Testimony

House Homeland Security Committee

Subcommittee – Cybersecurity, Infrastructure Protection and Security Technologies

Hearing: Examining the Infrastructure Protection and Security Technologies

Mischel Kwon

Mischel Kwon and Associates, LLC

March 16, 2011

Good morning Chairman Lungren, Ranking Member Clarke, and other distinguished members of the subcommittee. Thank you for the opportunity to testify before the Subcommittee for Cybersecurity, Infrastructure Protection and Security Technologies.

My name is Mischel Kwon and I am the President of Mischel Kwon and Associates, LLC, a consulting firm specializing in Technical Defensive Security, Security Operations and Information Assurance.

Previously I served as the Director of the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS), and as the Deputy Chief Information Security Officer and Director of the Justice Security Operations Center at the Department of Justice. Most recently I was the Vice President of Public Sector Security Solutions for RSA, the Security Division of EMC Corporation. I received my Bachelor of Science and Master of Science from Marymount University and a Master Certificate in Information Assurance from George Washington University. I was a Cyber Corps Scholar. In the nearly 30 years of my career to date as an IT professional I have been a programmer, systems developer, network engineer, program manager, and security professional.

Over the past 10 years the U.S. federal government has been struggling, learning, and discovering what to do about "cyber". We have been moving on a continuum that started with the discovery of adversaries in our networks, has found us struggling with how to manage our systems through the Federal Information Security and Management Act (FISMA) and compliance, how to identify threats, attacks, vulnerabilities and how to work together to defend our networks. As we move forward in a constantly evolving world of technology, life as we know it is changing rapidly. Soon, most companies, even government departments and agencies, will no longer have data centers or continue to own or manage their own email servers, applications, or desktops.

The use of virtualized IT infrastructure is the future. Virtualization, as the foundation of cloud computing infrastructure will enable the "Cloud" to be the provider of most IT services. You may say this is jumping ahead, but we must look at the answers to the questions you are asking with the near term future in mind, and the near term future is now – as many departments and agencies are already moving applications such as e-mail to the cloud, many are building private clouds, and many private sector companies are rapidly moving to the cloud. This is not only an innovative solution to a much needed technology refresh in the civil government space, but if done correctly, could be the answer to information sharing, infrastructure based defensive security, the cyber talent pool shortage and guaranteed life cycle management of our infrastructure resources. No longer will companies or departments and agencies with missions different than Information Technology need to be in the "IT" business. No longer will we need to educate the heads of these organizations and have them making IT risk decisions outside of the scope of their knowledge base. We will deliver the requirements to the vendors; the vendors will then supply the appropriate infrastructure and services, with security built right into the technologies and the offerings.

This brings us to a critical crossroads in the continuum of cybersecurity. Not only are we at the point where we realize the need for governance, leadership and cooperation between the government and private sector in order to have a chance at combating the adversaries in an efficient manner, but we also are now at the part of the continuum where the responsibility of protecting our assets processed on IT systems -- whether it is data or an operational function -- will be the responsibility of the private sector infrastructure providers. This point was driven home during the initial phases of the Comprehensive National Cybersecurity Initiative (CNCI) when the federal government realized just how much of the Internet is private sector owned and operated, and that even if we do better at securing federal systems, we can't improve our nation's cybersecurity posture without improvements in the private sector in partnership with industry.. As we continue to move infrastructure and services to the "cloud", effective and lasting partnerships with the private sector must be fully embraced and leveraged.

Understanding the Information Technology roadmap that we are all moving rapidly on also increases the importance of enhancing the governance, authorities, and relationships that the federal government has between and among the civilian departments and agencies, the homeland security and law enforcement communities, the defense and intelligence community and of course, the private sector.

As I move into the portion of my testimony where I will be identifying obstacles and problems I have encountered during my federal government service, there are a few caveats and points I would like to make clear. First of all, cyber is a new field. At most, we can say this is a 25-30 year old industry. We must understand this is going to take some time to mature. We will and have encountered issues, we will learn of new problems…but we must work together to overcome these challenges, quickly and effectively. Second, the Department of Homeland

Security (DHS) is a new Department and because of that it struggles with the fundamental daily functions of being a Department from procurement and budgets to hiring and operations. DHS is going to take some time to develop the processes, policies, and procedures needed to run smoothly and efficiently. It will not happen overnight and will not occur without specific actions and programs to improve the baseline operations. In addition, DHS has a very broad set of missions and duties. Cybersecurity often takes a back seat to physical threats and natural disasters in the daily and weekly grind of the Department. Congress should do more to enable the cybersecurity components in the Department to operate more effectively and independently without getting bogged down in other DHS mission spaces, allowing Cyber to effectively operate as an independent component; allowing Cyber to separate itself from the quagmire of internal politics and jostling for resources and mindshare. Third, there are a lot of really good people who have worked this problem in the past and are working on cybersecurity challenges today. As we point out the weaknesses and problems, we must be cautious of tying the hands of dedicated security professionals who are currently doing battle on a daily basis (unfortunately not just with adversaries in cyberspace, but with the bureaucracy within DHS). We cannot afford to forget these people. We need these qualified individuals in this young and growing field. They make sacrifices with their families, careers, and personal sanity to serve our country in trying to fix these problems. We should take the time to remember their service and take care not to diminish their contributions as we examine and address cybersecurity challenges in both the public and private sector.

During my tenure at US-CERT, we were at the very early stages of developing critical relationships with federal civilian departments and agencies as well as relationships with the homeland security, law enforcement, defense and intelligence communities and the private sector. It was clear there was a lack of governance and lack of authorities to carry out the poorly defined mission US-CERT set out to accomplish. To examine this problem it is critical to break down the US-CERT mission into 1) protecting the federal civilian departments and agencies, and 2) coordinating and collaborating with the private sector.

Governance over IT in the Federal space has been an issue for many years and to date has not been solved. FISMA, which was enacted in late 2002, was a start in attempting to set up roles and responsibilities, including defining the roles of federal CIOs and CISOs enabling security structures to be built in federal executive branch departments and agencies, as well as establishing reporting process for incidents to US-CERT. This all being said, there were overarching and important components of a success risk management strategy that have been missing. As it stands today, the only requirement a federal department or agency has is to report the incident to US-CERT in the dictated timeframe based upon incident categorization using a 20-year-old taxonomy that no longer describes the types of attacks that organizations are experiencing. This creates inaccurate metrics, and little to no real data on the actual attacks that are occurring in the federal civil space. US-CERT does not have the authority to require the

Departments or Agencies to share detailed information, or follow any specific instructions. Departments and Agencies interpret their reporting requirements differently and therefore each reports incidents using different definitions and methodologies. When I was the Director of US-CERT if we needed federal departments and agencies to follow specific instructions, we would have to have the Office of Management and Budget (OMB) require them to follow the instructions. Despite even OMB guidance, the cooperation from federal civilian agencies was consistently on the low end.

Because many of the existing IT systems are owned and operated by federal departments and agencies, there is no existing direct authority for DHS to require cooperation with US-CERT. This being said, it should also be understood that some of the departments and agencies have more sophisticated operations than US-CERT. The security operations centers at State Department, Department of Justice, the Federal Aviation Administration have a much higher technical monitoring and response capability than US-CERT. In order for US-CERT to accomplish the mission of protecting the federal civilian agencies and departments' day in and day out, US-CERT must be empowered and its capabilities must continue to be developed. It must have a clearly defined mission, authority and budget. It must have tools. These tools must be determined by what will support the mission, not be tied to legacy systems, management or contractors. This must be a collaborative mission between US-CERT and the departments and agencies. A "dictatorship" is not what is needed. Collaboration and cooperation will enable the road to success. Even more important is to clearly define US-CERT's role and the authorities the organization and Director carry. Developing a "council" of federal department and agency Security Operations Center Directors and the Director of US-CERT to help guide this mission makes sense in order to ensure the mission of US-CERT stays on track, serves its government customers, and has a focused and effective mission strategy.

Today US-CERT is buried too deep within DHS. To even confuse the issue more, US-CERT is a part of the National Cybersecurity and Communications Integration Center. Instead of integrating the NCC into US-CERT, yet another functional area has been opened, creating and compounding the confusion. US-CERT must be given autonomy to allow it to function as a successful operational entity – not laden in the political quagmire of DHS, NPPD, CS&C, NCSD. In my view, in order to be successful, US-CERT should be removed from the National Cybersecurity Division (NCSD) and treated as a component organization similar to FEMA. It should have its own budget that is not constantly diluted by other, projects, programs and internal politics in NPPD, CS&C and NCSD. US-CERT should have a clearly defined mission with attainable goals and the autonomy to succeed in this operational mission. Yes, operational. This is a roll up your sleeves and respond mission. This mission cannot be performed anywhere else in the federal civilian government…the White House cannot carry out an operational function, the DoD cannot perform an operational function of this nature domestically based on the Constitution, and no other department or agency has the overarching mission that allows for

both emergency response and homeland protection. DHS makes functional sense; US-CERT must be empowered to fulfill its operational mission. As it stands today, US-CERT is constantly caught up in political priorities and much time is spent thrashing around, attempting to service too many projects and stakeholders. A clear governance process in the federal space, a clearly defined mission and the authorities to support that mission, a budget to carry out this operational mission, as well as autonomy to operationally perform the operational duties are the steps to US-CERT having the capability to make a difference in supporting the departments and agencies as a part of DHS.

US-CERT's other mission is to coordinate and collaborate with the private sector – specifically with critical infrastructure owners and operators - is equally as important. Again, great mission, but rarely accomplished. The work is often clouded by poorly defined expectations and internal politics. USCERT has absolutely no authority within critical infrastructure that is owned or operated by the private sector - nor should it. The federal government has no claims or authority over privately held companies. Even in some of the current draft legislation in both the House and Senate, participation in government led cyber activities is by invitation only. Today's private-public partnership efforts are bogged down with the same rhetoric, politics and legal barriers of the past 20 years. I will say that presently USCERT does little of the coordination. This is done primarily through NCSD. Most of the communications is done by the CSCSWG (Cross Sector Cybersecurity Working Group, a working group of the ISACs) and most of the members are not actual security professionals running security organizations, but a confusing mix of IT and communications companies with individual company focused agendas and little or no focus on the operational agenda. An operational unit like US-CERT must be firewalled away from this kind of dysfunction to allow it to concentrate on the operation response mission.

The relationship between US-CERT and the private sector must be a focused and well defined mission. Prioritizing work with the infrastructure providers – not individual IT product vendors – such as ISPs, Web hosting and caching, cloud providers and IT infrastructure providers – to enable the focus on the operational response mission. I understand the entire private sector IT and communications sector wants to participate in future policy creation, but that function must not be mixed with the operational mission US-CERT must succeed in.

So far, I haven't painted a very pretty picture of what is going on at DHS in regards to cyber, but I want to re-iterate that I do believe DHS is the right place for cyber. I also believe changes need to be made in order for DHS to have a successful cyber mission. Giving US-CERT the autonomy to embrace a well defined operational response mission (both with the departments and agencies as well as with critical private sector players), with a budget and capabilities to execute on the mission, and authorities to enable them to execute on the mission is a very important step to success.

Creating a successful public/private partnership to help secure cyber space is yet another mission that must be addressed. I think we need to approach this problem from a different direction. We must not look at it as a "cyber space" problem. That mission space is far too broad. We must look at this problem in digestible pieces. Internet infrastructure: Internet Service Providers, Cloud Providers, Web Providers and Information Infrastructure Providers. Separate this from the "cyber war" issue, separate this from the policy and legislative issues. Move these layers away from the operational mission of US-CERT. Take on the protect the infrastructure problem first. Work on the information sharing problem with an operational lens. I truly believe a technical solution must come in order to break the stalemate we find ourselves in with regards to cooperation and information sharing. The stalemate is centered on procurement, legal, privacy and proprietary information issues. We must determine a technical function for anonymously exchanging information. In addition, we must start articulating the problem with the same vernacular. We must spend time redefining the taxonomy and vernacular we use to work the cyber problem. We must do this in order to establish meaningful metrics, solutions, and focused solutions to the problem.

The ancient category one through eight taxonomy, where 99% of all incidents are categorized as category three "malware" - is useless in the world of complex attacks and sophisticated adversaries. I do believe this will become easier as we move on our continuum to the cloud. I believe as it becomes a more defined industry and who actually runs the "IT infrastructures" (i.e. clouds) becomes more defined, information sharing will become better as a function of how many entities must actually participate in the defense of IT as a whole. It must be understood that a public private relationship is a two way street. Often the government is left holding the bag of failure when it comes to this relationship. The burden here is not and should not be solely on the government. We all have critical information that, if shared, would help the community as a whole. In the near future, the government will be squarely in the customer role as we move on the IT continuum to the Cloud. We must look at how the government and private sector can shape a healthy relationship. I am a firm believer that the private sector needs a private non-profit entity that would facilitate the relationships of the many privately held IT companies. This non-profit entity would facilitate the information sharing both on the private side as well as a focused conduit for information sharing with the government. I do not see this as an inherent government only role. I clearly understand there is a national defense role for the Government in times of war, but we need to clearly define what that means in terms of cyber, and yes that is clearly a DoD role – not a civil government role.

This being said, I do see technology developments that will remove the legal and privacy issues around information sharing. We must technologically come to a place where we can exchange information on a technical level about threats, attacks and mitigations without disclosing information about the entity or entities involved. We must focus as a community – not as a government - on moving this solution track along. We must be mindful of the circular rhetoric

trap we get caught in when we hear the words – public private partnership – and realize the actual work that needs to happen to accomplish the goal – defending our IT assets and missions. The work that needs to be done is to create technical processes, overcome procurement and legal issues. This must be done as a community, lead by the private sector. The government's participation should be as a member of the community.

In conclusion, I do believe DHS has a primary role in cyber. Though I have not always thought DHS could handle the important mission because of its maturation level, I do believe the operational mission of US-CERT belongs in DHS – but as an autonomous operational component with direct reporting capabilities to the Secretary. I believe the mission of US-CERT must be more clearly defined to enable it to be successful. The appropriate authorities must be given to US-CERT to allow it to function. Public/private partnerships need to be rescued from the circling drain of rhetoric and lead by the private sector with Government participation.

We are moving rapidly to a new world – we must clear our plates of the static yada yada of stale circular discussions, identify the operational function and technical solutions. Empower US-CERT to succeed. Empower the private sector to lead. Empower the Government to participate.

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