Remarks of Cybersecurity and Communications Assistant Secretary Greg Garcia at the National Cyber Security Awareness Month Kick-Off Summit

Release Date: October 1, 2007

Washington, D.C.
(Remarks as prepared)

Thank you Ron for that warm introduction. On behalf of Homeland Security Secretary Michael Chertoff, I would like to welcome you all to this important summit. It is wonderful to see such a tremendous turnout for this event.

And thank you Chairman Majoras for your inspiring remarks. Not only do I admire the FTC's efforts to educate all Americans on the important issue of identity theft, I appreciate the proactive measures your agency has taken to enhance the security of its own networks.

DHS and FTC are working together to address this formidable cyber security challenge. As the lead Federal Government agencies for consumer protection and infrastructure protection, we have learned that individual and enterprise cyber security are really two sides of the same coin. Without one, it's not possible to have the other.

In 2005, our partnership led to the launch of www.OnGuardOnline.gov, which has become the leading government site for consumer education on the issue of Internet fraud.

It provides clear, actionable tips on how to conduct secure online shopping and keeps people from falling victim to phishing scams, which continue to be the number-one cyber incident reported to us at DHS.

The site is a model for government and industry collaboration and leverages the collective expertise of not only the FTC and DHS, but the Department of Commerce, U.S. Postal Inspection Service, Office of Justice Programs, the Securities and Exchange Commission, and the National Cyber Security Alliance.

Our agencies have also joined forces on the President's Identity Theft Task Force and, under your leadership as Co-Chairman of that effort; we have charted a path toward improving all aspects of the identity theft continuum, including awareness, prevention, detection, and prosecution.

When Chairman Majoras and I met earlier this year, we discussed ways that our agencies can further our partnership and continue to enhance the Nation's overall cyber security posture.

I am pleased to say that meeting is already yielding fruit with this summit and that today's agenda reflects the complementary roles our respective agencies play in consumer and infrastructure protection. So I look forward to our continued collaboration.

Four years ago, DHS, in partnership with its public and private partners, launched the first National Cyber Security Awareness Month in this very room. I am told there were only about 25 people in attendance and just two members of the press, one of whom was from a local university paper.

Look at how far we've come. What started as an idea is now a national movement. This month, we are uniting with our partners all across the nation to change attitudes about cyber security and get results.

There's a lot going on. During this month we will:

Co-host the Software Assurance Forum with the Department of Defense. This is to collaborate with software developers to build increased security measures into their programs before they are acquired and deployed; coordinate a cyber security education effort at the state level in partnership with the multi-state information security and analysis center; and release a draft of the IT Essential Body of Knowledge for public comment. This will provide guidance about the skills and expertise our IT security professionals need to meet the cyber security challenges that exist today and in the future.

And that's just the start.

This month marks not only the 4th Annual Cyber Security Awareness Month, but in fact the one-year anniversary since I took office as the Nation's First Assistant Secretary of Cybersecurity and Communications.

Soon after I took office, I outlined three priorities to guide the direction of my organization: strengthen Federal systems; develop a national preparedness and deterrence strategy; and, enhance our operational cyber response capabilities.

Together with our public and private sector partners, I believe we have made great progress in each of these areas. We only have the room until 5 p.m. so I'll quickly mention just three of these accomplishments now.

First, the national cyber exercise program.

This past year, we began actively planning for the March 2008 National Cyber Exercise, or cyber storm II, which follows the highly successful cyber storm I held in February 2006. DHS is the sponsor of the Cyber Storm exercises, which examine response and coordination mechanisms against a simulated cyber event affecting international, Federal, State, and local governments, and the private sector.

I believe you play how you train. By performing an exercise such as Cyber Storm, DHS is able to test our planning, information sharing and response to attack scenarios, assess our strengths and weaknesses in those areas, and learn how to do it better. In short, as Jack La Lanne said, exercising makes you stronger.

Second, training future it security professionals.

DHS is actively enhancing the professional development of the Nation's IT security workforce through its collegiate programs. This year, 12 centers of academic excellence in information assurance education were added in 11 states. This joint program between the National Security Agency and DHS/NCSD is now educating students for careers in it security at 86 centers in 34 states and the District of Columbia.

The second annual national collegiate cyber defense competition, sponsored by my National Cyber Security Division, involved 44 schools – up from five original schools – and capped a series of state and regional cyber security competitions. This effort continues to expand.

And third, building a national preparedness and deterrence strategy.

Last spring, we established the Cross-Sector Cyber Security Working Group (CSCSWG) to address cross sector cyber risk and explore interdependencies. The working group serves as a forum to bring government and the private sector together to address common cyber security elements across the 17 critical infrastructure and key resource sectors.

Yet in spite of our best efforts cyberspace is far from secure.

The developments we have made in strengthening Federal systems, developing a preparedness and deterrence strategy, and enhancing our operational cyber response capabilities have been aggressive, but our work has just begun. It's an evolutionary process.

What is the threat?

We're in a time of increasing global threats to our cyber infrastructures and to the services, systems, and assets that depend on them. While these at-risk-systems are vast, they easily fade into the background of everyday life. The local ATM, the overhead lights, and the water faucets are all dependant on larger, more comprehensive systems controlled by it networks.

An exploited vulnerability in one of these it control systems could range from the annoying to the catastrophic. Our adversaries would like nothing more than to gain control of our financial markets, power generation plants, water purification facilities, or transportation systems. That's why, here in our Nation's capital, as in any American city, cyber vulnerabilities can have real world consequences.

Botnets, phishing, ad-ware, spyware and other attacks make up the more-than-$100 billion global market for cyber-crime –¬ surpassing drug trafficking from a monetary perspective. Worst of all, the money obtained through cyber crime can be used to finance terrorism. The threats are real. Hackers are becoming more sophisticated and focused in their efforts. Cyber crime is big business; cyber espionage is on the rise.

The numbers say it all. From October 1, 2006, through last weekend, our US-CERT—which I'll describe in more detail in a moment – handled 37,006 incidents, compared with 23,993 the year before. This increase can be attributed to not only increased attacks on our public and private networks, but also increased situational awareness levels and reporting rates.

These numbers won't get any smaller without the same level of organization and coordination that our adversaries are using against us. This dynamic underscores the absolute necessity for IT security and the importance of a nationwide call to secure American cyberspace this October. It's something we can't afford not to do.

Our mission is clear. Securing the systems that maintain and operate critical infrastructures is vital to national security, public safety, and economic prosperity.

How will we do this? We know the Federal Government alone cannot address the cyber threats posed to our critical infrastructures because over 85 percent of critical infrastructures in the United States are owned and operated by private industry. Obviously, the immediate victims of cyber attacks also will be in private industry.

So the solution must rely not just on government, but on industry and academia coming together with government to successfully address the cyber threats posed to our critical infrastructures.

So let's start with a brief discussion of each of these priorities.

First -- securing Federal systems. Expansion of Einstein program

Situational awareness, in cyberspace or the physical world, is a critical component in how we deter crime and terrorism, and catch criminals and terrorists. Without it, we're an easy target.

We know from our friends in law enforcement that situational awareness is the primary method a cop on the beat uses to protect his or her neighborhood. A veteran officer deters crime and catches criminals by understanding their environment, watching for trends and patterns, and knowing the rhythms of the community.

We know the same is true for cyber first responders. So we created an early warning system that watches for malicious patterns in network traffic and notes irregular activity. Just as in neighborhood policing, out-of-the-ordinary events or activities could tip off agency cyber responders to potential trouble.

Einstein, as it is known, is that early warning system. It supports Federal agencies' efforts to protect their computer networks. Including the FTC, 13 Federal Government agencies participate in this program, with plans to expand Einstein to all Federal Cabinet agencies.

Einstein monitors participating agencies' network gateways for traffic patterns that indicate the presence of computer worms or other unwanted traffic.

By collecting traffic information at agency gateways, Einstein gives government analysts and participating agencies a big-picture view, synthesized of potentially malicious activity across Federal networks.

Einstein helps identify configuration problems, unauthorized network traffic, network backdoors, routing anomalies, network scanning activities, and baseline network traffic patterns.

It enables rapid detection of cyber attacks affecting agencies and provides Federal agencies with early incident detection.

Here's the measurable value-add: Einstein has reduced the time it takes the United States Computer Emergency Readiness Team (US-CERT) to gather and share critical data on computer security risks from 4 to 5 days to 4 to 5 hours.

Second priority – formulation and implementation of sector specific plans. Building a comprehensive risk management framework

Whether you are a business leader, civil servant or head of household, you often have to make tough choices with limited resources.

Now, I'm not talking about eliminating risk. At DHS, we determine our priorities based on a risk management

framework that allows us to focus our resources on those areas that pose high risks and face high consequences.

Experts from Federal, State, and local government, industry, and academia, including some here in this room today, have all made significant contributions to our risk management approach, and, as a result, we're strengthening America's homeland security every day.

The underlying foundation for our risk management approach is called the national infrastructure protection plan (NIPP). If you're not familiar with the NIPP, it provides a singular, unifying structure for the integration of a wide range of efforts to protect our critical infrastructure and key resources.

It was developed in collaboration with industry representatives from all 17 unique critical infrastructure sectors, working through the component "sector specific plans" which were released last May. These individual plans were put forward – and are now being implemented by – the communications sector, financial services, energy, water, transportation, chemical and many others. And I applaud them all for their commitment to strengthening their respective infrastructures, including their cyber networks.

These plans demonstrate how true public/private collaboration allows each of us to share our knowledge and build the strongest security foundation possible for all our critical infrastructures and key resources.

And third – enhancing cyber response operational capabilities. We all agree information sharing among the different sectors and stakeholders is essential to strong cyber defense and response capabilities.

That's why we established US-CERT, the United States Computer Emergency Readiness Team, back in 2003.

As the Nation's cyber watch and warning center, US-CERT coordinates the defense against and response to cyber attacks in conjunction with the private sector. It also analyzes and reduces cyber threats and vulnerabilities, disseminates cyber threat warning information, and manages incident response activities with a wide range of stakeholders.

One of US-CERT's most important roles is sharing potential and real cyber threat information with its partners. This allows us to see potential trends and develop appropriate prevention and response activities.

With the convergence of the IT and communications sectors, we need to ensure synchronized information sharing and response capabilities across our communications and cyber networks, precisely because those networks are becoming one and the same.

That's why I plan to further enhance US-CERT's information sharing activities by co-locating it with the National Coordinating Center (NCC), the operational arm of the National Communications System (NCS), which ensures that we have available and resilient communications during a national disaster.

In time, I would like to see key representatives beyond IT and communications, such as financial services, energy and power, transportation, etc, along with state and federal bodies, even more actively integrated in this information sharing and operational environment.

Here are a couple of examples of the value the US-CERT has provided just this year to our stakeholders.

US-CERT provided incident response assistance and analytical training to the Estonian government following widespread cyber attacks targeting the country's information technology infrastructure.

US-CERT provided on-site cyber incident response assistance to a half-dozen Federal agencies.

It also collaborated with the Multi-State Information Sharing and Analysis Center for dissemination of critical cyber security information, tools, and resources to all 50 States and the District of Columbia.

But despite the growing impact of such efforts, the exponential growth in cyber security incidents is likely to continue. Why? Opportunity. Where there's opportunity, there will be danger. Knowing cyber security will forever be a part of the Internet, we have to be that much more vigilant.

Just these numbers illustrate the problem. Of the nearly 63,000 cyber incidents reported to US-CERT over the last three years, nearly 4,000 were policy violations, more than 4,600 malware findings, and a staggering number of nearly 42,000 were phishing attempts. The significance is that no matter what form the attacks take,

they continue to come. We must meet these incidents with preparation and resolve.

Our task to secure our systems has no simple solution and no foreseeable end.

Regardless of the threat, whether the latest scam or virus, cyberspace will continue to suffer from the incurable disease of criminal intent, which will only be encouraged by our complacency. We as a Nation must inoculate ourselves with every keystroke.

To keep our cyberspace secure, we need every individual and enterprise user – every man, woman and child using networked technology – to take personal responsibility for securing their part of cyberspace.

Not all Americans can write computer code but each of us can take reasonable precautions with our technology.

You don't need to know how to build an engine to safely drive a car.

While we may not be able to cure the disease, we can: Deny our adversaries targets of opportunity; Build systems that are extraordinarily difficult to exploit; and Extract a high cost, so attacks are prohibitively expensive and detection assured.

We've got to make the United States the most dangerous place in the real world for cyber criminals to do business.

The stakes could not be higher.

The front lines in the struggle to secure our future will be fought from: Millions of hand-held portable networked devices; From every home, classroom and office; And from the vast array of infrastructures, factories, and worksites interconnected to the online world.

From each of these virtual addresses our personal security and national defense will hang in the balance. Our Nation will be only as strong as our individual dedication and perseverance. We all have to share in the burden, because we all depend on shared critical infrastructures and systems to maintain our national security, fuel our economy, and support our way of life.

Cyberspace reflects the beauty and genius of the open societies that created the online world and allowed it to flourish. Protecting cyberspace without changing its spirit of openness will challenge us all. We have to balance the temptation to sacrifice the best of cyberspace in the name of precaution with the urgent need to share our great experiment – the digital democracy – with the rest of the world.

I have three requests for each of you here today.

Take cyber risks seriously and ask your neighbors and coworkers to do the same. Think of the famous utterance by the character Howard Beale in the 1976 movie Network.... "I am mad as hell and I'm not going to take it anymore."

Educate yourself on ways to safeguard you and your family from identity theft, fraud and other cyber threats at www.OnGuardOnline.gov and at StaySafeOnline.org

Spread the word and become an ambassador of cyber security. At work, ask your IT security specialists to report any potential cyber incident, threat, or attack to the United States Computer Emergency Readiness Team (US-CERT) at 1-888-282-0870 or www.US-CERT.gov. We're open 24 hours a day, seven days a week.

Finally, help explain the importance of protecting yourself online to those around you.

It’s a complex problem, yes, but the dangers are easily understood, and the solution is simple: you can't guard all of cyberspace, but you can take care of your piece of it. Thank you.

###

This page was last modified on October 1, 2007