Testimony
House Permanent Select Committee on Intelligence
"Intelligence Implications of Recommendations from the CSIS Commission on Cyber Security for the 44th President."
Amit Yoran
NetWitness Corporation
September 18, 2008

Mr Chairman and Ranking Member Thank you for the opportunity to testify before the Committee on the Intelligence Implications of Recommendations from the CSIS Commission on Cyber Security for the 44th Presidency.

My name is Amit Yoran and I am currently the CEO of NetWitness Corporation, a company providing next generation cybersecurity monitoring technologies to the US Intelligence Community, the broader Federal Government and the private sector, including Fortune 500 companies delivering critical infrastructure services to the Nation.

Previously I have served:

As Director of the National Cyber Security Division (NCSD) and the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS), CEO and founder of Riptech, a leading managed security services provider, and 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 computer 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 the US Intelligence Community.

Commission Findings

As you know, this Commission was established a year ago and while the formal results are expected to be published in November, the Commission's findings are not yet in their final form. As such, the observations below are based upon personal experience and my perceptions of the Commission's work to date and expectations of what the Commission's findings will likely be.

Some expected findings of the CSIS Commission are:

- The Department of Homeland Security lacks the personnel, capability, authority and culture required to do the job entrusted to them by the President and Congress. "Most of the time, every day, I spend most of the bullets in my single 30-round magazine that I bring to work every day shooting into the backs of our own bureaucracy trying to clear a field of fire. So, I have one bullet left to either pump at al Qaeda or save it for me because the bureaucracy is about to overwhelm me," said Robert Stephan, DHS assistant secretary for infrastructure protection. DHS' cyber efforts are disorganized and disjointed and practical operations continued to be buried deeper within the organization. U.S. National Security interests require ongoing support from the White House if they are to succeed.
- The U.S. Government lacks a comprehensive national strategy to effectively deal with the opportunity and manage the risks associated with cyber security. The Comprehensive National Cyber Initiative (CNCI) represents a significant step forward and commitment to the challenge. A national strategy can inform and better leverage efforts such as the CNCI
- An effective offensive capability in the cyber domain are required for a wide variety of intelligence purposes including a credible deterrence and defense. Defense, deterrence and offensive capabilities affecting the cyber domain should not be limited to cyber means.
- An overly broad definition of what constitutes critical infrastructures risks diluting scarce resources, expertise and efforts. Such definitions risk lowering our overall preparedness.
- Interaction between the Federal government and critical infrastructures in the private sector remain disjointed and inadequate for national security objectives.
- The incoming administration should work with Congress to modernize authorities such as T3, FISMA and Clinger-Cohen to better address the cyber environment.
- The private sector attempts to bring effective cybersecurity technologies to market. At times such efforts include investment in development activities which result in new cyber capabilities. Only in very rare instances is the private sector making significant investment in cybersecurity research. The Federal government should organize and invest in a series of fundamental research efforts to longer term improve the state of cyber security and reduce our national exposure.

In addition to the expected recommendations of the CSIS Cyber Security Commission, I believe that a National Privacy Oversight function is required. This function is needed, not so much on the specific details of program implementation, but more so to assure that privacy issues have been taken into account when designing various cyber security programs by the government and specifically in the intelligence community. 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.

Contributions of the Intelligence Community

An effective national cyber strategy must leverage the strength of its 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 its in order to assure its appropriate dissemination to decision makers.

The intelligence community also performs two additional functions in support of a national cyber activity. In its counterintelligence capacity, the Intelligence Community is responsible for "identifying, understanding, prioritizing and counteracting the intelligence threats (from foreign agents) that are faced by the United States." Given the pervasive evidence that cyber operations are increasingly the preferred asymmetric method for foreign intelligence services collection against the U.S., the counterintelligence functions need significant prioritization and resources. In a context of cyberspace, these activities often target the economic and industrial bases of the U.S. It is target that the intelligence community has not traditionally dealt with as a target for foreign intelligence services.

And the Intelligence Community has an additional function in performing special activities; such as covert and clandestine actions, in the cyber realm computer network attack and computer network exploitation respectively. These operations are typically classified at the highest levels. They are also most effective when conducted in combined operations leveraging cyber capabilities in support of other intelligence capabilities or other intelligence operations enable information to be gained or exploited using cyber means.

While the intelligence community has a pivotal role to play in a national cyber strategy it must also be an evolving role. The intelligence community is not particularly adept at interacting with entities outside of the intelligence community. Often the community's desire to protect sources and methods causes information to be classified at very high levels. Such classification of data

causes great impediments when attempting to share it as actionable information with those in attempting to protect their systems. In recent examples adversary internet addresses used in attacks and their various attack signatures have been classified to the point they were not broadly available for defensive purposes or provided through channels which prevented their being used effectively in cyber defense. As the private sector is increasingly the target of foreign intelligence efforts the intelligence community will need to further evolve its abilities in working with the private sector.

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