April 29, 2013

U.S. Department of Commerce
Docket Number 130206115–3115–01
Incentives to Adopt Improved Cybersecurity Practices

Comments of VOXEM, Inc.

VOXEM thanks the Department of Commerce for the opportunity to respond to the Notice of Inquiry on Incentives to Adopt Improved Cybersecurity Practices. In support of the Department of Commerce's effort to evaluate cyber incentives, an incentive idea is presented along with responses to specific questions asked in the Notice of Inquiry.

Creating a compelling incentive to spur action on cyber security is challenging. To be highly effective, the incentive must create a sustained collective action for cyber assurance [†] that is compatible with and integrated into private sector business models. This effort must be undertaken with the understanding and support of all stakeholders, and must be measurable and integrated into existing processes to ensure accountability. Even more importantly, any incentive must be economically sustainable for both the organization undertaking the investment and the Federal Government. Optimally, an effective cyber incentive should promote innovation and increase our economic prosperity while improving our long term productivity.

With an understanding of the significance of cyber security to our national security and economic prosperity and within the limitations of our current fiscal environment, the Capital Gains Tax Incentive for Cyber Assurance is presented. The Capital Gains Tax Incentive for Cyber Assurance reinvents the capital gains tax to reward shareholders with a lower capital gains tax rate on the sale of assets (stocks and bonds) of corporations that voluntarily adopt the NIST Cybersecurity Framework.

The idea is to offer shareholders a differential capital gains tax rate – a lower capital gains tax rate on transactions involving corporations that adopt the NIST Cybersecurity Framework and a higher capital gains tax rate on transactions involving corporations that elect not to participate in the Program. Corporations that elect to participate in this voluntary Program would certify their adoption of the NIST Cybersecurity Framework to the Securities and Exchange Commission (SEC), without disclosing confidential or private information to the Federal Government.

[†] Cyber assurance is the level of confidence that the technology that we depend on (hardware, software and network infrastructure) functions as intended without vulnerabilities that impact reliability and security.

It is important to note that there is a precedent for the use of the capital gains tax rate as an incentive. The tax code differentiates between short and long-term investments and rewards shareholders who make longer-term investments with a lower capital gains tax rate.

A concise summary of the Capital Gains Tax Incentive for Cyber Assurance is included in the Appendix. Economic analysis is needed to determine the optimal capital gains tax rates to maximize voluntary participation within our fiscal constraints.

In response to the July 2010 Notice of Inquiry for Cyber Incentives, several of the respondents suggested tax credits to encourage action on cyber security. There are numerous limitations to using tax credits for cyber security. Tax credits shift the costs of cyber security to the taxpayer and then depend on the corporation to assess risk and take action as a result of these cost savings. Other factors beyond costs may influence an organization's decision to assume rather than mitigate risks. For example, there may be an unwillingness to divert resources away from other corporate goals, an unwillingness to disrupt operations to prevent potential adverse events or an unwillingness to incur delays in the introduction of new products or services. Time to market considerations often out-weigh costs in determining private sector actions. In fact, corporations that undertake an investment in cyber assurance may be placed at a competitive disadvantage if other corporations fail to make similar investments.

There is a need to create a level playing field through a collective action in support of the NIST Cybersecurity Framework. Instead of shifting the costs of cyber security to the taxpayer, the Capital Gains Tax Incentive creates *a culture of cyber assurance* by making support for the NIST Cybersecurity Framework a *top corporate priority in response to shareholder demand*. The value of creating a culture for risk management has been previously identified by NIST. From NIST Special Publication 800-39 - *Managing Information Security Risk*,

> *"The organization's culture informs and even, to perhaps a large degree, defines that organization's risk management strategy. At a minimum, when an expressed risk management strategy is not consistent with that organization's culture, then it is likely that the strategy will be difficult if not impossible to implement. Recognizing and addressing the significant influence culture has on risk-related decisions of senior leaders/executives within organizations can therefore, be key to achieving effective management of risk."*

It is anticipated that shareholder demand will drive significant and sufficient private sector participation in the Program. The resulting collective action in cyber assurance will be beneficial to society's overall interests.

In addition, tax credits may not be feasible in our current fiscal environment, and represent a long term, on-going cost of uncertain size to the Federal Government. Depending on how the tax credit is structured, the amount of investment in cyber assurance will determine the size of the tax credit. Limiting the amount of the tax credit to cap costs will minimize the impact on the federal budget but may also reduce the effectiveness or level of participation. In addition, tax credits may also distort economic activity by encouraging organizations to either accelerate or defer investments in cyber assurance to optimize tax credit reimbursements for a specific tax year.

The Capital Gains Tax Incentive is fiscally sustainable; the tax benefit is received as a result of transactions involving the assets of corporations that adopt the NIST Cybersecurity Framework rather than for incremental activity. The Capital Gains Tax Incentive for Cyber Assurance effectively integrates cyber security into an organization's business model. Linking the capital gains tax rate to the NIST Cybersecurity Framework will address a significant national concern within private sector business models and motivations.

Key Benefits

The Capital Gains Tax Incentive for Cyber Assurance will:

- Promote significant and sustained voluntary support for the NIST Cybersecurity Framework across the entire private sector – not just critical infrastructure,
- Integrate support for the NIST Cybersecurity Framework into private sector business models to ensure that cyber security is an essential part of maximizing overall profitability and return to shareholders – rather than a burden,
- Align the interests of shareholders with addressing a national security concern,
- Work within the constraints of our fiscal environment,
- Significantly increase visibility into the level of private sector cyber preparedness through SEC reporting while ensuring protection of confidential or sensitive information,
- Facilitate cyber security insurance underwriting by confirming compliance with the NIST Cybersecurity Framework, and
- Foster innovation and economic growth by encouraging increased private sector investment in cyber security and in new products and services.

The remaining comments are in response to specific questions from the Department of Commerce Notice of Inquiry regarding incentives.

Regarding the adequacy of existing incentives to address the current risk environment for your sector or company

A more comprehensive view of risk is needed when evaluating incentives to include overall risks to all stakeholders beyond a specific company or sector. While corporations have an incentive to protect their assets, intellectual property and reputation, focusing on the risk for a specific company or sector fails to recognize the unique characteristics of our interconnected world. A given company's willingness to assume risk may not be in the interests of all stakeholders as the costs of adverse cyber events are frequently externalized.

For example, a company creates a software patch to mitigate a security issue in their product. To be effective, their customers must, in turn, apply the patch. Companies that fail to apply the patch and then suffer a breach will experience a direct cost. In addition, this failure to act may create substantial indirect costs for others. These indirect costs may include the use of

compromised systems to launch attacks, the loss of personal identifying information and privacy and reputational risks to others.

An incentive's effectiveness should be evaluated on its impact to our overall society. Therefore, broader participation beyond critical infrastructure is desirable.

Regarding incentives and small firms

The role of small companies in driving innovation is critical and an effective incentive must create market conditions where there is broad and sustained demand for products and services that help our nation achieve its cyber assurance goals. To achieve this, steps must be taken to ensure that the NIST Cybersecurity Framework enables flexible implementation options and that the measurement of voluntary compliance supports the concept of grades or higher levels of assurance. In this way, cyber assurance becomes an opportunity for product and service differentiation instead of a burden.

Regarding changing threats and new business models

The Capital Gains Tax Incentive will drive voluntary adoption and integration of the NIST Cybersecurity Framework into both existing and new business models. By creating a corporate culture for cyber assurance, organizations will be better able to respond to new threats having the full support of senior-level management and shareholders.

VOXEM thanks the Department of Commerce for the opportunity to comment and urges the Department to include the Capital Gains Tax Incentive for Cyber Assurance in the set of incentives under evaluation. Please direct any questions to: joann@voxem.com.

Sincerely,

Jo-Ann Polise
President of VOXEM

Co-chair
DHS Software Assurance Business Case Working Group
(*The views expressed are those of the author and do not necessarily reflect the opinion of the Department of Homeland Security or the members of the Software Assurance Business Case Working Group*).

Capital Gains Tax Incentive for Cyber Assurance

A GAME CHANGING APPROACH TO ASSURE THE TECHNOLOGY THAT WE DEPEND ON AND PROMOTE SUSTAINABLE ECONOMIC GROWTH

Although cyber events may significantly impact an organization, there is limited understanding and support to increase expenditures on cyber security. As a society we are caught in a seemingly intractable situation – while there is unwillingness to support regulation, market forces alone are insufficient to drive investment in a socially optimum level of cyber assurance.

While flaws in both the design and implementation of software and hardware place our information assets, critical infrastructure and privacy at risk, investment in cyber assurance is limited by perceived risks to the corporation which may not reflect the actual threat level and ignores the greater impact to society.

Spending on cyber assurance increases costs, may result in product delays and is often viewed as providing insufficient return on investment. Furthering the problem, organizations that do take steps to improve their cyber assurance may be placed at a disadvantage. There is no certainty that their actions will prevent a cyber-attack; and despite their efforts, they may be negatively impacted by the lack of cyber assurance in others. As a lack of cyber assurance erodes our trust in technology, diminishes our economic productivity and represents a national security risk, a new approach is needed to inspire a Y2K-level of response to achieve technology assurance.

Reinventing the Capital Gains Tax

The idea is to reward shareholders with a lower capital gains tax rate on the sale of assets (stocks and bonds) of corporations that undertake an assurance effort. As a voluntary incentive, corporations would elect to participate by undertaking assurance activities in support of raising their level of confidence in the technology they depend on rather than for achieving a specific level of cyber security. Since current limitations in technology may impact the ability to secure our resources, cyber assurance should be viewed as a societal commitment to innovation and on-going technology improvement.

Creating “Patient Capital”

This game-changing tax incentive will motivate both individual and corporate shareholders to support cyber assurance and creates patient capital to endure increased costs and potential product delays. By integrating cyber assurance into an organization’s overall strategy with shareholder support, corporations will sustain investment in cyber assurance while maximizing overall return on investment to shareholders. For corporations that fail to meet their assurance objectives or elect not to participate, investor’s capital gains would be subject to a higher capital gains tax rate. It is anticipated that shareholder pressure will motivate significant support for this effort.

A Powerful Incentive

By empowering shareholders to make cyber assurance a top priority, the private sector will be motivated to embrace cyber assurance and act in the national interest while at the same time delivering value to their shareholders. With input from an advisory group of government, non-government organizations and other industry experts, corporations would determine the level of cyber assurance required by their business model, contractual commitments, the current threat environment and any *existing* regulatory requirements. Guidelines such as the *Critical Controls for Effective Cyber Defense* could serve as a reference framework. Instead of mandates or prescriptive solutions, this incentive would give the private sector maximum flexibility to respond to emerging threats and changing technologies.

Visibility without Disclosure of Confidential or Private Information

To qualify their shareholders for the lower capital gains tax rate, corporations would certify to the Securities and Exchange Commission (SEC) that actions were taken in support of cyber assurance activities with penalties for misrepresentation. This will provide greater visibility into the private sector's level of cyber preparedness without requiring the disclosure of confidential or private information to the Federal Government. In addition, this enhanced visibility would encourage and facilitate cyber insurance underwriting.

Improved Risk Management and Corporate Governance

Participation in the cyber assurance effort will improve risk management and aid corporate governance. By integrating cyber assurance into their overall strategy, management will be better able to identify and prioritize risks based on their potential impact, put mitigation plans in place and more effectively monitor the effectiveness of the technology in their organizations.

In addition, corporations will be better able to restore confidence in the event of a security breach. By communicating their level of preparedness and contingency planning, corporations may minimize any adverse impacts to their stock price, credit rating, and customer confidence.

Jobs and Economic Growth

By linking the capital gains tax rate with cyber assurance, we promote both our national security and economic prosperity. During these uncertain economic times, corporations are conserving cash and reducing capital investment in technology which is contributing to our economic slowdown and increasing unemployment. In turn, technology companies are hesitant to undertake a significant R&D effort uncertain of the demand for new, assured products and services. In this environment, undertaking fiscal austerity without taking steps to increase private sector capital investment will only further slow the economy and increase the national debt.

By facilitating a coordinated economic action on the same scale as the Y2K effort, the Capital Gains Tax Incentive for Cyber Assurance will spur investment in technology infrastructure, drive innovation and promote sustainable economic growth while strengthening cyber security.