedures.

All of the work done by NIST incorporated into the Guidance was undertaken in the context of NIST's statutory mandate, which is in furtherance of its responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. Thus, "NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all *agency* operations and assets."[4] As such, "This guideline has been prepared for use by *Federal agencies*. It may be used by nongovernmental organizations on a *voluntary* basis..." (emphasis added) It is inappropriate, and outside of HHS' authority, to require private entities to abide by the requirements of FISMA. This fundamentally alters FISMA's statutory mandate.

The Guidance also states in this regard, in Section II.B(a)(ii), that entities must comply with "valid encryption processes for data in motion .. [which] may include others which are FIPS 140-2 validated." The reference to FIPS 140-2 is not a focus on a "technology or methodology", but instead a reference to specific products, which is not found in the ARRA. This Guidance, in essence, selects winners and losers in this marketplace, rather than allowing the best technology to thrive. Moreover, choosing static products in this dynamic field undermines the goal of protecting health information as there is no incentive for our members to adopt newer technology that might be more secure, if to do so prevents our members from availing themselves of the safe harbor.

---

[2] HHS does state "that any further comments regarding this guidance received in response to the interim final rule will be addressed in the first annual update to the Guidance, to be issued in April 2010." However, this mention does not address the factual issue raised previously to HHS, and leaves the current Interim Final Rule Guidance faulty and inconsistent with the requirement that a rulemaking address factually substantive issues.

[3] HHS asserts that "the guidance on securing protected health information is not mandatory; it is discretionary" but recognizes that "many covered entities and business associates are voluntarily choosing to secure their protected health information in accordance with the guidance in order to avoid the possibility of having to provide breach notifications pursuant to this subpart." (emphasis added) HHS misses the mark in its analysis on this point. First, HHS provides no evidence to this effect, as we explain in our letter, the Special 800 Series are neither designed nor intended to be used in this way.

[4] "...but such standards and guidelines shall not apply to national security systems."

Finally, FIPS are developed and adopted by NIST as a standard that "is applicable to all *Federal agencies* that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106." While "this standard is available to private and commercial organizations," FIPS have never been imposed by federal rule or regulation as a predicate to a legal obligation, liability or safe harbor on commercial implementations.

It is our view that it is beyond the authority provided in the Recovery Act for HHS, as a condition of a legal safe harbor, to impose on the commercial sector Special Publication requirements, many of which are not even mandatory to Federal agencies.[5]

Second, the Guidance states factually inaccurate information about a number of NIST Special '800 Series' Publications. The Interim Final rule Guidance asserts that the "encryption processes identified [in the NIST publications] have been *tested* by NIST and *judged* to meet this standard [the provisions of the Stimulus Act cited by HHS]."[6] (emphasis added)

This statement in the Guidance is factually incorrect. Without prejudice to the useful technical analysis that is provided in these Special Publications and the well recognized role of NIST as a facilitator with industry in this important area, *nothing in these documents has been "tested" nor been "judged" to meet a particular standard.* On the contrary, the entire "Special Publication 800-series" reports on NIST's Information Technology Laboratory's *research, guidance, and outreach efforts* in computer security and its collaborative activities with industry, government, and academic organizations." The "800-series Publications" are distinct from other NIST responsibilities which "include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems." (emphasis added) In developing the "800-series Publications", NIST has carefully refrained from labeling these Special Publications as even 'best practices.'

Third, the Guidance incorporates documents which are not designed to be nor in fact capable of being evaluated against. The Guidance imposes on affected entities a virtually impossible burden: to benefit from the safe harbor, they must show they meet often inconsistent, generally designed 'requirements' found in documents which have neither been subject to comment and review, much less the requisite scrutiny that is required for 'assessments' Thus, a company may have implemented some of the

---

[5] The implication of HHS imposing these documents on commercial implementations raises profound questions about the process that NIST has gone through in the development of Special Publications. If HHS were to require, as provided in the Guidance, conformance to these documents, each of these documents would have to be opened up for a formal notice and comment process. None of these documents are the product of such a process.

[6] This language is identical to that in the earlier draft Guidance, and remains unchanged – without any explanation.

elements of the "research" that are found in the Special Publications, but not all of them, but enough to make data unusable, unreadable or indecipherable. As such, it is not clear from the language in the Guidance whether this is satisfactory.

As a general matter, SIIA is deeply concerned that the Guidance gives legal benefit only to those processes that have been tested (or, of deeper concern, *'certified'*) in satisfaction of the Guidance. Nothing in the authority given HHS under the ARRA permits the imposition of testing or certification requirements, *even if HHS could demonstrate that such conformance were technically possible using common place evaluations – which it has not, and we would add, could not be done.* Additionally, nothing in the record establishes that such tests or certification is a necessary prerequisite to benefitting from the safe harbor established in the Guidance.

We appreciate the hard work of NIST on so many fronts that are important to our industry. And we very much appreciate your consideration of our concerns. We strongly urge an appropriate adjustment to the use and characterization of the Guidance in this Rule, and a continued collaboration with NIST on the many issues of importance to our industry.

Sincerely,

Mark Bohannon
General Counsel &
Senior Vice President, Public Policy

cc: Aneesha Chopra, Chief Technology Officer, White House

Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

June 14, 2010

Honorable Barney Frank
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Honorable Christopher Dodd
Chairman
Committee on Banking, Housing and Urban Affairs
U.S. Senate
Washington, DC 20510

Dear Chairmen Frank and Dodd:

I am writing on behalf of the Software & Information Industry Association (SIIA), to express my concern that our member companies may have difficulty in accessing the public debt markets because of Section 933(b) in the *Restoring American Financial Stability Act* currently being finalized in your conference proceedings.

SIIA is the principal trade association of the software and digital information industry, with more than 500 members that develop and market software and electronic information content for business, education, consumers and the Internet. SIIA's members include software companies, e-businesses, and information service companies, as well as many electronic commerce companies.

SIIA members have led the way in establishing and expanding our nation's information infrastructure – a key to sustained economic growth in the 21st Century. Like many new and emerging markets, our members have and will continue to depend on access to the public debt markets in order to expand the suite of innovative products and services available to American citizens. We are, however, concerned that our member companies may have difficulty in accessing the public debt markets because of Section 933(b) in the *Restoring American Financial Stability Act* currently being finalized in your conference proceedings.

Specifically, we believe there may be unintended effects of Section 933(b) because it places discriminatory liability burdens on credit rating agencies by exposing them to an unprecedented, new "state of mind" standard for securities fraud claims under the 1934 Securities and Exchange Act. These provisions would establish a standard different than that which has applied to any other market participant and therefore could force rating agencies to become more defensive in the issuance of ratings, possibly substituting litigation concerns over independent analytic judgment. They will therefore likely be less willing to rate debt in new and emerging markets, including innovative software and information technology firms. Without such ratings, our companies are likely to find it much more difficult to access the public debt markets, resulting in significant increases in capital costs that will slow the pace of innovation and economic growth.

We therefore respectfully urge that Section 933 be deleted or redrafted. The provision should ensure that credit rating agencies provide ratings that maintain strong investor protection against intentional bad faith acts without causing disruption in the quality and timeliness of robust ratings that are, and will remain, so important to our members.

Thank you for your consideration of this request.

Sincerely yours,

Ken Wasch

Ken Wasch
President

Cc: Members of the Conference Committee

Tel: +1.202.289.7442
Fax: +1.202.289.7097