**Tom Kellermann**
**Vice President of Security Awareness, Core Security Technologies**
**CSIS Cyber Security Commission Member**
**Certified Information Security Manager (CISM)**

**Before the**
**United States Senate**
**Homeland Security and Government Affairs Committee**
**April 28, 2009**

## Introduction

Chairman Lieberman**,** Ranking Member Collins and Members of the Committee, I profoundly appreciate the opportunity to address you today on these matters of cyber-security before us which are so critically important to protecting the well-being of our nation's citizens, physical infrastructure, intellectual property and economy.

Over my years of work as an information technology (IT) security practitioner for organizations including the World Bank, as an advocate for policy efforts including the Center for Strategic and International Studies Commission on Cyber Security for the 44th Presidency, and as a representative of Core Security Technologies, I've had the unique opportunity to gain detailed insight into the incredible challenges facing organizations of all kinds today, including federal agencies, in relation to the multifarious risks posed by hackers, virus-writers, state actors and a litany of other malicious operators involved in executing cybercrimes.

It is without any shade of doubt that I sit here before you determined to convince you further that the problems facing our nation today as it relates to stemming the ability of individuals, organized criminals, terrorists and foreign nations themselves to infiltrate our electronic infrastructure – for the purpose of assailing everything from our most

strategic national information resources to our critical physical grid systems – cannot be understated.

Looking back at the horrible events of Sept. 11, 2001, it should be recognized that while those attacks did not leverage a heavy dose of computing assets, one important lesson that we should take from the tragedy is that terrorist groups and other state enemies can and will leverage the technologies that we as a society depend upon most to achieve their nefarious objectives. Since 9/11, it should also be noted, cybercrime has facilitated terrorist financing. As illustrated by the planning and execution of the Bali bombings of 2005, cyber-attacks have become the business model of choice for a wide range of organized elements, including international terrorists, who have employed widespread campaigns as a significant source of funding for themselves and their real-world activities.

While it may not yet be common knowledge that organized, extremist terrorist efforts are already engaging in sophisticated cyber-attacks for the purpose of damaging U.S. computing assets, and even infiltrating our critical grid infrastructures, it should be noted that these groups are also using cybercrime as a significant source of financial support. The evolution of information technology has empowered our culture with an incredible capacity to advance many of our personal, business and governmental interests, but these computing and communications tools have also a created a new, virtual and highly vulnerable frontier on which parties can carry out attacks on Americans from halfway around the globe behind the obscurity of their computers.

As many of you already know, from instances of foreign government-backed entities compromising the computing systems of our most sensitive and closely guarded national agencies, including the Department of Defense, to individuals launching computer virus attacks meant to exfiltrate the most valued intellectual property from private enterprises responsible for powering our nation's economy, the complex

risks posed to the United States by the current epidemic of cybercrime should not be underestimated.

To note, the United States Computer Emergency Response Branch (U.S.-CERT) reported that there was a 40 percent increase in external computer intrusions into systems operated by the U.S. government during 2008. As far back as 2005, the Department of Justice assessed that over two-thirds of U.S. businesses had already been impacted by cybercrime. And at last year's World Economic Forum in Davos, world leaders estimated that there have already been over $1 trillion in losses suffered by the global economy via the electronic expatriation of intellectual property and financial data.

Most recently, in a study published by security consultants at Verizon Business, the experts reported that of the 90 individual breaches they investigated among customers in 2008, over 285 million records were stolen via those cyber-attacks alone.

To summarize, cyber-attacks have become a wholly pervasive phenomenon based in part on:

- Increasing connectivity and availability of assailable network, systems and applications vulnerabilities.
- The ability of cybercriminals to derive significant financial rewards through successful attacks.
- Worldwide federation between various classes of cybercriminals and malware developers.
- Nation-state, terrorist and politically driven backing of targeted cybercrime efforts.
- A lack of cohesive law enforcement around the globe.

My goal today is to outline to the Committee several areas of federal activity where I believe that more aggressive and devoted effort must be exerted to improve the ability of our government agencies, critical

infrastructure providers and the many private contractors with whom they interact, to improve their ability to manage the risk posed by a hostile cyberspace.

I will also highlight several elements of enforcement currently operating under the Department of Homeland Security that deserve expanded support, both in their funding and their level of authority, to substantially improve our national cyber-defenses.

It is my contention that given this Committee's consideration and leadership, our government will not only secure itself but each of us as individuals from the range of cyber-attacks that we will continue to encounter both now and tomorrow as the adoption of technology and the subsequent evolution of the cybercrime ecosystem.

## Recommendations

### I. Expanding Capabilities Under DHS

One of the primary aspects of my appearance here today is to help shed light on some of the strengths and weaknesses of current enforcement mechanisms operating under the auspices of the National Cyber-security Division of the Department of Homeland Security. It is my overall assessment that while these efforts have significant value and potential in advancing important matters of cyber-defense, for the most part these initiatives have not been given sufficient financial or operational support to address their all-important mission.

Overall, while the DHS has made a good faith effort via all of these programs to improve U.S. federal standing in relation to cyber-attacks, the agency continues to struggle with major issues in its approach. Over-arching challenges that continue to detract from these efforts include:

- **Lack of Management Continuity** – many of DHS' senior cyber-security leadership positions are political appointments and by nature,

result in frequent turnover of management personnel, and changes in priorities and focus of the organization's mission. Compared to other departments, DHS has an inordinate number of political appointments in leadership positions.

- **Insufficient Support Structure –** within DHS to provide fundamental functions to support cyber-security needs, such as procurement, budget/accounting, human resources, facilities, and compatible information systems.

- **Lack of Identity/Motivation** – compared to more mature departments and agencies, DHS has not realized a true *cultural identity* within its workforce, particularly in its cyber-security mission. This is an intangible characteristic, but critical to motivating and sustaining the professional workforce for the long term. One outcome of this problem is tremendous personnel turnover with political appointments and career government officers since DHS' inception.

There are three groups currently operating under DHS that I will address specifically, the U.S. CERT, the Secret Service Electronic Crimes Task Force, and the DHS Federal Network Security Branch – along with touching on the DHS Cyber-Storm incident response exercises:

1. **U.S.-CERT**

The United States Computer Emergency Response TEAM, or CERT, serves one of the most important roles in federal oversight of issues impacting matters of national cyber-security, both for government entities and our legions of private organizations. In researching and responding to emerging cyber-security threats ranging from virus and malware attacks to IT security vulnerabilities discovered in widely used technologies, U.S.-CERT fills the vital role of our national cyber-defense first responders.

Among the few existing efforts that successfully reach across both public and private sectors to help advance U.S. readiness for, and response to, cyber-security issues, it is my opinion that U.S.-CERT is fulfilling a critical role in providing our nation with crucial intelligence needed to stay ahead of both existing and future cyber-attacks. While there is continued emphasis being placed by executive leadership on any efforts that can be made by the federal government to create partnerships that foster closer cooperation between public and private entities to share information and expertise in the area of warding off cybercrime, U.S.-CERT is perhaps the best example of an established resource that is meeting those expectations today.

At the same time, U.S.-CERT has been limited in its ability to move beyond mere information sharing into other more dynamic operations that can provide even greater insight into cyber-security problems, based on a lack of sufficient funding and organizational authority.

U.S.-CERT needs to be the country's cyber-defense and coordination agency that has the ability to introduce private subject matter expertise to get actionable threat mitigation information to critical infrastructure and federal agencies.

## 2. Secret Service Electronic Crimes Task Force

Much like their colleagues at U.S.-CERT, the dedicated special agents working for the Secret Service Electronic Crimes Task Force have been doing an admirable job in helping to monitor and react to cyber-security trends. As an extension of the Secret Service's core mandate to safeguard the nation's financial infrastructure and payment systems, the Electronic Crimes Task Force has served a crucial role in aggregating vital cyber-intelligence, investigating specific cybercrime incidents, and channeling the information garnered via those efforts into subsequent attempts to identify and impede those organizations and individuals responsible for executing these illegal activities.

However, from both a resource and organizational standpoint, the Secret Service Electronic Crimes Task Force currently faces several major hurdles in order to expand its own intelligence-gathering and enforcement capabilities.

Firstly, like U.S.-CERT, the Task Force needs greater financial backing to track and pursue operators attempting to carry out cybercrime activities in our nation, and overseas, today. From providing the Task Force with the more substantial manpower and technological tools necessary to complete these tasks, to ensuring that the most qualified agents working across the Secret Service can be enlisted and retained in executing these responsibilities, the Task Force requires a higher level of support, and greater authority among its peer organizations, to deliver on its current mandate.

A specific problem that the Task Force must address is the Secret Service's operational tradition of rotating agents through frequent post transitions to maintain a fresh approach to all its matters of enforcement. While this is clearly a very useful approach in many aspects, the work being tackled by the Task Force requires the highest level of technical acumen to address the sophisticated nature of today's real-world cybercrime activities and to maintain the continuity necessary to investigate these attacks. I would specifically suggest that in addition to providing the Task Force with greater financial backing, that the Secret Service be encouraged to adjust some of its longstanding staffing functions to ensure that it has the most qualified people on the job every day dedicated to this crucial cyber-security effort.

### 3. Operation Cyber Storm

I would also like to call attention to the twice-completed/bi-annual Cyber Storm cyber-security defense exercises, which have provided valuable insight into the ability of government and private organizations responsible for management of critical national infrastructures to react to cyber-attacks.

As noted, these organized tests run by the DHS to assess cyber-security readiness across public and private infrastructure offer us a vital window into the ability of our nation's critical grid services providers and law enforcement communities to respond to major cyber-attacks. However, to permit us even greater insight into the specific strengths and weaknesses in these areas, and understand how critical infrastructure (specifically energy, telecommunications, financial and health IT systems) stand up in the face of widespread and targeted campaigns, the Cyber-Storm exercises must be expanded, with participation from crucial private entities transitioned from voluntary to mandatory status.

In addition to requiring organizations responsible for critical grid infrastructure to take a more active role in simulating cyber-attacks, they must be pushed to participate in these exercises on a frequent and regimented basis. I would also suggest that these exercises must be altered to be less oriented toward check-box, paper-based requirements and expanded into more dynamic, realistic emulations of real-world cyber-attack conditions. Specifically, these tests should become focused less on issues of infrastructure resiliency and service performance, and encompass more of the highly sophisticated staged infiltration techniques being employed by today's heavily organized cyber-criminals and state actors.

### 4. NCSD Federal Network Security Branch

Even more so than the two previously cited organizations addressing cyber-security under DHS management, the Federal Network Security Branch finds itself in a challenging position in terms of fiscal backing and authority. For, while the Branch currently maintains a worthy desire to address its goals of hardening U.S. network computing infrastructure against cyber-attack, the organization has not been provided with the necessary support to deliver on its strategic objectives. That said; the Branch has done a tremendous job in maximizing the resources that have historically been placed at its disposal.

A specific example of the many organizational challenges faced by the Branch can be found in its oversight of Presidential Directive 23, which addresses governance of Network Operations Center (NOC)/Security Operations Center (SOC) operating standards. While this management function represents a substantial opportunity for the Branch to have a significant impact in improving the capabilities of these installations to help our nation predict and respond to emerging cyber-security issues, it has not been granted the necessary authority to foster the needed defense-in-depth protective IT mechanisms needed to empower these operations.

One of my specific criticisms of the manner in which the NCSD Federal Network Security Branch is currently operated is that its initiatives have been focused too heavily on enforcement of policies related to regulatory compliance based on existing FISMA requirements. An example of this reality can be found in its efforts around the advancement of the Trusted Internet Computing (TIC) program, an effort mandated in an OMB memorandum issued in November 2007. This memorandum was meant to optimize individual external connections, including Internet points of presence currently in use by the federal government of the United States, to address security issues.

While the Branch has played a vital role in forwarding this important infrastructure hardening enterprise, it has not been able to serve in a lead role in driving expansion and enforcement of TIC, which has deteriorated the initiative's overall ability to produce substantive, measurable improvements to our national cyber-infrastructure.

I would suggest that in re-addressing the National Cyber Security Divisions efforts, that the Federal Network Security Branch be empowered to act as the lead when driving TIC and similar programs. A red teaming penetration testing capability should also be established within the Federal Network Security Branch to provide greater

situational awareness of weaknesses in civilian agency network security postures.

## II. Realizing IT Risk Management via Red Teaming Security/Penetration Testing

As evidenced by specific campaigns carried out against federal agencies in recent years, and further illustrated by trends emerging on the larger cybercrime landscape, a lack of situational awareness and an inability to predict the specific methods being utilized by electronic assailants of all archetypes has been one of the most significant failures in stemming the tide of successful attacks.

While organizations across the federal space, as well as the private sector, have gone to great lengths to employ layered defensive mechanisms aimed at preventing specific classes of threats from infiltrating their IT systems, clearly, based on the successful campaigns that we know of – such as the set of coordinated cyber-attacks emanating out of China beginning in 2003 labeled "Titan Rain" – which compromised assets at the DoD, NASA and Sandia National Laboratories, as well as those of federal contractors – these existing perimeter defenses have been proven vastly insufficient. And as we know there are many more incidents that have occurred and that have not been reported publicly.

To address this dire reality, which has been highlighted most recently by widely publicized hacking of the U.S. energy grid and electronic data theft carried out against private merchants such as Heartland Payment Systems, which saw thieves make off with millions of its sensitive customer payment card records, the federal government must expand the Federal Information Security Management Act (FISMA) to compel all agencies to undergo more frequent internal assessments to gauge their risk to cyber-attacks.

Agencies must embrace the results of exercises including “Operation Eligible Receiver" – an audit of the Pentagon’s exposure to cyber-attack ordered by the Joint Chiefs of Staff in 1997 – through which internal security testing specialists, dubbed Red Teams, found it exceptionally easy to circumvent existing defenses to compromise and infiltrate some of the government’s most heavily guarded IT systems – to better assess their own exposure to hacking techniques of all varieties.

Specifically, agencies must be required to conduct regular, extensive security audits of their IT systems using Red Team penetration testing methodologies to gain a more precise fix on where their most significant weaknesses lie by emulating the same tactics as those being employed by cybercriminals. I would suggest that these Red Team exercises be carried out on at least a quarterly basis due to the dynamic nature of the cyber-threat environment.

These quarterly security and IT systems penetration tests (as defined by NIST special document 800-53A, Appendix G) must be applied to all federal networks and computing assets, as well as those of critical infrastructure providers across the energy, telecommunications, finance and health sectors, among others, to empower both government and private organizations to gain a better understanding of where they are most vulnerable to real-world attacks. Using classic risk management practices via the employment of techniques that mirror those used by attackers in a safe, controlled manner, those critical vulnerabilities that are identified via this process can then be remediated.

In addition, I would ask this Committee to consider the creation of systems of accountability, including penalties, for those organizations found to be unable to properly address their critical vulnerabilities.

By compelling federal agencies and their business partners to engage in this proactive security testing, and specifically conduct regular internal Red Team penetration testing assessments, these organizations will be able to both identify their most pressing instances of IT risk to ward off

attacks, and to create concrete benchmarks that they can refer to frequently over time to mark their progress in improving their security posture. Subsequently, this will also allow organizations to more wisely allocate finite IT security resources.

## III. Securing the Managed Service Supply Chain

The infamous breach of DHS three years ago was based on a lack of standard of care and due diligence enforced by a third-party managed service provider. The previously noted 2008 Verizon Data Breach Report noted that 39% of breaches were a result of hackers transiting/island-hopping through strategic partner networks. For these reasons, it is imperative that we grapple with the systemic risk posed by outsourcing which permeates our digital ecosystem.

The reason why global businesses open offices in New York City and pay astronomical rent is because they have trust and confidence in the safety and soundness of U.S. markets. These businesses have faith in the rule of law, the enforcement of contracts and the security of the physical U.S. marketplace.

This real world phenomenon can someday manifest itself in cyberspace if political leadership challenges the Web hosting, data warehousing and many other managed IT service providers serving the federal market to improve their standard of care per cyber-security.

In order to promote and create a secure U.S. cyber-ecosystem, this Committee should mandate that all entities who provide Managed Information Services of any sort to the U.S. government or providers of critical infrastructure (as defined by the NIPP) sign Information Security Service Level Agreements (ISSLAs) which include at a minimum a specific standard of care. The agreements must require that these service providers:

- Verify that the legal requirements to which service providers are contractually obligated to provide security are compatible with NIST 800-53.
- Outline and review their incident response plans prior to any movement of data or provision of service.
- Confirm that their policies and agreements regarding security breaches include customer notification on a timely basis (within one hour) and maintain the right to test their incident response plans on an annual basis.
- Confirm that service providers have adequate data backup facilities which are also regularly tested for security vulnerabilities.
- Conduct Red Team penetration testing of their network security posture, and verify whether they have sufficient layered IT defense mechanisms (NIST 800-53A, Appendix G serves as excellent guidance on this matter).

We must use federal acquisitions policy to require these service providers comply with all of these individual requirements. Those organizations that cannot or will not comply in this manner should have their contracts revoked.

This Committee might also consider a federal bill giving tax credits to all commercial entities that currently are FISMA compliant, as well as offer tax credits to those organizations who maintain ISSLAs with third parties and strategic partners in 2009.

## IV. Closing Remarks

In summary, while the national and worldwide cybercrime pandemic is currently scaling in an exponential manner, I would submit that significant gains can be realized throughout the federal government today via the political application of more aggressive attention and

investment on the part of involved stakeholders. The CSIS Report noted that since markets have failed to evolve in the face of unprecedented market forces, new public policies are necessitated.

By aligning our organizational assets and international relationships more effectively, and adopting a more comprehensive risk management approach to securing our critical national computing and communications assets, the United States can turn back the tide of cyber-attacks.

In this dark hour we need strong bipartisan leadership. The dramatic increase in cyber-attacks necessitates action. The recent 60 Day Cyber Review developed by Melissa Hathaway, the Obama Administration's acting director for cyberspace, represents a great starting point for the Administration to lead our nation’s cyber security efforts. However, it is paramount that this Committee understands that it too can serve a fundamental role in defending our nation’s critical infrastructures.

I appreciate your consideration of my statement and your public service.

Sincerely,

Tom Kellermann, CISM
Vice President of Security Awareness
Core Security Technologies