Tiger's Lair, Inc.
8619 Westwood Center Drive
Vienna, VA 22182

To: Internet Policy Task Force
Department of Commerce
From: Tiger's Lair, Inc
Re: Docket No.: 100721305–0305–01
Docket No. 100721305-0436-02
Date: September 20, 2010

Dear Sirs;

In response to the Department of Commerce's Internet Policy Task Force's Notice of Inquiry for Cybersecurity, Innovation, and the Internet Economy (Docket No.: 100721305–0305–01; extension Docket No. 100721305-0436-02), we are submitting the following opinions for questions 3, 7, and 8.

Question 3: ***Website and Component Security***

Should the government alone, the private sector, or the government and private sector collaboratively explore whether third-party verification of Website and component security is or can prove effective in reducing the proliferation of malware? If so, what measures should be considered? What would be the implementation challenges in deploying such measures?

It is our opinion that the government and private sector should collaborate in order to most effectively and expeditiously reduce the proliferation of malware. We recommend a proactive, system level approach, rather than a reactive or "after the fact" verification approach of web or component security. The latest attacks are originating at the microchip level. Today's security must be rooted in the hardware as well as the software. Additionally, the security should be designed into the system, not screened, or 'verified' after the manufacturing process. This is a proactive and comprehensive approach that addresses the next generation malware attacks as well as anti-tamper and anti-counterfeit exposure which also enables malware attacks.

Challenges of implementing the next generation security measures include the reality that the general public will not realize the benefit of purchasing such security until they have experienced

the harm of not having such protection. The reality is that it will likely take grand scale personal financial loss, identity theft or even a national security incident for the average consumer to understand the current cyber-security risks at hand. A large scale upgrade of the current internet and cyber-security offerings will take at least 3-5 years to complete. Since consumers will not see the benefit of such a program until they have been impacted; and businesses will absorb risk levels until the cost is high enough to cause each individual business' cost/risk threshold to an 'investment' decision, the government should be the lead driver and collaborate with industry to define the requirements. The government should mandate industry to enable the next generation of system level hardware/software cyber-security, and then incentivize consumers to adopt these solutions before widespread consumer or critical infrastructure attacks begin.

The best way to get this protection on the market as quickly as possible is through public and private collaboration. From a public perspective, new policies need to be implemented to force those compute devices with critical security implications to be protected at the hardware and software level. Traditional devices such as PCs, laptops, and servers that operate within government, utility, financial services, and healthcare verticals absolutely must be protected in order to guard the core operations. Outside of existing critical infrastructure, the collaboration should also drive non-traditional devices such as smart grid components, smart phones, and medical devices to upgrade their security to better protect the average consumer. Today's 'new' devices pose an immediate security threat as they are loaded with features, exist outside traditional data centers, are more at risk of physical tampering, and the motivation for all types of malware attacks increases daily.

The most prudent course of action is to address all attack types in the machines themselves. This requires a necessary coordination of both hardware and software defense mechanisms in order to prevent web-based as well as component-based attacks. With the software providing the intelligence and decision-making, and the hardware enforcing policies at the lowest levels and ensuring the authenticity of all components within the device, this combination security strategy is absolutely required to fight current and future malware attacks.

The internet security policy needs to specify the features of a secure computing device, including anti-tampering, anti-counterfeiting, and anti-malware features rooted in the hardware itself. These features would deliver anti-malware far above the current "blacklist" signature model, and prevent new and unknown attacks before they are identified in the lab (when it is often too late). They would also protect against the chip and device embedded malware that is starting to appear in the market.

Anti-counterfeiting is one of the cornerstones of the policy. Validating that the chips are authentic, and that they are exactly as designed without additional rogue code and back doors baked into them is the most critical element of the policy. This will stop the chip-embedded attacks that are occurring across multiple industries completely unbeknownst to current anti-virus solutions.

Anti-tampering is required functionality for field-deployed units, such as smart meters and smart phones. Hackers that have physical access to a device can easily get behind the software and get

access to core systems without anti-tamper hardware provisions. Anti-tamper functionality needs to include tamper awareness, and countermeasures to stop a compromised device from allowing access to the core operating systems and data. These must be hardware rooted in order to be effective.

Anti-malware is a combination of hardware and software working together to identify attacks and stop them proactively. While traditional signature-based anti-virus has its place and is 99% effective in stopping most basic attacks, the next generation of anti-virus solutions need to be smarter and look for aberrant behaviors within the device. With the hardware-based monitors providing feedback to smarter software, and hardware-rooted countermeasures designed to stop attacks instantly as soon as they are discovered (automatically, through the software engine, and/or via manual intervention), a more robust next-generation anti-malware solution can be deployed.

Once a firm policy is established, the business sector will then be able to fill the requirements and deliver secure devices to market. Innovation will be encouraged as those that are able to deliver devices that conform to the policies will have first mover advantages in a very large market. R&D dollars will be spent to address these concerns, and in a very short period of time there would be viable solutions in the market from numerous vendors. This would allow the entire computing industry to take a quantum leap forward in security, and move the defenses ahead of where our adversaries currently are today.

Challenges of implementing an effective anti-malware policy include consumers, industry, time, and a clear driver. Will consumers need to 'feel the pain' before they protect themselves and adopt new solutions? Industry needs either a monetary incentive or a mandate. The security of a system is only as good as its weakest link. Currently, a typical IT refresh cycle is 3-5 years for new technology.

Today, the strength of our free-market society is our weakness in cybersecurity. In order to unify consumers, business, and critical industry suppliers, we need the government to lead the effort with mandates, technology collaboration, and incentives. This would be the most effective and efficient method to implement system level cyber-security and internet policies which will protect consumers, businesses, critical infrastructure and military systems, and a best effort to prevent catastrophic events.

Question 7: ***Research and Development***

How can the federal government best promote additional commercial and academic research and development in cybersecurity technology?

The Small Business Innovation Research program (or another similar program) must rapidly be modified and expanded to incorporate the following objectives:

a) to foster collaboration between small business and academia
b) to encourage small businesses and academia to propose new topics publicly
c) to provide modest and *more frequent* funding opportunities (e.g. twelve times a year)
d) to establish formalized processes and incentives to expose research and development programs to the private investment community to accelerate commercialization efforts requiring sizable capital investments.

The federal government must also hasten the pace of discovery through the improved efficiency of these programs. At present, the current SBIR and BAA process is unnecessarily slow, with significant backlogs in solicitations and contract awards that have immediate national-security implications. Such inefficiencies are alarming, considering the resources being brought to bear by individuals, organizations, and states with nefarious intent. The threats posed against our computerized military infrastructure, utilities, governance and financial institutions are well documented, yet the attack space, for all practical purposes, remains unguarded. With the rapid development toward mobile computing combined with the advent of computer-based services in the healthcare and financial industries (to name but a few), there is increasing risk for wide-scale and undetected cyber-crime. As such, the research and development initiatives must be reinforced with educational programs that generally raise awareness, proactively inform the public of the practical risks posed by a computerized society and the reasons behind the research and development efforts.

What particular research and development areas do not receive sufficient attention in the private sector? What cybersecurity disciplines most need research and development resources (e.g., performance metrics, availability, status monitoring, usability, and cost effectiveness)?

There are three related concepts that need to become the focus of both technical and economic research: system resiliency, self-healing, and the need for heterogeneous computers. As with the human body, we must design computer systems that continue to function even after infection. While such concepts are not new, few theoretical models and no practical models exist. Likewise, the concepts of self-healing must be researched and adapted to computer systems to take the human-computer interactive element out of the computer repair process (except in the direst situations). Finally, we must consider the use of heterogeneous computers to moderate the rate of infection and provide micro and macro defenses against all forms of “injury”. There are significant economic barriers that must be researched and addressed. Perhaps outside the scope of this specific topic - we must also research the integration of electronic and biological computers and sensors.

How effective would a federal government-sponsored ‘‘grand challenge program’’ be at drawing attention to and promoting work on specific technical problems?

A federally sponsored and highly visible program will be effective at raising the awareness of the problem, but will not in and of itself enable the rapid pace of discovery required to regain control of the current cyber-security situation.

The federal government should also consider creating a “hybrid open-source micro-funding” program, where awards of $1k-25k are used to facilitate the rapid construction of intellectual property and open-source solutions to complement existing long-term research and development efforts. Unlike traditional R&D funding models that rely on a small number of reviewers, this program should leverage web/internet-based resources to construct a social review, award and rating system. In addition, the program should be initiated with the construction of a secure repository system and social networking interface that ensures origin attribution, usage tracking, object and user ratings, and efficient monetary transfer. This system can evolve to a marketplace with many of the benefits of open source practices but with immediate incentives to encourage participation from large segments of the scientific and engineering community. Done properly, such a program will produce a research and development model that is optimally suited to leverage the “next generation” of scientists and engineers who more frequently contribute to society as individuals or within small organizations.

Question 8: ***An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices***

The incentives to address cybersecurity are inadequate at present for commercial, and consumer assets, and more importantly, national security and critical infrastructure assets. Commercial assets are protected based on a cost-to-risk balance, as the current market dictates. Today, a company is able to spend less and not guard against every possible kind of threats. They accept the consequences of data breaches, including losses of customer data and the associated fines and business harm. Typically, the consumer trusts the commercial entities to protect them, and bear the pains in a very individual way when affected by such breaches. Both commercial entities and consumers trust the government to drive and deliver security, including all aspects of cyber-security. Given the attacks on the Pentagon, as well as Google, and the TJ Maxx data breach, we know that the incentive to protect commercial and consumer assets as well as national security and critical infrastructure assets, is, to be polite, inadequate. The question is: what to do and where to start?

Given that national security is the most important area of concern; and that technology developed for this purpose then migrates to commercial and consumer applications, we first look at security gaps related to national security and critical infrastructure. The most stringent technology security guidelines are required when deciding how to protect assets essential Federal, State, or Local government asset.

"Good enough" simply isn't good enough today. As the adversaries of this nation are staging well-funded and coordinated attacks against our nation with an effort to destroy our way of life, any asset deemed of national security or critical infrastructure absolutely has to be hardened to the full extent possible, against all known attack vectors.

One example of today's technology security inadequacies is the occurrence of chip-embedded malware. As 98% of the chips used in purposes deemed "national security" assets are made overseas, and as there have been numerous documented cases where malware has been found embedded in the chips, it is clear that there are assets of national importance that are compromised before they are introduced into a system; and, the security software will never find them. Yet there is no policy to close this gap.

The US Government absolutely needs to define the policies as they pertain to national security compute assets and mandate certain standards of protection. These standards need to include monitoring the hardware as well as having adequate software protection to provide a unified defense against malware and trojans, whether they are attacking from web-based sources, tampering, or hardware embedded.

The US Government should work collaboratively with the private sector to define the following:

- What is a "national security" asset?
- What are all of the potential threats to these assets?
- What sorts of hardware and software solutions are required to protect these devices?

- How can we make the security technologies flexible enough to protect against future unknown attacks, and not just the known ones?

The US Government needs to be proactive in defining these policies and in defining sufficient penalties to force the adoption of the specified security practices to be mandatory, not a “business decision”. Incentives including funding should continue to be made available by the government in critical national security areas to encourage partnerships and the development of new products, but needs to trickle down at a pace that allows technology developments to get ahead of the adversaries, just barely keeping pace with them. Also, the US Government should define a rigorous test bench and test criteria to certify new security solutions are in adherence to the new policies. Through government mandates, continued incentives programs, and certification of compliance we can ensure we are doing all that can be done to secure our national assets and protect our businesses and citizens.

About Tiger's Lair

Tiger's Lair, Inc. is a cyber security company based in Vienna, VA and Ashland MA. Our expertise lies in system level cyber security which is designed in at the hardware level. Tiger's Lair is currently engaged with several branches of the US Intelligence community as well as large defense and critical infrastructure contractors as well as several large OEM's on consumer products.

Paul Bradley, CTO; Shawn Mastrian, VP/Sales, Bill Bonde, SVP, Business Development, and Trish Jennings, VP/Marketing and Product Research contributed to the opinions set forth. Please contact Trish Jennings at trish.jennings@tigers-lair, or at 617-851-9677 for any inquiries.

Thank you again for the opportunity to contribute, and best wishes.

Sincerely,

Trish Jennings