Testimony
House Homeland Security Committee
"Reviewing the Federal Cybersecurity Mission"
Amit Yoran
NetWitness Corporation
March 10, 2009

Mrs Chairman and Ranking Member, thank you for the opportunity to testify before the Homeland Security Committee on Reviewing the Federal Cybersecurity Mission.

My name is Amit Yoran and I am the CEO of the NetWitness Corporation, a company providing next generation cybersecurity monitoring technologies to the US Government and private sector, including Fortune 500 companies delivering critical infrastructure cyber protection to the Nation. I serve as a member of the CSIS Cyber Commission advising the 44th Presidency and on numerous security industry advisory bodies.

Previously I have served as the first Director of the National Cyber Security Division (NCSD) in standing up the United States Computer Emergency Readiness Team (US-CERT) and Einstein program at the Department of Homeland Security (DHS), as founder and CEO of Riptech, a leading managed security services provider, and as manager of the Vulnerability Analysis Program (VAP) of the US Department of Defense's Computer Emergency Response Team (DoD CERT). I received Bachelor of Science degree in Computer Science from the United States Military Academy at West Point and Master of Science in Computer Science from The George Washington University.

Over the past fifteen years, automation and use of computer systems has permeated every aspect of modern life. Our Nation is entirely reliant upon computer systems and networked technologies in everything from national security and intelligence activities to commerce and business operations to power production and transmission to personal communications and correspondences.

Today's Internet has become one of the unifying fabrics driving Globalization at an increasingly accelerated pace. It represents the core means by which personal and organizational interactions occur whether those communications take the form of Internet email or simply phone calls, which invariably traverse the cyber realm. Beyond its role as a communications medium, computer based automation and technology are the driving forces behind every major industrial and economic base in the world. Simply put, computer technologies and communications represent the greatest threat to and opportunity for expansion of the US values system.

Evolving into a National Cyber Strategy

The past two years have brought about an unprecedented level of federal focus and attention on cyber security matters culminating in a portfolio of activities commonly referred to as the Comprehensive National Cyber Initiative (CNCI). Advocacy for CNCI under the Bush Administration resided in the Office of the Director of National Intelligence (ODNI), under whose charge the billions of dollars in programs were conceived and orchestrated. While many of the CNCI programs are well intended and designed, there are several significant flaws in adopting the Bush Administration's CNCI as an ongoing national cyber strategy.

- White House leadership. The Obama White House is currently conducting a comprehensive 60 day review of cyber. The purpose of the review is to develop a strategic framework to ensure that "initiatives in this area are appropriately integrated, resourced and coordinated both within the Executive Branch and with Congress and the private sector." This review effort will culminate in recommending an optimal White House organizational structure for dealing with the cyber challenges facing our national and economic security as well as "an action plan on identifying and prioritizing further work in this area." For the reasons outlined below, an effective national effort to address cybersecurity can only succeed through continuous, active and decisive White House leadership.

- Intelligence.

  o An effective national cyber strategy must leverage the strength of the intelligence community. As information and computer-based technologies increasingly permeate how the world works, opportunities abound to improve the types, quantity and quality of intelligence the community can provide at various levels of classification to its consumers. In the primary intelligence functions of collection, analysis and dissemination, cyberspace can provide an effective aspect to operations. The volumes of information and the diversity of sources can quickly become overwhelming. The intelligence community must continue to refine its ability to evaluate the quality and value of such information and accurately assess it in order to assure its appropriate dissemination to decision makers. This should include improved functionality around attribution in cyberspace.

  o There is a clear and distinct conflict of interest between intelligence objectives and those of system operators. Simply put, intelligence organizations prioritize the intelligence and counter-intelligence missions; which in cyber focuses on monitoring adversaries, determining their methods and techniques, tracking their activities to a point of origin, and determination of compromise scope, intent and objective. While these are very important, they frequently conflict directly with the information assurance objectives of system owners and operators, who are primarily concerned with system defense and protection, and in the event of

compromise, a speedy restoration to a functional and assured state. This distinction in core objectives is critical because it represents the difference between programmatic emphasis on information gathering, or system resilience and availability. For instance, Intelligence and Law Enforcement entities often prioritize attack attribution, while almost no emphasis is placed on attribution by those defending systems. Rather than sharing information with operators and better informing them as to how they can defend and monitor themselves, an intelligence community centric mindset around cyber would limit information exchange and instead focus on enabling the intelligence community to perform an expanded and aggregated monitoring program. Such a monitoring program would face significant cost and scalability impediments. We must remember the purpose for a monitoring program. Are we in fact monitoring to enable better defenses? Who makes the decisions to inform the defense? It is a clear conflict of interest for those who collect to make this decision. The decision should be a balanced one. Prioritizing the intelligence mission also has significant resource allocation implications. Amid news stories of billions of dollars in cyber spending under CNCI a majority of resources are going to intelligence and centralized monitoring activities. For instance, the Center for Disease Control, where sensitive information resides about biological threats, such as Anthrax, has ongoing incidents which they do not have the manpower or technology to adequately investigate. In the face of these challenges, this year the CDC's cybersecurity budget will be reduced by 37%.

o For ill defined reasons, the CNCI led by ODNI has been shrouded by a high degree of secrecy and lack of transparency. The plan itself is so classified that even members of Congress have not been provided copies and industry has had no access to the document. While the need for high levels of classification may exist in certain components of a national cyber effort, such as offensive capabilities or for the protection of sources and methods, such a broad over-classification is counterproductive to supporting an effective cyber defense. Such information is prevented from being shared with operators, most of which do not hold adequate clearances and creates significant hurdles when trying to defend unclassified systems. In recent examples adversary internet addresses used in attacks and their various attack methods have been classified to the point they were not broadly available for defensive purposes or provided through channels. In numerous cases this roadblock prevented information from being used effectively in cyber defense and provided further advantage to our adversaries. If you can't or won't share useful information with cyber defenders, their job is made far more difficult. As the private sector is increasingly the target of foreign intelligence efforts, a national cyber effort will need to further evolve its abilities in working with the private sector. Most importantly, over-classifying a national

cyber strategy prevents adequate public review and debate to assure that the programs are designed optimally, contain the highest level of innovation, and are well-aligned with and informed by the total body of knowledge of the cyber security profession. Often classification is used to hide weaknesses found. Classification cannot be used effectively as a cyber defensive technique, only one for avoiding responsibility and accountability.

- o Intel loss/gain analysis has historically been performed by the intelligence community's judgment without substantive subject matter input from those whose are being damaged. If the intelligence community takes on a leadership role for the cyber mission it is likely that additional monitoring programs will be put in place to find the adversary. While the technical acumen within NSA is strong, better controls over operations would be needed to reduce the natural emphasis on collection and instead prioritize the protection and availability of government and industry systems. The cyber mission suffers in favor of the intelligence mission all too often. While protecting sources and methods, the intelligence community needs to better inform public and private sectors on the threat environment and how they can better defend themselves. Moreover, some organizations may be less likely to act responsibly and invest properly in monitoring and defending their own systems if they feel as though they can rely on some federated intelligence monitoring operation.

- Research and Development. The current paradigm in cyber security is not likely to change significantly through improved security products, monitoring and incident response capabilities. While the private sector makes significant investment in incremental product, application and protocol improvements; fundamental research is required to meaningfully improve the security of the cyber and critical infrastructures.

- o According to the CSIS Commission work, "The federal government plans to spend about $143 billion in 2009 on R&D. We estimate that two-tenths of 1 percent of that will go to cybersecurity." An inherently government investment must drive long term research agendas in cybersecurity, where private sector focus on shorter term commercialization limits results to more tactical or incremental advancements. The Department of Homeland Security's Science and Technology Directorate invests less than $20 million per year on cybersecurity research efforts, a far cry from any responsible level of resource allocation.

- o The government should not use this money to be in the security product development business, especially via classified venues. In an overwhelming majority of instances, government cyber requirements are substantially similar to if not exactly the same as the private sector and only in the rare cases where they do not or in classified instances, do specific tactical government development

efforts make sense to consider. In addition, it is a fact that there is a severe lack of qualified engineers needed to develop these systems. Today, the majority of these engineers are employed by the security industry. The government and intelligence community should guide and assist in functional requirements for the development of technologies which can help us best address the sophisticated cyber threat environment, not enter the product development business. The resulting improvement in security technologies will not only benefit the government in protecting its systems, but will also benefit the nation's critical infrastructure operators and rest of the shared Internet fabric that joins our digital world. Additionally, government development efforts have stranded enterprise cyber defenders without the benefits of product management, maintenance and professional support.

- Standards and Acquisition reform. The CSIS Commission report provides a lot of insight into how the government can positively improve its situation as well as security of private networks by using leveraging its expertise in standards setting and using its procurement size to effect product vendor behaviors. We also need to consider more dynamic methods for systems procurement and lifecycle management as opposed to the current processes which seem marginally nimble enough to enable the purchase of a battle tank or fighter jet. Antiquated and poorly maintained systems compound our challenges. The systems on federal networks average 5 years old. Unlike responsible parties in the private sector, federal networks frequently do not have centralized patching, vulnerability understanding or adequate monitoring technologies and processes. Simply put, they are not achieving or maintaining an appropriate standard of care by any responsible measure. It should be understood the reasons for this are a lack of IT and IT Security Governance. The technology here is not overly complex, the real challenge is the people and the process. The average government executive, whether DoD or Civil, stays in his/her position for an average of 18 months. There is little or no reason to look ahead at the next executive's tenure and budget or plan for the life cycle management or security of a system 18 months later. In addition, because planning was not done in the previous executive's tenure, the system the executive has to care for is more likely than not to be in an unkempt, dated, and insecure state. There is no governance mechanism or motivation for government systems to plan, budget, or perform best practice life cycle management which can significantly reduce risk of loss. Please see the recently published Consensus Audit Guidelines for a reasonable approach to minimal security practices.

- Legal Review and Privacy Oversight.

    o Congress and the Obama Administration must work together to modernize authorities FISMA and Clinger-Cohen are dated and fraught with politics and

games. Without hard hitting, detailed legislation that structures governance and authorities no program will be enabled to succeed. Today the CNCI is not codified. HSPDs 54 and 23 are not supported by legislation, therefore are not mandated. An immediate, thorough and transparent legal analysis of the governance, authority, privacy requirements to secure Federal Cyber space must occur.

- o An effective national cyber function requires an informed privacy function. Privacy issues need proper review and advocacy when designing various government cyber security programs, especially those of the intelligence and law enforcement communities. An effective program should be implemented in a non-partisan fashion by qualified privacy professionals who are not members of the executive branch and have fixed terms of service without eligibility for reappointment or extension terms. Security can be implemented with and even contribute to enhanced privacy, but it is not easy and often not without strong and deliberate privacy advocacy and oversight.

- Homeland Security.

    - o The Department of Homeland Security (DHS) has demonstrated inefficiency and leadership failure in its cyber efforts. While pockets of progress have been made, administrative incompetence and political infighting have squandered meaningful progress and for years now our adversaries continue to aggressively press their advantage. Recently, the Director of National Intelligence, Admiral Dennis Blair, told the House intelligence committee that the NSA, rather than the Department of Homeland Security which currently oversees cybersecurity, has the smarts and the skills to secure cyberspace. In his assessment of both organizations he is absolutely correct. DHS has repeated failed to either attract or retain the leadership and technical acumen required to successfully lead in the cyber mission space. On a number of occasions proven, talented and knowledgeable leaders from within the government or successful experts from private sector have joined the department in hopes of meaningful contribution. In its cyber responsibilities DHS has a consistent track record for tolerating political infighting, individual egos and shenanigans over prioritizing and executing its cyber responsibilities in a mature fashion. While the tendency would be to migrate the cyber mission to the NSA, that would be ill advised for all of the reasons provided earlier. In Rod Beckstrom's resignation letter last week, he states, "NSA effectively controls DHS cyber efforts thru detailees, technology insertion and the proposed move of NPPD and the NCSC to a Ft Meade NSA facility. NSA currently dominates most national cyber efforts…The intelligence culture is very different than a network operations or security culture. In addition, the threats to our democratic processes are significant if all top level government

network security and monitoring are handled by any one organization." This could not have been more accurately stated. We must enable civil government to succeed at this mission. This being said, it is far past time we fix the DHS problems and move forward.

o Interaction with the Private Sector. In addition to defining increased security functionality and assurances for Commercial off the Shelf Software (COTS), the government must work more closely with the private sector and understand their businesses if it is to be effective in generating useful programs. Programs managed in a vacuum by the intelligence community at a highly classified level are unlikely to work well and in concert with system operators within the federal government, let alone in the private sector, where not only are mission objectives completely foreign, but where there are very few people with government clearances. Government programs need to focus on open dialog and information exchange, and enabling the private sector to better understand the security challenges they face and how they might be overcome with the help of the Government.

o Public Private Partnership. DHS is the natural and appropriate placement for public private partnership and cooperative activities, including those in cyber security. The current set of public private partnerships are at best ill defined. While well intentioned and occasionally valuable information is brought to the department, they categorically suffer from meaningful value creation to the private sector. A deeper understanding of cyber defense and security operations in the private sector is required by those crafting the evolution of these programs or future programs so that adequate incentives can be appropriately incorporated into these programs. Such incentives might include tax consequences, fines, liability levers, public recognition, or even at an operational level, such as the sharing of threat intelligence, technical knowledge or incident response support to name just a few. In news reports and discussions among privacy and civil liberties groups the role of the NSA in monitoring or defending domestic private networks is debated. Should such intelligence programs exist, DHS should be very careful to distance itself from participation, support or engagement in these activities. Due to its fluid nature, trust relationships when dealing in cyber security matters are at least as strongly emphasized as in physical security. The department's ability to fulfill its primary mission and responsibilities may be permanently damaged by a loss of public confidence and trust. At a bare minimum, in order to preserve public trust interaction with domestic intelligence collection efforts should be explicitly and clearly articulated.

o NCSC and US-CERT. Focus DHS where it can have the greatest positive impact. The department's culture migrates toward increasing its own mission and scope

and infrequently emphasizes a crawl, walk, run mentality. Sometimes, it's time to close PowerPoint and Word, stop the rhetoric and simply get the sleeves rolled up and begin the work itself. For instance, spending the department's limited resources on advocacy programs for better software development, where the department has very limited experience, expertise and credibility is of exceptionally limited value. At present the US-CERT remains torn apart into three arms; a technology deployment arm (lead by an intelligence community detailee), a security arm (managing the Trusted Internet Connection program), and the operations arm (performing the core US-CERT mission). This stove piping has added political strife, inability to spend 09 money this year, and defocusing all from accomplishing the single US-CERT e mission. US-CERT must be the primary mission lead by a single federal civil executive. On the other hand, the coordination function of the National Cyber Security Center is underutilized. Rod Beckstrom's recent resignation claims that only eight weeks of the annual funding have been provided to it. In order to regain any efficiency, the department's operational security role, which has been ripped apart by years of political infighting must be reconsolidated in the US-CERT. The US-CERT, whose mission is to support the security of government networks through design, deployment and monitoring the Einstein series of programs to enhance situational awareness, be the centralized incident reporting authority for the federal civilian networks, facilitate efficient incident response and cleanup efforts, and support the private sector through information exchange with critical infrastructure operators, and working with IT and IT security product vendors to assure that they can address the needs of the broader federal government and critical infrastructures. The critical work of the US-CERT with its operational mission is resourced only marginally better than the NCSC (fewer than 20 government FTEs, a budget of only $67 million out of the departments $355 million spend on cybersecurity). As with the NCSC, the US-CERT also reports to detailee from the USSS, who reports to detailee from NSA/Navy. All special assistants around the Acting Assistant Secretary are also NSA detailees. The US-CERT must be provided appropriate staffing levels to move forward and given adequate funding. Not doing so cannot help but send the strongest message to the cyber community, the rest of government, the intelligence community and the private sector that cybersecurity under DHS will not be treated any more responsibly under the Obama Administration than it was previously. A newly focused cyber mission must report directly to the Secretary of DHS. This critical mission has been sought aggressively by so many parties, but resisted so strongly by the department responsible for its successful execution. Cyber must not remain buried in the bureaucracy of DHS or it must be taken from the department in its entirety.

The House Homeland Security Committee and Congress should work with the executive branch to assure these fundamental changes are made:

1. DHS must be charged with and enabled to build an effective cyber capability in support of securing federal civilian systems.

   a. Make special provisions in the hiring, contracting, human resources, political issues within the cyber mission of DHS to prevent it from remaining a victim of the department's broader administrative failures.

   b. Enable the US-CERT to stand up the capabilities necessary to assist in the defense of federal civil government as a component of the federal civil agency charged with defending the homeland.

   c. DHS should also be given specific emergency authorities to specifically address security concerns in civil systems, to include the ability to measure compliance with security standard, protocols and practices and take decisive action where organizations are not applying reasonable standards of care.

2. Flesh out, define roles, responsibilities and authorities of DHS, DoJ, DoD, NSA, and other federal departments and agencies engaged in securing digital infrastructure. Such a framework should be publicly stated so that trust and confidence in cyber programs can be restored. It will also be a critical step in guiding more informed and consistent interactions with the private sector. Steps must also be put in place to allow the White House, Congress, Departments and Agencies to have visibility, input and clear oversight into the process and solutions.

3. Adequately resourcing for success.

   a. A large-scale reallocation of the DHS cyber monies toward the programs which are operational and provide meaningful value add to its responsibilities to the federal civil networks is needed.

   b. There exists tighter control and millions of dollars spent by DoD and NSA to protect the DoD networks, and that they still are under-resourced to adequately defend themselves. Only a fraction of that is being spent to defend federal civilian systems and in reality those networks are by comparison 10 times larger than the Defense Department's.

Thank you for the opportunity to testify. I would be happy to answer any questions you may have at this time.