Remarks as Prepared for Delivery by Assistant to the President for Homeland Security and
Good afternoon, everyone. Thank you, Jane, for your kind words, for your leadership on national security, and to everyone here at the Wilson Center for hosting me today. Some of you may not know this, but my very first job in Washington, I’m afraid to admit nearly 25 years ago, was working as a research assistant at the Wilson Quarterly—back when it was a quarterly, paper journal. Now, like everything else in our world, the Wilson Quarterly is online and much more up-to-the-minute. So today feels a bit like coming home.

Before I get to my main subject today, I’d like to say a few words about the terrible news of this morning. With deep sadness, we have confirmed the death of Kayla Mueller, who had been held hostage by ISIL for more than a year. Today, our hearts go out to her family, and my thoughts in particular are with her parents, Carl and Marsha Mueller, who have shown strength and dignity over many difficult months. Kayla represented the best of us—she was a testament to the boundless human spirit, and her legacy of compassion will serve as an inspiration to all those who seek to make our world a more just place. Her life reaffirms a clear truth: that a hateful and barbarous terrorist group like ISIL will never overcome the basic decency and hope that dwells in the human heart. And, as the President made clear, we will find and bring to justice the terrorists who are responsible for Kayla’s captivity and death—no matter how long it takes.

As President Obama’s Homeland Security and Counterterrorism Advisor, I brief him every morning on the most significant, destructive, and horrific threats facing the American people. I am oftentimes, as the President reminds me, the “bearer of bad news.” Since I began this job two years ago, I can tell you that an increasing share of the bad news I deliver is unfortunately on cyber threats. In just the last nine months, we’ve seen a growing list of high profile targets—Home Depot, JPMorgan Chase, Target, Sony Pictures, CENTCOM, and the U.S. Postal Service, to name a few.

We are at a transformational moment in the evolution of the cyber threat. The actions we take today
and those we fail to take – will determine whether cyberspace remains a great national asset or increasingly becomes a strategic liability. An economic and national security strength, or a source of vulnerability.

So today, I want to talk about the threat we face and the Administration’s approach to countering it, drawing on counterterrorism lessons learned from the last decade of war.

Let me start with the facts. According to a recent U.S. Government assessment, cyber threats to our national and economic security are increasing in their frequency, scale, sophistication, and severity of impact. The range of cyber threat actors, methods of attack, targeted systems, and victims are expanding at an unprecedented clip.

The pace of cyber intrusions has also ticked up substantially—annual reports of data breaches have increased roughly five-fold since 2009. And the seriousness of those breaches is also rising, causing significant economic damage.

No one, it seems, is immune – from healthcare companies and universities to the tech industry, critical infrastructure, and entertainment sector. Just last week, Anthem, one of the nation’s largest health insurance providers, announced that hackers had breached a database containing the personal information of 80 million customers and employees. Inside the U.S. government, we know that state and non-state actors, terrorists, hackers, and criminals are probing our networks every day – seeking to steal, spy, manipulate, and destroy data.

At the state level, threats come from nations with highly sophisticated cyber programs, including China and Russia, and nations with less technical capacity but greater disruptive intent, like Iran and North Korea. Several nations regularly conduct cyber economic espionage for the commercial gain of their companies. And politically motivated attacks are a growing reality, as we saw with North Korea’s attack on South Korean banks and media outlets last year.

As for non-state actors, threats are increasingly originating from profit-motivated criminals—so-called hackers for hire—those who steal your information and sell it to the highest bidder online. Transnational criminals use cyber as a vector for profit. There are the ideologically motivated hackers or terrorists. You have groups like Anonymous that thrive on creating disruptions on company’s websites and leaking personal information online. You have groups like the so-called Syrian Electronic Army, which conducts cyber attacks in support of the brutal regime in Syria.

And then there is ISIL, which has harnessed social media for a propaganda machine that’s radicalizing and recruiting young people to their hateful message around the world.

Most concerning, perhaps, is the increasingly destructive and malicious nature of cyber attacks, as
we saw with Sony Pictures Entertainment last fall. This attack stole large amounts of data and rendered inoperable thousands of Sony's computers and servers. It was a game changer because it wasn’t about profit—it was about a dictator trying to impose censorship and prevent the exercise of free expression. At bottom, it was about coercion, which the United States believes is unacceptable, and which is why we took the extraordinary step of publicly identifying North Korea as responsible for the attack and responded swiftly, imposing additional sanctions on Kim Jong-Un’s regime.

In short, the threat is becoming more diverse, more sophisticated, and more dangerous.

And I worry that malicious attacks like the one on Sony Pictures will increasingly become the norm unless we adapt quickly and take a comprehensive approach, just as we have in other contexts. Which brings me to the counterterrorism model.

Now, to be sure, there are many differences that make it difficult to apply lessons learned from the counterterrorism experience to cyber. For one, the private sector plays a more central role in spotting and responding to cyber incidents than they do in the counterterrorism realm, where the government largely takes the lead.

Having observed our Nation’s response to terrorism post 9/11 from three different perches in the U.S. government—at the FBI, as Assistant Attorney General for National Security at the Department of Justice, and now at the White House—I can tell you there are structural, organizational, and cultural shifts that were made in our government in the counterterrorism realm that also apply to cyber. We need to develop the same muscle memory in the government response to cyber threats as we have for terrorist incidents.

Structurally, since 9/11 our government has done the hard work of breaking down walls in our counterterrorism agencies and bringing people together to share information so that we get the best possible assessment of the threat. Whenever possible, we’re bringing partners together to share information and extend our operational reach. This model has made our counterterrorism mission against an evolving enemy more effective and sustainable.

Like counterterrorism, meeting cyber threats requires a whole-of-government approach that uses all the appropriate tools available to us—including our global diplomacy, our economic clout, our intelligence resources, our law enforcement expertise, our competitive technological edge, and, when necessary, our military capability. Those who would harm us should know that they can be found and will be held to account.

In the cyber context, we need to share threat information more broadly and coordinate our actions so that we’re all working to achieve the same goal—and we have to do so consistent with our fundamental values and in a manner that includes appropriate protections for privacy and civil
liberties. We need to sync up our intelligence with our operations and respond quickly to threats against our citizens, our companies, and our Nation.

Make no mistake. Over the last few years, we have developed new and better ways to collaborate across all levels of government and with our partners in the private sector—including at the operational hubs in our government charged with monitoring threats, issuing warnings, sharing information, and protecting America’s critical infrastructure.

At the White House, we’ve taken steps to improve our policy response. Last summer, following a rising number of breaches and intrusions to public and private networks, we created the Cyber Response Group, or CRG—modeled on the highly effective and long-standing Counterterrorism Security Group. The CRG convenes the interagency and pools knowledge about ongoing threats and attacks and coordinates all elements of our government’s response at the highest levels.

Despite this progress, it has become clear that we can do more as a government to quickly consolidate, analyze, and provide assessments on fast-moving threats or attacks. As President Obama said during the State of the Union last month, we will make “sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism.”

So today, I’m pleased to announce that we will establish a new Cyber Threat Intelligence Integration Center, or CTIIC, under the auspices of the Director of National Intelligence. Currently, no single government entity is responsible for producing coordinated cyber threat assessments, ensuring that information is shared rapidly among existing Cyber Centers and other elements within the government, and supporting the work of operators and policy makers with timely intelligence about the latest cyber threats and threat actors. The CTIIC is intended to fill these gaps.

In this vein, CTIIC will serve a similar function for cyber as the National Counterterrorism Center does for terrorism—integrating intelligence about cyber threats; providing all-source analysis to policymakers and operators; and supporting the work of the existing Federal government Cyber Centers, network defenders, and local law enforcement communities. The CTIIC will not collect intelligence—it will analyze and integrate information already collected under existing authorities.

Nor will it perform functions already assigned to other Centers. It is intended to enable them to do their jobs more effectively, and as a result, make the Federal government more effective as a whole in responding to cyber threats. CTIIC will draw on the existing Cyber Centers to better integrate their relevant expertise and information to improve our collective response to threats.

Of course, responding to today’s threat is only part of the task. The real challenge is getting ahead of where the threat is trending. That’s why the President’s National Security Strategy identifies cyber as a critical focus area to ensure we both meet the challenges of today and prepare for the threats we
will face tomorrow. The President’s new budget backs up this commitment with $14 billion to protect
our critical infrastructure, government networks, and other systems.

And later this week, at Stanford University, President Obama and I and several Cabinet members will
join hundreds of experts, academics, and private sector representatives for a first-of-its-kind summit
to discuss how we can improve trust, enhance cooperation, and strengthen America’s online
consumer protections and cyber defenses.

But to truly safeguard Americans online and enhance the security of what has become a vast cyber
ecosystem, we are going to have to work in lock-step with the private sector.

The private sector cannot and should not rely on the government to solve all of its cybersecurity
problems. At the same time, I want to emphasize that the government won’t leave the private sector
to fend for itself. Partnership is a precondition of success—there’s no other way to tackle such a
complicated problem. It requires daily collaboration to identify and analyze threats, address
vulnerabilities, and then work together to respond jointly.

To the private sector, we’ve made it clear that we will work together. We’re not going to bottle up our
intelligence—if we have information about a significant threat to a business, we’re going to do our
utmost to share it. In fact, within 24 hours of learning about the Sony Pictures Entertainment attack,
the U.S. government pushed out information and malware signatures to the private sector to update
their cyber defenses. We want this flow of information to go both ways.

The private sector has vital information we don’t always see unless they share it with us, and the
government has a unique capacity to integrate information about threats, including non-cyber
sources, to create the best possible picture to secure all of our networks.

When companies share information with us about a major cyber intrusion or a potentially
debilitating denial of service attack, they can expect us to respond quickly. We will provide as much
information as we can about the threat to assist companies in protecting their networks and critical
information. We will coordinate a quick and unified response from government experts, including at
DHS and the FBI. We will look to determine who the actor is and hold them to account. And, as we
respond to attacks, we will bring to bear all of the tools available to us and draw on the full range of
government resources to disrupt threats.

I want to commend companies that have shown strong leadership by coming forward as soon as they
identify breaches and seeking assistance so we can work together and address threats more rapidly
—which is good for the company, good for the consumer, and good for the government. Across the
board, we’re tearing down silos, increasing communication, and developing the flexibility and agility
to respond to cyber threats of the 21st century, just as we have done in the counterterrorism world.
Moving forward, as our lives become more and more dependent on the Internet, and the amount of territory we have to defend keeps expanding, our strategy will focus on four key elements.

First, we need to improve our defenses—employing better basic preventative cybersecurity, like the steps outlined in the Cybersecurity Framework announced last year, would enable every organization to manage cyber risk more effectively. But even just employing basic cyber hygiene could stop a large percentage of the intrusions we face, so we’ve got to start by getting the basics rights.

Second, we need to improve our ability to disrupt, respond to, and recover from cyber threats. That means using the full strength of the United States government—not just our cyber tools—to raise the costs for bad actors and deter malicious actions.

Third, we need to enhance international cooperation, including between our law enforcement agencies, so that when criminals anywhere in the world target innocent users online, we can hold them accountable—just as we do when people commit crimes in the physical world.

And fourth, we need to make cyberspace intrinsically more secure—replacing passwords with more secure technologies, building more resilient networks, and enhancing consumer protections online, to start with.

President Obama will continue to do everything within his authority to harden our cyber defenses, but executive actions alone will not be enough. We need durable, long-term solutions, codified in law that bolster the Nation’s cyber defenses. This is not, and should not, be a partisan issue. The future security of the United States depends on a strong, bipartisan consensus that responds to a growing national security concern. Everyone shares responsibility here, including the Congress.

In December, Congress passed important bills to modernize how the government protects its systems and to clarify the government’s authorities to carry out its cyber missions. Today, we need the Congress to build on that progress by passing the package of cybersecurity measures that President Obama announced last month that encourage greater information sharing, set a national standard for companies to report data breaches, and provide law enforcement with updated tools to combat cybercrime. And we look to Congress to pass a budget with critical funding for cybersecurity, including for DHS. The Administration is ready to work with Congress to pass these measures as quickly as possible.

Cybersecurity is and will remain a defining challenge of the 21st century. With more than three billion internet users around the world and as many as ten billion internet-connected devices, there’s no putting this genie back in the bottle. We have to get this right. Our prosperity and security depend upon the Internet being secure against threats; reliable in our ability to access information; open to all who seek to harness the opportunities of the Internet age; and interoperable to ensure the free
flow of information across networks and nations.

But we are at a crossroads, and the clock is ticking. The choices we make today will define the threat environment we face tomorrow.

All of us have a responsibility to act—to take preventative measures to defend our systems; to build greater resilience into our networks to bounce back from attacks; to break down silos and improve information sharing and the integration and analysis of threats; to pass cybersecurity legislation; and to ensure we take a comprehensive, whole-of-government approach to respond to cyber attacks, just as we do in other contexts.

These are hard and complicated issues. But I’m confident that working together—government, industry, advocacy groups, the public, and Congress—our networks will be safer, our privacy protected, and our future more secure. I look forward to tackling these threats with all of you. Thanks very much.