

Prepared Statement of Dan Maurer¹
Intuit, Inc.

I am Dan Maurer, senior vice president and general manager of the Consumer Group of Intuit Inc., which includes our TurboTax consumer tax and Quicken personal finance businesses.

The electronic tax preparation and filing industry has grown and steadily evolved over the past several decades. The industry has delivered fundamental improvements in tax compliance and administration by enabling tax preparers and taxpayers to utilize innovative information technology tools to prepare tax returns with significantly more accuracy and substantially less burden (including both the time and cost of compliance), all while simultaneously slashing the approximately 20% error rate associated with paper and pencil returns filed through the U.S. Mail down to only approximately 1% in computer-generated, electronically filed returns.

The industry's technology innovation has also aggressively driven consumer adoption of electronic filing, which has not only simplified tax compliance but helped both federal and state income tax administrators sharply reduce the operating cost of return processing and increase the accuracy of the taxpayer information in their databases.

In short, the innovation and investment of the private technology sector, in partnership with government, has fundamentally reinvented income tax compliance over the last 25 years. This is a significant success story here in the United States, and we've been proud to work with government at all levels to help make this innovation journey a reality.

A. THE SOFTWARE INDUSTRY – COMPOSITION, INNOVATION & BENEFITS

The electronic tax preparation and filing industry (referred to generically as the “software industry”) that enables our system of electronic tax administration includes a large number of software developers that create tax-related software tools for both professional preparers and “do-it-yourself” consumers. These software developers are primarily commercial information technology companies, but they also include some publicly-funded entities that range from certain community-based organizations to some state government departments of revenue. The number of commercial software developers in the marketplace today is quite significant. We estimate the consumer software segment alone includes over thirty companies offering online software tools that enable taxpayers to self-prepare their individual returns quickly and easily. Several developers also offer “boxed” software that is installed and used locally on a consumer's desktop or laptop computer. Moreover, the range of software tools available facilitates the preparation of not just individual income tax returns, but also of business income tax and payroll tax returns.

¹ This Statement supplements Intuit's written comments submitted to IRS dated August 31, 2009.

The professional tax software segment also includes several companies that develop and offer installed-software and online tools for tax professionals to use to prepare returns for clients that are individuals, corporations, partnerships, and other types of entities. In addition to offering full-featured tax preparation software, several companies develop “tax utility” software, which are specialized applications that calculate specific tax areas or complete specific forms such as Schedule D.²

In addition to software developers, the software industry also includes the transmitters who operate the substantial technology infrastructure, including the application software, data center and customer service operations, required to electronically receive, process, transmit, acknowledge and resubmit tax returns with the Internal Revenue Service and states.

The competitiveness of the technology sector and software industry drives constant innovation in the tools of tax compliance, which over time have significantly reduced taxpayer burden while increasing return accuracy. For example, many tax software companies enable connected services that support the electronic importation of W-2 and 1099 information reports directly from source companies such as payroll providers and financial institutions. This innovation alone both increases accuracy and reduces tax preparation burden. Another innovation trend over the past several years is the extension of tax software into the “online environment,” which includes not just the remote use of a software developer’s Web-based application but, primarily in the professional segment, also the hosting of “desktop” applications on remote servers. Finally, competitive innovations across the consumer tax software segment have resulted in the wide availability of free online tax preparation and electronic filing, generally for simpler tax returns.

Finally, the innovations of the software industry benefit tax administration in many ways. As compared to manual preparation using IRS forms and publications, consumers benefit from increased accuracy and sharply reduced compliance burden, preparers benefit from increased accuracy and speed of preparation and, finally, the IRS and state departments of revenue benefit from both more accurate tax returns and significantly reduced operating expenses.

B. CURRENT REGULATION OF THE SOFTWARE INDUSTRY

The software industry today is subject to considerable regulation and oversight but, as with so many things, there is room for improvement and enhancement in the furtherance of the public interest.

Existing public protections include, but are not limited to numerous federal and state consumer protection, advertising and privacy laws, including the Federal Trade

² See, for example, the broad scope and character of tax utility software offered by one company, CFS Tax Software, Inc. (www.taxtools.com).

Commission Act³ and numerous state “unfair competition” laws. Additionally, tax software companies are subject to IRS electronic filing regulations, which extend the requirements and penalties of various laws and regulations to Authorized IRS efile Providers in the following areas:

- *Authorization to operate*...under Revenue Procedure 2007-40 and related IRS Publications 3112 and 1345, including the Participants Acceptance Testing System (PATS) and back ground checks.
- *Privacy*...under the Federal Trade Commission (FTC) Privacy Rule,⁴ the Gramm-Leach-Bliley Act,⁵ and, of course, Internal Revenue Code (IRC) Section 7216⁶ and its associated regulations,⁷ which were comprehensively updated in recent years.
- *Security*...under the FTC Safeguards Rule,⁸ and of course the new IRS Security rules which have been promulgated in just the last year.
- *Professional or performance standards*...under IRS Publications 3112 and 1345, including certain advertising standards and other preparer responsibilities such as those found in IRC Sections 6694 and 6695.⁹

One other significant consideration should not be overlooked – commercial software developers operate and compete in the open marketplace, where customers can vote with their feet. Every year, taxpayers and tax professionals make a choice about which software company they will use. The cost of acquiring new customers in a highly competitive industry such as this one is significant. Ultimately, companies can only succeed by serving their customers well and earning their confidence and loyalty year-over-year. Significant brand damage is incurred when fundamental performance expectations are not met. Therefore, we believe taxpayers themselves wield the ultimate penalty – they can choose to use a competitor when a company fails to meet their needs and expectations.

Nevertheless, the industry’s increasingly important role is accompanied by potential risks, as recently suggested in a GAO report, particularly in the areas of security, privacy, accuracy and reliability.¹⁰ Therefore, the software industry has a responsibility to ensure

³ 15 U.S.C. §§ 41-58. The FTC Act has provided the basis for legal enforcement actions in a broad range of areas. For example, The FTC Act (and the FTC Safeguards Rule) has been the basis for aggressive enforcement action by the FTC for both security breaches (<http://www.ftc.gov/opa/2008/03/studlend.shtm>), as well as for deceptive claims concerning security and privacy policies (<http://www2.ftc.gov/opa/2008/01/lig.shtm>).

⁴ 16 C.F.R. Part 313

⁵ Also known as the Financial Services Modernization Act of 1999 (Pub. L. 106-102, 113 Stat. 1338, enacted November 12, 1999).

⁶ 26 U.S. Code 7216

⁷ In addition to its “penalty” aspects, IRC 7216’s implementing regulations and revenue procedures in effect establishes a “performance standard” because of their extensive requirements concerning the use and disclosure of tax return information and obtaining taxpayer consent. See 26 CFR Section 301.7216 and IRS Revenue Procedure 2008-12.

⁸ 16 C.F.R. Part 314

⁹ 26 U.S. Code 6694 & 6695.

¹⁰ “Tax Administration: Many Taxpayers Rely on Tax Software and IRS Needs to Assess Associated Risks” (GAO-09-297 dated February 2009).

that both taxpayers and policy makers have confidence that the tax software tools and electronic filing systems it provides will deliver accurate calculations, protect the confidentiality of tax return information, and operate in a highly secure and reliable manner.

We believe this is a good time to take a fresh look at industry standards and oversight, and we support the Commissioner’s Tax Preparer Review initiative to strengthen the integrity of the tax system, to increase taxpayer compliance, and to ensure uniform and high ethical standards of conduct.

C. REGULATORY PRINCIPLES & FOCUS

Regulation and oversight serve a vital interest. When properly designed and implemented, regulation advances important public interest objectives that outweigh the cost and burden of such regulation to consumers, tax professionals and industry. Conversely, when regulations are not thoughtfully designed and implemented, they can drive unanticipated outcomes that increase costs and complexity, reduce innovation, and alter behaviors in unexpected ways – all without bringing the corresponding intended benefits. Those cautionary realities should not cause us to shrink from the need to act in the public interest, but they should inform and guide public policy strategies to make the best choices possible among available alternatives in a phased, deliberate manner. For this reason, the Tax Preparer Review initiative that IRS leadership has undertaken is a very important and valuable process to optimize the opportunity to get this right.

We believe there are two key operating principles underlying proactive oversight: (i) *Standards*, which set the expected level of performance, and (ii) *Certification*,¹¹ which proactively verifies and evidences compliance with recognized standards. Certification has two elements. The first element is the structured, consistent methodology by which compliance with the standard is verified, which could vary depending on the nature and significance of the particular standard. For example, the methodology could be some type of structured assessment in a consulting engagement or, alternatively, a more rigorous form of attestation such as an agreed upon procedure or audit. The second element is the formal recognition or issuance by an appropriate body that, based on the verification methodology, reflects the party being certified is compliant with the standard.

As the IRS considers the best ways to shape an oversight strategy that would optimally serve both the taxpayer and the income tax system itself, Intuit believes certain principles should guide this important initiative:

- Any standards and oversight model should leverage and derive maximum benefit from existing, proven oversight models, existing rules, law and regulation, and well-established industry best practices.
- Any new standards should focus on high level requirements, assurances and controls, rather than setting an overly prescriptive approach or detailed

¹¹ As used in this statement, “certification” is intended to be a generic reference to a verification and recognition process, and is not meant to have any particular, specialized meaning under some existing government or industry certification process.

specifications that effectively result in government design or operation of technology products, services and functionality for American consumers and tax professionals.

- Any standards must recognize that shared accountability is the hallmark of a voluntary compliance tax system, including the responsibilities of preparers and taxpayers in using software as a compliance tool.
- An effective standards and oversight model must be designed to ensure that tax software companies are not prevented or constrained from their ability to continue to rapidly respond to needs and requirements in an increasingly dynamic tax environment, frequently dealing with late passing legislation, new government economic policy initiatives, and the emerging needs of both taxpayers and revenue agencies.

In our view, the principal risks identified by GAO with regard to the software industry are technology-related issues – security, privacy, accuracy and reliability. Technology risks in the information age are not unique to the tax environment or to the private sector alone. However, we believe the challenge presented by these risks also creates an opportunity for a proactive oversight approach based on shared learnings and commercial best practice standards and certification models, while organizing and rationalizing established rules and regulations in a coordinated structure for greater synergy and effectiveness.

D. REGULATION: STANDARDS & CERTIFICATION

To be successful and effective, any adopted strategy must preserve the environment for – and actually encourage -- continued innovation in the technology industry in the further development and invention of tax preparation tools. Moreover, a thoughtful strategy will preserve the industry’s inherent rapid response core competency that represents a significant asset in the American income tax system today.

To achieve these critical objectives and more, Intuit believes there are four key areas where IRS should focus its oversight – Security, Privacy, Accuracy and Reliability. We also believe that the two key operating principles -- Standards and Certification -- must be applied across all four of these areas to make any oversight meaningful and to provide confidence to taxpayers and policy makers. Let me begin by discussing Security.

1. Security.

The protection of taxpayer information is foundational to achieving taxpayer trust and confidence in electronic tax preparation and filing. Security is a critical priority in the modern world for government, industry and citizens alike. Currently, all Authorized efile Providers are subject to the FTC Safeguards Rule, which requires them to “develop, implement, and maintain a comprehensive information security program.” Additionally, IRS has promulgated its own security requirements for Authorized IRS efile Providers in IRS Publication 1345.

The FTC Safeguards Rule outlines the requirements for a comprehensive information security program, and provides a sufficient regulatory structure for many types of companies and activities. However, its application across a broad range of companies requires that it be necessarily general. Given that fact, the Safeguards Rule provides little to no guidance concerning particular types of security controls that should be implemented and does not require any type of proactive third-party review, verification or associated certification.

In the area tax administration, we believe IRS could implement a more proactive approach to securing sensitive tax return information. In fact, IRS recognized the value of having a data security framework in Revenue Procedure 2008-35 (http://www.irs.gov/irb/2008-29_IRB/ar13.html) in which it required “adequate data protection safeguards” in connection with certain permitted disclosures of tax return information outside of the United States. We believe IRS should consider setting clearer security requirements in the area of tax administration by specifying those frameworks that would provide an adequate data protection safeguard.

Intuit has two key recommendations for IRS in the security area:

- Specify a recognized industry security standard as the relevant data protection safeguard (standard) that all software and electronic filing companies must implement.
 - ISO 27000 series (formerly ISO 17799) is one clear example of a recognized, comprehensive standard – it was consulted in establishing federal government’s FISMA standards,¹² is frequently referenced by federal government security organizations such as the National Institute of Standards and Technology (NIST), and is applicable to some government organizations.¹³
 - The focus should be on a “controls based” framework that sets the right outcomes, but enables companies to respond quickly in a fast-moving security environment – it therefore must not be an overly prescriptive directive or based on specific technologies. Cyber-security strategies and technologies necessarily change rapidly to meet emerging threats, and preserving the industry’s ability to respond is essential.
 - The application of an existing, recognized industry standard avoids layering “new” requirements on companies that might create either duplicative activities or unnecessary expense.
- Require that a recognized, qualified, reputable and independent security company or major accounting firm periodically verify a company’s implementation of any required security standard or framework, and issue an associated certification.

¹² “The security controls in Special Publication 800-53 have been developed using inputs from a variety of sources including...ISO/IEC Standard 17799...” See <http://www.csrc.nist.gov/groups/SMA/fisma/controls.html> (ISO 17799 is the predecessor to ISO 27002).

¹³ See NIST Special Publication 800-53 Rev. 3, Appendix H. In fact, NIST has a “harmonization Initiative” underway to identify common relationships and the mappings of FISMA standards, guidelines and requirements with ISO 27000 series information security management standards to minimize duplication of effort for organizations that must demonstrate compliance to both FISMA and ISO requirements. See <http://www.csrc.nist.gov/groups/SMA/fisma/overview.html>

- Several highly competent security companies and accounting firms conduct security related reviews, assessments, audits and certifications. A good example is the “SAS 70 audit” which is frequently relied on by financial services companies to demonstrate compliance to federal banking regulators.
- Leveraging existing, recognized third-party private industry experts and practices ensures an independent assessment of compliance and a uniform standard of quality, while enabling companies to minimize duplication of effort and cost.

One final observation. Security is not a destination – it is business discipline and culture, reflected in not only standards but in the mindset of business leaders, policies and practices -- it is a continuous journey. No organization, public or private, ever “achieves” 100% security. Instead, as evidenced by the challenges experienced by government itself,¹⁴ security is an ongoing, continuous effort that requires significant operational diligence and top management attention.

2. Privacy.

Safeguarding the privacy of taxpayer information is essential to maintaining public confidence in electronic tax administration. Fortunately, there are high standards to protect the information of American taxpayers.

First, tax return information is subject to what has long been described as the toughest privacy law on the books – Internal Revenue Code 7216. Second, tax software companies are also subject to the FTC Privacy Rule.

The IRS Free File Program requires independent certification of participating software companies’ compliance with their privacy obligations. We believe that requirement should be extended across the entire software industry.

Given the recognized rigor of the 7216 rule, Intuit recommends that in the privacy area IRS should:

- Require that all electronic tax companies obtain a recognized privacy assessment from a qualified, reputable and independent privacy company.
 - Such an assessment program must have verifiable substance and discipline. The best example may be the TRUSTe Privacy Seal program, which requires continuous business accountability through ongoing technology scans and other processes to verify compliance, provides a customer complaint and resolution program, including an escalation process through its ability to directly engage regulatory enforcement agencies such as the FTC or IRS to mandate and enforce privacy compliance.

¹⁴ See, for example, GAO Testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives: “INFORMATION SECURITY: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist” (GAO-09-701T, released May 19, 2009)

Public confidence in the privacy and safety of their tax return information is an essential foundation of our Voluntary Compliance tax system, and going forward efforts should enhance that confidence through verification and associated certification by leveraging recognized, effective mechanisms for meaningful accountability.

3. Accuracy.

The accuracy of the calculations in tax software and utilities is critical to build taxpayer confidence and produce reliable outcomes. Tax software accuracy is not a coincidence. It results from the proactive management of the inputs, process and outputs of the comprehensive tax software development system, including:

- Having highly qualified tax experts, as well as software and design experts, on the development staff;¹⁵
- Researching and analyzing tax law diligently (including engagement with IRS tax experts);
- Having effective customer learning and design processes, that enable the development of a deep understanding of consumer and professional users;¹⁶
- Having rigorous software development processes;
- Conducting robust software testing,¹⁷ and
- Conducting exhaustive consumer/taxpayer research, including usability testing.

Some might propose that the government should prescribe tax software development or technical and user interface design practices, and “certify” software. We believe this sort of approach would not only be significantly suboptimal but, in fact, a potentially damaging approach that would actually present high risk to timely and accurate tax administration outcomes without improving accuracy.

Software development methodologies are in a constant state of evolution, as illustrated by the introduction of “agile” development methodologies¹⁸ versus traditional “waterfall” software development methodologies. Government intrusion into software development

¹⁵ For illustration, Intuit has about 200 tax professionals working on its consumer tax software products alone, including approximately 100 CPAs, EAs and other certified professionals (California Tax Education Council certifications), with an average of tax experience of approximately 14 years, as well as over 200 design and software development professionals with expertise in a broad range of technologies.

¹⁶ For illustration, in addition to reviewing and acting on customer feedback, Intuit invests millions of dollars in funding and resources to conduct extensive consumer and professional user research throughout the year using a variety of research methodologies, e.g., field research (such as “follow me homes” and “follow me to the office” to observe taxpayers using software in their personal environments, which are much different than usability labs), design collaborations with taxpayers, in-depth interviews, focus groups, online studies and surveys, beta testing, A/B testing, laboratory research, etc.

¹⁷ Rigorous testing processes go well beyond PATS testing, and include the creation and updating of thousands of test cases to fully cover legislative requirements, conducting a robust regression test suite including automated and manual test cases, functional and compliance testing, customer usability studies, and alpha and beta testing.

¹⁸ Agile methods generally promote a disciplined project management process that encourages frequent inspection and adaptation, a leadership philosophy that encourages teamwork, self-organization and accountability, a set of engineering best practices that allow for rapid delivery of high-quality software, and a business approach that aligns development with customer needs and company goals.

methodologies and practices could hinder product innovation and increase software development costs, while resulting in software that is actually more defective and costly. Similarly, government intrusion into software design (or specifying the user experience) presents other significant risks. In our decades of experience working with consumer and professional users, a screen or functional implementation that appears to be the “best” approach is often, in the user’s experience, not the best approach. User experience design, and the practical understanding that the user derives from the experience, is both an art and a science that requires significant investment and rigorous pre-release testing. Even with the most aggressive pre-release design testing, software developers never know for certain about the viability of the design and the resulting user experience until the product is in the hands of thousands of actual users.

Intuit has four key recommendations for IRS in the accuracy area:

- Require that all tax software companies have “highly qualified” tax professionals on their permanent staffs to research the tax laws, and review and approve their tax software products, e.g., at least CPA or EA.
- Work with the tax software industry to develop a set of controls-based tax software development best practices, the implementation of which could be reviewed and validated by third-party experts.
 - The focus should be on a “controls based” model that specifies the right high-level development requirements, but enables companies to respond quickly in a fast moving tax development environment – it therefore must not be an overly prescriptive directive or mandate certain methodologies or technologies.
- Leverage IRS’ current “software scorecard” processes to identify potential accuracy issues that might arise with specific software products, whereby IRS and the affected company can investigate software accuracy issues and take appropriate remedial action.
- Implement a formalized mechanism for ongoing collaboration between IRS and industry by creating a permanent ETAAC Subcommittee that would serve as a joint working group to address mutual tax software issues and needs as they emerge over time, providing a vehicle to identify and review, share information, and collaborate on action-oriented solutions as appropriate.

4. Reliability.

As with software accuracy, the reliability of tax administration systems requires exceptional people, process and technology.

From a standards perspective, reliability requires the high availability of core data center facilities. Tax applications must be hosted in secure and highly available (“99.999%” or “five nines”) core data center facilities that offer less than 5 minutes of downtime per year, which are supported by redundant and back-up power supplies, independent electrical generation capabilities, cooling and ISP/network access.

But, that’s not enough. In our experience, to be highly reliable, companies must also execute rigorously across a range of “IT service management” initiatives, including:

defining operational requirements (availability, security, compliance); building and testing systems to meet peak scalability requirements (capacity planning); identifying single as well as multiple points of failure and planning for contingencies; executing effective release & change management processes; diligently monitoring systems to enable the rapid detection of problems; and, having clearly defined and effective incident and problem management processes.

Additionally, companies must also have a highly reliable technology infrastructure including: redundant and diverse systems and networks; robust technology components (e.g., server hardware, operating systems, network infrastructure, databases and storage); and, expert teams of IT professionals staffed around the clock including in-house subject matter experts supplemented by strategic partnerships with key hardware and software vendors).

Currently, we are unaware of any IRS standards governing the “operational reliability” of electronic tax companies.

In industry generally, there appear to be a variety of potential sources of best practices and standards for IT service and infrastructure management including ITIL,¹⁹ the Uptime Institute,²⁰ the Microsoft Operations Framework,²¹ components of ISACA's CobIT framework²² and, finally, ISO 20000.²³

However, current industry standards and practices in this area seem to be evolving, and there does not appear to be any single recognized “dominant” industry standard for IT service management and technology infrastructure. Neither does there appear to be a clearly recognized method of “certifying” companies to any particular standard, which should be based upon assessment and verification of actual practices.

Fortunately, the U.S. electronic tax infrastructure is by its nature highly distributed and redundant, and has served taxpayers reliably. In its report, GAO noted that “...*IRS has multiple filing options and has not experienced similar disruptions large enough to significantly affect returns processing,*” but that “*it does not know the potential for such disruptions or the likelihood of their occurrence.*”²⁴ (The reference to “similar disruptions” is related to the serious system failures with the highly centralized government operated national online tax filing systems of Canada and Great Britain).

¹⁹ ITIL stands for Information Technology Infrastructure Library. See <http://www.itil-officialsite.com/home/home.asp>

²⁰ See <http://www.uptimeinstitute.org/>

²¹ See <http://technet.microsoft.com/en-us/library/cc506049.aspx>

²² See

<http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=79>

²³ See http://www.iso.org/iso/catalogue_detail?csnumber=41332

²⁴ “Tax Administration: Many Taxpayers Rely on Tax Software and IRS Needs to Assess Associated Risks” (GAO-09-297 dated February 2009), page 18.

Intuit believes that, despite the reliability of the distributed, decentralized US electronic tax preparation and filing systems to date, the risks associated with tax system availability and reliability should not be ignored.

Given its critical importance, Intuit has two key recommendations for IRS in the reliability area:

- Tax applications should be hosted in secure and highly available (“99.999%” or “five nines”) core data center facilities that offer less than 5 minutes of downtime per year, which are supported by redundant and back-up power supplies, independent electrical generation capabilities, cooling and ISP/network access.
- IRS should, over time, engage with industry to evaluate best practices in IT service and technology infrastructure management and, in the future, consider the opportunity to adapt and apply such emerging standards to IT service management and operational reliability as they become more generally recognized.

E. OVERSIGHT MODEL

We believe a Self Regulatory Organization (SRO) that operates outside of Government, but is overseen through standards and certification requirements provided or approved by Government, is a tried and tested mechanism for a great many industries that has served the public interest well and is the optimal strategy that should be adopted.

The needs and requirements for providing training and education, proficiency testing, dispute resolution, certification and licensure of tax practitioners, paid preparers and volunteer agents logically lead to development of an oversight model that is specific to those needs and requirements. In this instance, Intuit believes the characteristics and needs of overseeing the live tax preparer community and those necessary for oversight of the electronic tools and technology systems provided by the tax software industry are quite different. However, although the differences between the tax preparer industry and the technology industry are significant, they should simply dictate that any new IRS oversight strategy must have sub-components to it that appropriately address both environments and modalities.

In defining the role of an SRO in broad terms, we believe IRS must carefully consider a number of areas including:

- Scope – the scope and nature of regulatory responsibilities to be performed by the SRO
- Powers – the powers granted to the SRO to execute its responsibilities
- Expertise – the expertise of the SRO’s staff to execute its responsibilities
- Funding – the level and reliability of funding required by the SRO to execute its assigned responsibilities
- Governance – the method and composition of the governance structure to ensure good and timely decisions are made
- Enforcement – the ability of enforcement mechanisms to ensure compliance, whether executed by the SRO or by government agencies

- Government oversight – IRS should provide regular oversight of the SRO’s operations

In terms of the specific functioning of an SRO with regard to tax software industry, there is a clear opportunity to leverage the many existing industry standards, rules, requirements and certification processes, together with a range of existing government regulations, rules and requirements, in order to establish and operate a new SRO with the necessary level of oversight and assurance.

We believe the key features of any “Electronic Tax SRO” are:

- Should be separate and differentiated from SRO structure and activities overseeing “human” tax preparers, given the substantial differences in the relevant standards and oversight methods.
- Should specify standards along with review and verification processes, which would lead to or result in associated certification, for electronic tax companies, covering areas such as security, privacy, accuracy and reliability.
- Should leverage and rely upon recognized standards, rules and regulations, public and private, organizing them in a coordinated, structured and understood framework.
- Should focus on the administration of IRS requirements for electronic tax companies, and leverage and rely on other centers of particular third party expertise to conduct verifications, upon which actual certifications would be based.
- Should validate the completion of and compliance with any requirements by electronic tax companies (software developer or transmitter) as a pre-condition for any company becoming an Authorized IRS efile Provider.
- Could initially investigate any potential violations of specified IRS regulations, but refer any apparent violations to IRS for final investigation, enforcement or other disciplinary actions.
- Should benefit from an ongoing dialogue and collaboration between IRS and the technology industry through an ETAAC permanent Working Group which would address issues and help define standards to address emerging needs and developments over time.

F. CONCLUSION

Unlike the circumstances of traditional preparer oversight involving testing and education, we believe the oversight of the tax software industry is a new area for IRS in many respects. As a result, the risk of “mis-regulation” and unintended consequences is significantly higher. We strongly recommend that IRS take the opportunity to engage with companies and technology associations in the tax software industry to better understand how the information technology sector uses people, processes, research and technology to support software development, security and operations.

We look forward to working together with IRS to advance the public interest, and appreciate this opportunity to share our views.