

**Statement of Stuart McKee**  
**National Technology Officer, U.S. Public Sector**  
**Microsoft Corporation**

United States House of Representatives  
Committee on Oversight and Government Reform

“Policies Affecting High Tech Growth and Federal Adoption of Industry Best Practices”

San Jose, California

April 18, 2011

Thank you, Chairman Issa and distinguished members of the Committee. I appreciate the opportunity to testify today on behalf of Microsoft Corporation. My name is Stuart McKee, and I am the National Technology Officer for the US Public Sector at Microsoft, a position I have held since 2004. In this role, I work with governments of all sizes across the country and around the world on effective technology policy. Prior to joining Microsoft, I had the privilege to serve as the Chief Information Officer and an Executive Director for the State of Washington with responsibility for a \$150 million central IT operation, direct oversight authority for \$1 billion in technology spend, and overall accountability for statewide technology policy. I have also held technology leadership positions with large and small private sector organizations, including The Walt Disney Company and Starwave.

We thank the Committee for focusing on policies affecting high tech growth and federal adoption of industry best practices. At a time when our country is facing significant economic challenges, it is essential that government take advantage of the very best practices and innovations that the information technology community has to offer and that it pursue policies that support innovation and growth. In my testimony today, I will focus on four areas in which government and industry each has a role to play in driving progress toward policies that can promote IT innovation:

1. Information security and the new FedRAMP program;
2. An updated policy framework to facilitate a responsible move to cloud computing;
3. Efforts to drive growth through international trade and respect for intellectual property; and
4. The importance of the H-1B visa program.

#### Information Security and FedRAMP

Let me begin with a topic of utmost importance -- information security. As background, allow me share some of our experience. Microsoft is a world leader in information technology security. The company opened its first datacenter in September 1989, and today our globally-distributed, high-availability datacenters are managed by our Global Foundation Services (GFS) group. GFS's Online Services Security and Compliance team has built upon Microsoft's existing capabilities, including being one of the first major online service providers to achieve ISO/IEC 27001:2005 certification and SAS 70 Type II attestation, which also met Federal Information Security Management Act (FISMA) requirements.

Microsoft has also gone beyond the ISO standard, which includes approximately 150 security controls, and developed more than 300 security controls to account for and mitigate unique challenges and risks of cloud infrastructure<sup>1</sup>. The additional rigorous testing and continuous monitoring required by FISMA have been incorporated into Microsoft's overall information

---

<sup>1</sup> <http://blogs.technet.com/b/gfs/archive/2010/12/02/microsoft-s-cloud-infrastructure-receives-fisma-approval.aspx>

security program, which is described in several white papers located on Microsoft's Global Foundation Services web site<sup>2</sup>.

At Microsoft, **Trustworthy Computing**<sup>3</sup> is a core value. We have been recognized for the development of the Microsoft Security Development Lifecycle<sup>4</sup> (SDL) which we follow internally and share with governments and other companies. SDL is a security assurance process that is focused on software development. It is a collection of mandatory security activities, grouped by the phases of the traditional software development life cycle. Many of these security activities would provide some degree of security benefit if implemented on a stand-alone basis. However, practical experience at Microsoft has shown that security activities executed in established order and as part of a repeatable process can result in greater security gains than those resulting from ad-hoc implementation. Combining a holistic and practical approach, the SDL introduces security and privacy throughout all phases of the development process with the goal of protecting customers.

For government specifically, Microsoft has several programs and trusted partnerships in place, including:

- The **Government Security Program**<sup>5</sup> which provides national governments with information to help evaluate the security of Microsoft products. The Government Security Program is a collaborative partnership to design and build more secure computing infrastructures, and in many cases involves working with and providing governments with access to Microsoft source code. The National Institute of Standards and Technology (NIST) is a Government Security Program partner of Microsoft.
- The **Security Cooperation Program**<sup>6</sup> focuses on computer incident response, attack mitigation, and citizen outreach. The Multi-State ISAC<sup>7</sup> is a direct signatory whose membership includes every state in the country. In addition to coordination with state level entities, related state and local government entities benefit directly from this security information sharing program.
- The **US Government Configuration Baseline (USGCB)**<sup>8</sup> continues to be one of the most successful IT programs in the federal government to help increase security, reduce costs, and accelerate the adoption of new technologies, while creating a more managed desktop environment. The USGCB was initially developed as the Federal Desktop Core Configuration (FDCC) in conjunction with many agencies including the Office of Management and Budget (OMB), the Department of Homeland Security, the Department of

---

<sup>2</sup><http://www.globalfoundationservices.com/security/documents/InformationSecurityMangSysforMSCloudInfrastructure.pdf>

<sup>3</sup> <http://www.microsoft.com/about/twc/en/us/default.aspx>

<sup>4</sup> <http://www.microsoft.com/security/sdl/default.aspx>

<sup>5</sup> <http://www.microsoft.com/resources/sharedsource/gsp.msp>

<sup>6</sup> <http://www.microsoft.com/industry/publicsector/Government/programs/scpabout.msp>

<sup>7</sup> <http://www.msisc.org/>

<sup>8</sup> <http://usgcb.nist.gov/>

Defense and NIST. The security-focused standard is maintained by NIST and recommended by the Federal CIO Council.

To date, the federal government's focus on information security has been on enterprise systems located on-premises at the various federal agencies and data centers. However, much like the telegraph and telephone systems that grew across the country and around the world throughout the 20<sup>th</sup> century, our technology systems today are increasingly connected. Although it is often positioned as something new, "cloud computing" can be simply understood as a natural evolution and expansion of "network enabled" systems. While the federal government has already recognized the enormous opportunity for efficiency in standardization, consolidation, and centralization of core technology infrastructure (such as networks, data centers and purchase aggregation), there will also be opportunities to take advantage of shared infrastructure not located and/or operated directly by government entities. While cloud computing represents an evolution in technology, it is not a surprise that the standards and protocols established in the past are not a perfect match for a future in the cloud. They provide a base from which to work, but they must be adapted to recognize the new cloud computing environment.

The OMB, in concert with the General Services Administration (GSA), has embarked on a new effort known as the Federal Risk and Authorization Management Program or "FedRAMP." Microsoft appreciates the efforts underway, but we urge Congress to oversee this process to ensure that it meets the policy objectives established by Congress in the Federal Information Security Management Act of 2002.

In particular, FedRAMP must be consistent and fair with a process that is repeatable across platforms and immune from preferences for particular vendors or technology. While government and cloud service providers will benefit from a process that allows multiple federal agencies to rely on reviewed and accepted information security procedures, it is essential that the process itself must be transparent, consistent and fair to all.

FedRAMP has a great deal of potential to streamline, strengthen, and secure cloud implementations across the federal government. However, while FedRAMP offers these potential benefits, Microsoft has identified a few challenges posed by the program as proposed that warrant deeper discussion. For example, the single review process, new controls and control enhancements, and continuous monitoring are areas which, if not addressed, may delay implementation, limit adoption, and reduce effectiveness. We look forward to working with OMB, GSA, federal agencies and other stakeholders as related issues are addressed.

### Cloud Computing

Beyond issues related to information security and government, Congress has a role to play in facilitating a responsible move to the cloud for all customers, including commercial enterprises and consumers. Cloud computing promises to promote new efficiencies and foster innovation, but there are significant questions related to privacy and security that need to be addressed before

the potential of cloud computing can be fully realized. Microsoft is committed to doing its part to achieve these goals, but new government action is also needed to allow the cloud to deliver on its promise.

***Security.*** Although the cloud is being built with powerful and unprecedented security safeguards, the aggregation of data in cloud datacenters presents new and rich targets for hackers and thieves. All stakeholders must work together to protect the security of the cloud. At the same time, Congress should ensure that the penalties for launching an attack on cloud computing infrastructure are sufficiently severe to help deter would-be criminals.

***Transparency.*** It should not be enough for cloud service providers simply to claim that their services are private and secure. Customers should be provided with information about why this is the case so that cloud computing users can make informed decisions about the services that best fit their needs.

***National Sovereignty.*** Recent years have seen the emergence of a global thicket of competing and sometimes conflicting laws impacting cloud computing. These laws can place cloud service providers in a Catch-22, where the decision to comply with the lawful demand for data in one jurisdiction can risk violating the data privacy laws of another jurisdiction. This situation needs to be remedied.

Microsoft believes that these issues are interrelated and thus are best addressed in concert. That is why we have advocated for consideration of legislation that would:

- require transparency around cloud service providers' security and privacy practices, including by requiring that cloud service providers maintain a comprehensive written information security program with safeguards appropriate to the use of their services, provide a summary of that program to potential customers, and disclose their privacy practices to any customer from whom covered personal information is collected;
- ensure rigor in the federal government's procurement of cloud services by requiring federal agencies to evaluate and select providers based in part on an assessment of their information security programs;
- enhance criminal enforcement of computer crimes targeting cloud computing data centers, and allow cloud service providers to bring suit against violators directly to augment deterrence of such crimes; and
- encourage the federal government to engage in international efforts to promote consistency in national laws governing privacy, security and government access to cloud data.

With the benefit of a modernized regulatory framework, industry will have the solid grounding to deliver on the promise of cloud computing for both individuals and organizations.

## International Trade

With 95 percent of the world's consumers living outside the US borders, international trade is becoming an increasingly important element of a US pro-growth economic and trade strategy. And for the United States, information communications technology — “ICT” — will help to drive recovery by creating more than a million jobs in the next four years. In Washington State, one in every three jobs depends on trade. Microsoft is the largest employer headquartered in the state, and a recent study has found that one Microsoft job accounts for five additional jobs elsewhere in the state economy, accounting for a total of 270,000 jobs in the state of Washington — more than 8 percent of the workforce.

In his 2010 State of the Union Address, President Obama recognized the importance of trade when he announced his goal of doubling exports of goods and services in five years – from \$1.5 trillion in 2009 to \$3 trillion in 2014. Expanding opportunity, adjusting to competition, and leading on innovation as a means to promote the creation of better jobs and economic growth are all part of a robust trade agenda. Global competition in information technology is fierce. The IT industry depends on the rule of law, due process, intellectual property rights protection, transparency, and non-discriminatory policies — at home and abroad.

Microsoft advocates using existing trade agreements —including the World Trade Organization (WTO) and Free Trade Agreements (FTAs) -- to enforce intellectual property rights, expand trade, and ensure that the US IT industry remains competitive. Looking to the future, Microsoft and other American IT companies must seek new markets, expand opportunities, and ensure fair market access to compete. To accomplish these essential goals, we recommend the following:

***Swift passage of pending FTAs.*** The swift passage of the pending US-Korea, US-Colombia, and US-Panama FTAs must be part of the strategy to double exports of goods and services. Microsoft strongly supports passage of these agreements. Without them, America will continue to lose out to trading partners who are already benefiting from their own free trade deals.

The US-Korea FTA, the most economically significant of the agreements, contains world-class provisions that set the standard for future US trade agreements. In addition to strong IP provisions, the Korea FTA, like other FTAs negotiated by America, makes important strides in government procurement. Beyond requiring that there be no mandates that favor one technology over another, the FTAs require countries to ensure that their government agencies only purchase and use legitimate software, a provision that originated in the United States and now is embraced by key trading partners.

***Negotiating important new agreements.*** In addition, we must look to the negotiation of new market opening agreements, such as the Trans-Pacific Partnership (TPP). With partners in the Asia-Pacific region (Australia, Brunei, Chile, Malaysia, New Zealand, Peru, Singapore, Vietnam) and others such as Japan and Canada in the wings, the United

States has embarked on the creation of a 21<sup>st</sup> century trade agreement that includes rules and disciplines to address emerging trade and services issues. A strong TPP agreement, with state-of-the-art intellectual property rules that build on the US-Korea FTA, is essential. Similarly, strong rules in the areas of competition policy and regulatory due process, particularly with state-owned enterprises (SOEs), must be part of any agreement going forward. Trade agreements already deal with many Internet-related issues, such as the provision of cloud services like email, but further work is needed on emerging services issues to ensure that IT can be an enabler for economic progress.

***Maintaining a focus on stemming IP theft.*** A top priority for Microsoft is to counter the problem of IP theft around the world, including emerging markets such as China where the piracy rate for the business software industry stands at approximately 80 percent and is even often higher for popular Microsoft products. The US government is engaged in a series of exchanges with China, including the Joint Commission on Commerce and Trade, the Strategic and Economic Dialogue and most recently, the visit of President Hu to the United States. Although we are pleased with the commitment and hard work China is demonstrating in addressing piracy, we need to continue to strive for more progress and tangible results.

Software piracy in China (or any location) translates into fewer jobs and less economic growth both in the United States and in local economies. For example, the piracy in China of Microsoft products alone costs the US economy up to 60,000 jobs, when the multiplier effect is taken into account. China and the United States have a common interest in promoting strong intellectual property rights protection because technology holds the key to solving so many pressing global issues.

China's continued strong economic growth throughout the most recent economic crisis, means that its market has changed dramatically. And China's new consumers are both "connected" and tech-savvy. In 2010, China surpassed 420 million Internet users, broadband reached 363 million, and mobile Internet users totaled 277 million. Perhaps more significantly, China's middle class is now roughly equal in size to the entire population of the US.

China will soon be the largest PC market in the world. Microsoft's products are tremendously popular with Chinese users, with more than 95 percent of Chinese PCs today running Microsoft Windows and well over 80 percent of enterprise PCs running Microsoft Office. However, rampant software piracy remains a major problem. Microsoft's revenue per PC in China is far below other large emerging markets, such as India, Russia, and even Vietnam. To make progress, we need a comprehensive strategy that sets objective, measurable benchmarks and a timeline for securing results. One such benchmark would be seeing an increase in software sales and the emergence of an ecosystem that rejects trade in pirated software.

As a company, Microsoft faces a significant challenge in the rampant piracy we face in China and emerging markets. Even with these challenges, we believe the only option is to continue to advocate for the opening of new markets and strengthening the rules and disciplines of trade – particularly with regard to intellectual property rights protection.

### H-1B Visa Program

Finally, I would like to turn to the ongoing debate concerning the H-1B visa program that is critical to our success. As the Microsoft experience has proven, job supply in the United States is not a zero sum game. The fact that Microsoft and its IT partners and competitors seek to hire foreign nationals does not result in job losses for American workers. Quite the contrary is true. Throughout the history of the United States, we have generated jobs through creativity and invention that is dependent on attracting the best and the brightest. Our country has operated on the principle that the more brain power we can attract from around the world, the more creativity, invention, and growth we can achieve here at home.

There seems to be a reemerging consensus that we need to stick to this principle, and we welcome it. President Obama, in his State of the Union address, noted that to build America's future, we have “to out-innovate, out-educate, and out-build the rest of the world. We have to make America the best place on Earth to do business.” We could not agree more. The President went on to emphasize that we cannot continue our current path of welcoming students from abroad to come study at our colleges and universities, but sending them back to their native countries to compete against us once they complete their degrees.

Similarly, in a speech on strategies for economic growth at Stanford University, Majority Leader Cantor sounded the same theme: “As a country we have always invited the best and brightest from around the world – many of whom are educated in our universities – to contribute to our economic growth. Yet our visa system has failed to keep pace with the demands of our economy. If bringing in high-skilled workers from abroad helps us keep thousands of jobs here in America, our antiquated laws should not be a barrier.”

These statements recognize that the H-1B program is an indispensable part of America's technology innovation. Without a robust, fully functioning H-1B program, our ability to out-innovate the rest of the world, to keep jobs here, and to grow new jobs in this country will collapse. The H-1B is often the only way to get highly skilled foreign professionals on the job quickly when the economy needs them. The H-1B is often the only way to bring in a person with pinpointed skills to perform a crucial temporary assignment. And it is overwhelmingly the only way to bring bright foreign talent across the bridge to permanent residence and a permanent role as a contributor to the US economy.

There are many suggestions for improvement of the H-1B program which deserve full consideration by Congress. We strongly support efforts that will facilitate the ability of



information technology companies like Microsoft to attract, hire, and retain the best and the brightest innovators. If we are not allowed to do so, our international competitors will.

### Conclusion

We look forward to working with you, Chairman Issa, members of your Committee, and other Members of Congress as we move forward to:

- shape a FedRAMP program that is effective, efficient, and fair;
- establish a modern policy framework that promotes a responsible move to the cloud;
- advance a 21<sup>st</sup> century trade policy that allows the IT sector to compete and gain fair access to markets around the world;
- facilitate the ability of information technology companies to attract, hire, and retain the best and the brightest innovators.

At Microsoft, we are proud of the role we play in leading technology innovation and adoption by enterprise business systems. The federal government is a valued customer, and by adopting policies commercial practices it can take advantage of the proven strengths and efficiencies present in the marketplace. Effective use of information technology will help achieve the ultimate goal – maximizing the use of scarce resources for the benefit of all Americans.

Again, thank you for the opportunity to testify today.