The Computing Technology Industry Association

"The State of Federal Information Security"

Committee on Oversight and Government Reform

Subcommittee on Government Management, Organization, and Procurement

U.S. House of Representatives

Tuesday, May 19, 2009

Dear Chairwoman Watson, Ranking Member Bilbray, and Members of the Committee:

On behalf of the Computing Technology Industry Association (CompTIA), we thank you for your ongoing interest in the "State of Federal Information Security." This is a broad, yet critical subject ranging from the "Federal Information Security Management Act of 2002" ("FISMA") (P.L. No. 107-347), as well as a variety of practices that impact our national security, citizenry, and the computing industry at large. We appreciate the opportunity to share the following views.

The Computing Technology Industry Association (CompTIA) is the voice of the world's $3 trillion information technology industry. CompTIA membership extends into more than 100 countries and includes companies at the forefront of innovation; including, the channel partners and solution providers they rely on to bring their products to market, and the professionals responsible for maximizing the benefits organizations receive from their technology investments. The promotion of policies that enhance growth and competition within the computing world is central to CompTIA's core functions. Further, CompTIA's mission is to facilitate the development of vendor-neutral standards in e-commerce, customer service, workforce development, and ICT (Information and Communications Technology) workforce certification.

CompTIA's members include thousands of small computer services businesses called Value Added Resellers ("VARs"), as well as nearly every major computer hardware manufacturer, software publisher and services provider. Our membership also includes thousands of individuals who are members of our "IT Pro" and our "TechVoice" groups. Further, we are proud to represent a wide array of entities including those that are highly innovative and entrepreneurial, develop software and hold patents. Likewise, we are proud to represent the American IT worker whom relies on this technology to enhance the lives and productivity of our nation. Based upon a recent CompTIA survey, we estimate that

one in twelve, or about 12 million American adults, consider themselves to be IT workers.[1] This is larger than the number of American adults classified by the Bureau of Labor Statistics ("BLS") as employed in farming, mining, and construction combined. This is also close to the number of adults classified by BLS as working in manufacturing or transportation. CompTIA has concluded that the IT workforce is now one of the largest and most important parts of the American political community.

My name is M.J. Shoer, the President and Virtual Chief Technology Officer of a VAR, the Jenaly Technology Group and am testifying on behalf of CompTIA. I live in Portsmouth, New Hampshire, and have been an information technology entrepreneur. In 1997, I founded Jenaly Technology Group and have since served as its President. Jenaly Technology Group provides IT services to small businesses throughout the region. In my current role, I am active in several IT groups and regularly write about information technology and small business issues.

FISMA and the Current Federal Security Ecosystem

On behalf of CompTIA and its many small business member companies, we welcome the Subcommittee's exploration of FISMA and its effectiveness for today's ever increasingly cybersecurity challenges. Certainly many critics and the other witnesses, including the Government Accountability Office (GAO), have commented on the effectiveness of FISMA. Recently, the GAO submitted twelve recommendations to the House of Representatives.[2] One finding, in particular, the eleventh, is significant for your attention. This finding calls for "increasing the cadre of cybersecurity professionals," and the report states the following:

> **Increasing the cadre of cybersecurity professionals** – The strategy includes efforts to increase the number and skills of cybersecurity professionals but, according to panelists, the results have not created sufficient numbers of professionals, including information security specialists and cybercrime investigators. Expert panel members stated that actions should include . . . *making the cybersecurity discipline a profession through testing and licensing.*[3]

It is unfortunate we have so many challenges today because the Congress came very close to requiring certification of federal IT security workers in 2002. FISMA itself only requires "security awareness training" to inform impacted personnel of information security risks associated with their activities, and to comply with agency procedures. The undisputed evidence reveals that this is insufficient for the federal government's needs.

It is evident to critics, or anyone who regularly reads the newspaper, that the current awareness training model is not working. Security breaches among the agencies have increased instead of falling

[1] http://www.comptia.org/issues/us.aspx.

[2] *National Cybersecurity Strategy, Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO Rep. No. 09-432 (Mar. 10, 2009).

[3] *Id.* at 12. (emphasis added).

off. This may be due to a disturbing phenomenon. Recent GAO analysis compiling agency FISMA reports, the total employees and contractors receiving security awareness training fell from 91 percent in FY 2006 to 84 percent in FY 2007. Nine agencies reported a decrease in awareness training. One Inspector General reported that the agency was unable to ensure contractors received awareness training. Eight Inspectors General disagreed with their agency's estimation of individuals receiving security awareness training.

A. **FISMA: Identification of Fundamental Flaws**

In my view, the fundamental flaw of the FISMA framework and the federal government's policy is a lack of emphasis on the training and testing that is vital. My recent meetings with various Hill staff confirms this, after my hearing episode after episode about breaches in the federal system caused by human error (*e.g.*, removing a laptop from a federal site and improperly securing it).

A second and significant flaw is the lack of uniform, verifiable IT security training as the single largest problem regarding information security in the federal government. According to CompTIA's 7TH ANNUAL TRENDS IN INFORMATION SECURITY SURVEY,[4] 59 percent of government respondents attributed their security breaches to human error. In addition, 25 percent of federal government employees reported not having a written security policy. From 2007-2008, the percentage of government agencies that required security training for IT staff fell from 70 percent to 60 percent.

Today, I would like to share some of my observations, as someone who has dedicated his career to information technology and security, regarding ways of enhancing FISMA for the challenges we face today and beyond. The basic themes of my recommendations are that the human element to data security requires greater attention; security awareness training is not a sufficient solution; and, the Pentagon's 8570 approach to IT security training should be adopted by the federal government to provide training and certification needs to keep federal IT cyber secure. Further, many critics believe that the threat posed by "human error" is under appreciated.

B. **FISMA Solutions: Expanding the 8570 Defense Department Initiative**

As the Subcommittee considers amending FISMA to enhance the security of federal systems, your attention is directed to a very successful Department of Defense (DoD) IT initiative. The DoD has raised the bar for cybersecurity through a training and testing program, commonly known as the 8570 Directive. This initiative focuses on the certification of personnel. Based upon my own experience in this industry, I believe that accreditations and certifications offer many benefits, including lower transaction costs. This year, my own IT business, Jenaly Technology Group, became the first in the country to be accredited for best practices in information security.

Remarkably, throughout the federal government, only the DoD has formally required its employees and contractors to get certified. In August 2004, the DoD issued Directive 8570.1. These groundbreaking guidelines recognized that awareness training and casual contacts with security

[4] See http://www.comptia.org/sections/research/reports/200903-EUTSummary.aspx

organizations were insufficient. In establishing this program, the DoD surveyed its IT workforce, assessed its requirements, and created three tiers of industry certifications based on whether the worker was a technical or managerial employee.

According to George Bieber, Deputy Director of Information Assurance (IA) Human Resources and Training at the Pentagon:

> *The ultimate vision of Directive 8570.1 is a sustained, professional IA workforce with the knowledge and skills to effectively secure our enterprise information systems. This effort will enable DoD to put the right people with the right skills in the right places, and it's a tremendous opportunity for personnel to get the training they need to keep current with security in a continuously changing technology environment.*

The Congress should properly recognize the successes of 8570.1, which provides transparent, uniform and verifiable *industry-led* IT security compliance program for the Pentagon and its suppliers. Accordingly, it is recommended that FISMA be amended to clarify that "security awareness training" must also involve the testing and certification that personnel are properly trained.

Regrettably, this latest data shows that the civilian agencies are far behind the rigorous approach taken by the military. It is recommended that to enhance the IT security throughout the federal government, all federal agencies must adopt and implement the DoD 8570 model to expand training and testing.

Another reason for industry-based federal IT standards is the uniformity provided. Currently, many states, including the Commonwealth of Massachusetts, are prescribing certain new regulatory framework to reduce data breaches. Any effective national, federal security standard should be uniform and effective; in contrast, the prospect of 50 different state cybersecurity regimes poses significant problems for the small business community, including raising questions about its effectiveness and cost. A national, federal, regime akin to DoD's 8570 would set a uniform benchmark for agencies to meet, reducing complexity and administrative waste. The federal government should set a standard that could lead the country.

Conclusion

In conclusion, it is undisputed that we must protect the American public by having a security framework that guards information systems for both our federal critical systems, as well as, the private sector. The computing industry is hard at work facing the unprecedented challenges of securing our data from both malicious threats and human error. Congress' enactment of FISMA has provided a base level of protection. The key to securing our systems for the future lies in the partnership between technology and human capital. By effectively managing both technology and people in concert, through training and testing (such as through the certification process), we can win the battles in the security war. The current Defense Department model surrounding the 8570 directive is a model worthy for emulation throughout the federal government. Any modification of FISMA must recognize the lessons surrounding the human

capital contribution to the IT security equation by the certification and accreditations to enhance our security.