the nominations, and any statements related to the nominations be printed in the RECORD; that the President be immediately notified of the Senate's action and the Senate then resume legislative session; further, that following this vote, the Senate resume consideration of the EDA bill and vote on the motion to invoke cloture on that bill; that if cloture is not invoked, the Senate proceed to vote to invoke cloture on the motion to proceed to S. 679, the Presidential Appointment Efficiency and Streamlining Act; finally, that the mandatory quorum under rule XXII be waived on both cloture motions.

The PRESIDING OFFICER. Without objection, it is so ordered.

MORNING BUSINESS

Mr. REID. Mr. President, I ask unanimous consent that we now proceed to a period of morning business, with Senators allowed to speak for up to 10 minutes each.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from Rhode Island.

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent that I be allowed to speak for up to 17 minutes.

The PRESIDING OFFICER. Without objection, it is so ordered.

CYBERSECURITY

Mr. WHITEHOUSE. Mr. President, I rise today to speak about a serious issue that touches on our national security, our economic well-being, the safety of our families, and our privacy; that is, America's cybersecurity.

I look forward to conducting an in-depth examination of the aspects of this issue that falls within the Senate Judiciary Committee's jurisdiction during the Subcommittee on Crime and Terrorism's June 21, 2011, hearing, ''Cybersecurity: Evaluating the Administration's Proposals.'' However, because of the importance of improving our cybersecurity, as demonstrated by the recent Gmail spear-fishing attacks and hacks at Sony, Epsilon, Lockheed Martin, and even the Senate itself, I rise to make some initial remarks today.

American technological innovation ushered in the Internet age, bringing with it Facebook, YouTube, and the rest of the World Wide Web. It set off an explosion of new commerce, freedom of expression, and economic opportunity even in the smallest details of our lives—allowing a car company, for instance, to unlock your car doors remotely if you have locked yourself out of your car.

However, this increased connectivity allows criminals, terrorists, and hostile nations to exploit cyberspace, to attack America, to invade our privacy, to loot our intellectual property, and to expose America's core critical infrastructure to cyber sabotage. Entire online communities are dedicated to stealing and selling American credit card numbers. Consider the disturbing fact that the price of your credit card number stolen online actually goes up if the criminal also is selling your mother's maiden name. Some criminals have learned how to spy on Americans, hacking into our home computers and looking out through the video camera attached to the screen. Others run Web sites selling stolen entertainment without paying the American companies that created it. And millions of American computers—millions of American computers—have been compromised by malware slaved to botnets that can record your every keystroke and send it instantaneously across the world to a criminal's laptop.

I firmly believe that cyber crime has put our country on the losing end of the largest illicit transfer of wealth in world history. Whether by copying source code, by industrial espionage of military product designs, by identity theft, by online piracy, or by outright old-fashioned stealing from banks—just doing it the electronic way—cyber crime cripples American innovation, kills jobs here at home, and undermines our economic and national security.

Congress must act to protect Americans from these Internet dangers and to protect our civil liberties. Let me say at the outset that the government must not be allowed to snoop indiscriminately into our online activity, to read our e-mail, or to watch us online. There simply is no need for such an invasion of privacy, and we must move forward with that firmly in mind.

The majority leader has introduced a leadership bill that will be a vehicle for our work. The Commerce Committee, led by Chairman ROCKEFELLER and Ranking Member SNOWE, both of whom I had the privilege to serve with on the Intelligence Committee, and the Homeland Security Committee, led by Chairman LIEBERMAN and Ranking Member COLLINS, reported key bills last year. Chairman LEAHY and the Judiciary Committee have reported important legislation on data breach and other issues central to cybersecurity. The Armed Services, Energy, and other committees have studied the issue from the perspective of their particular jurisdictions and expertise, and under the leadership of Chairman FEINSTEIN, the Intelligence Committee Cybersecurity Task Force completed its classified report last July, authored by me, Senator MIKULSKI, and Senator SNOWE. So we have been ready in Congress.

The administration has now weighed in with its own proposal, recognizing that we need cybersecurity legislation to make our Nation safer and launching in earnest our legislative process.

We have hard work ahead to find the best possible solutions to this complex and grave challenge to our national and economic security. As we begin, I would like to flag five issues that I believe must be addressed as this legislation goes forward.

First, we need to build greater public awareness of cybersecurity threats going forward.

What is the problem? The problem is that information affecting the dot.gov and the dot.mil domains—the government domains—is largely classified. And in the dot.com, dot.net, and dot.org domains, threat information is often kept proprietary by the victim business so as not to worry shareholders, customers, and regulators, or give ammunition to competitors. The result is that Americans are left in the dark about the level of danger that is actually out there on the Internet.

The administration's proposal would require covered businesses to notify customers if their personal information is stolen, expand reporting of cybersecurity threats, and require some public assessments of cyber readiness.

I believe more can still be done on these fronts. I have had the pleasure of working with Senator KYL to introduce S. 931, the Cyber Security Public Awareness Act. I would like to urge interested colleagues to review it and consider including it as part of our larger cybersecurity legislation. That is first.

Second, the Senate needs to ensure that we give private industry the tools necessary for self-defense against cyber attacks.

Proper sharing among and within industries of cybersecurity threat information is vital. The administration took an important step by recommending, subject to various safeguards, enhanced sharing of cybersecurity threat information by the government with private industry. But we may also need to remove legal impediments that unnecessarily limit the sharing of threat information within industries, and we should be prepared to listen here to the private sector's needs as they set up those areas for safe communications about the cyber threats they share.

Third, our Nation does not have basic rules of the road for end users, ISPs, and software and hardware suppliers.

The administration proposal includes important provisions that would move us in the right direction. Assuming that ISPs—Verizon and Comcast and the companies that are actually providing the service—assuming that these companies qualify as critical infrastructure, which is an assumption we should clarify before getting too far down this path, the administration's proposal would require them to develop a standardized framework to address cybersecurity.

Sensible laws and regulations have made our highways safe, and we need similarly to make our information highways safe. Federal procurement can encourage effective cybersecurity standards with appropriate supply chain security so as to improve cybersecurity across the hardware and software industries. These improvements will benefit the government directly, but it will also improve the security of all products on which business and consumers rely.

Americans are too often unaware of dangerous malware that has been surreptitiously inserted into our own computers, and we do not take readily available measures to protect ourselves and those with whom we link.

One leading ISP, Comcast, deserves credit for developing a new mechanism to notify and assist its customers when their computers have been compromised by malicious software or botnets. All other ISPs should work together to join, strengthen, and standardize this program. In Australia, ISPs have developed a code of conduct that may be a model for their American counterparts in this regard.

The fourth point: It is vital that the government have an instant response plan that clearly allocates responsibilities for responding to a major cyber attack or breach. The administration proposal puts the responsibility for such incident response with the Department of Homeland Security Cybersecurity Center envisioned by the proposal. I look forward to working with the administration and my colleagues on that aspect of the proposal.

More generally, the administration proposal, like bills that have been reported in the Senate, gives the Department of Homeland Security a leadership role in our Nation's cybersecurity. We have to remember this is a relatively new role for the Department of Homeland Security. It is one of a great many different responsibilities that the Department of Homeland Security bears, and it is a role in which much of the government's expertise resides in other agencies than the Department of Homeland Security.

The Department of Homeland Security's role must be configured to attract sufficiently high-caliber cybersecurity professionals to ensure that DHS properly leverages the cybersecurity expertise at those other agencies and to assure sufficient independence and credibility of the Cybersecurity Center to perform this vital mission, even as administration change and attention to cybersecurity waxes and wanes. Cybersecurity is a real and present danger, so we must also plan for and minimize the interim period in which DHS builds up its cybersecurity expertise, promulgates necessary regulations, and otherwise grows into any new role with which it is tasked.

Cyber attacks happen at the speed of light, so the best defense requires that we preposition some of our defensive capabilities. Many of our Nation's leading experts who have seen the dark heart of the Internet's dangers and understand the cyber threat in its dimensions recommend rapidly creating secure domains for our most critical infrastructure—our electric grid being the most obvious example. These would be domains in which our Nation's best cybersecurity defenses could be both lawful and effective. Obviously, this would need to be done in a very transparent manner, subject to strict oversight. But we as a country have impressive capabilities in this area, and we need to make sure those impressive capabilities protect our critical infrastructure as soon as possible. They are not deployed to protect critical infrastructure now.

Fifth, countries around the world, including countries that dedicate significant resources to exploiting our cyber vulnerabilities, are working hard to build their cyber workforces. We must not fall behind.

This means enabling our colleges and universities, in partnership with private companies, government agencies, and other cybersecurity innovators, to research the next great cybersecurity technology and to build the cyber human capital our Nation needs to defend itself and continue to flourish on the Internet.

Academic and technological leaders in my State, such as the University of Rhode Island and Brown University, have been hard at work developing new cybersecurity technologies and strengthening our Nation's cyber expertise. I look forward to working with them as we go forward.

There are other vital issues we must address, many of which I have spoken about previously on this floor. We must work, for example, to scale up our Nation's cybersecurity and law enforcement resources to match the seriousness of the threat posed by cyber criminals, by terrorist organizations, and by hostile nation states using cyberspace to attack our Nation.

The bottom line is we have a lot of important work to do. I am glad there is every indication that it will be bipartisan work, undertaken with the country's best interests in mind. I look forward to taking on this task with my colleagues in the months ahead.

I yield the floor.

WELCOMING HIS EXCELLENCY TSAKHIAGIIN ELBEGDORJ

Mr. LUGAR. Mr. President, today as ranking member of the Senate Foreign Relations Committee, I am pleased to welcome the President of Mongolia, His Excellency Tsakhiagiin Elbegdorj, a renowned promoter of democracy and a longtime friend of the United States.

As a leader of the peaceful democratic revolution in Mongolia in 1990, President Elbegdorj was a pioneer of freedom in Mongolia. His distinguished service to Mongolia includes serving as Prime Minister and Vice Speaker of the Great Hural/Parliament.

The United States recognized Mongolia in 1987 and established our first Embassy in Ulaanbaatar in 1988. We have supported Mongolia in its move toward democracy and market-oriented reforms.

Our partnership with Mongolia is vibrant and growing with multiple intersects covering trade and economic issues, defense cooperation, and people-to-people programs. Mongolia is also active in regional and global affairs and would be an appropriate host for future multilateral talks related to North Korea and its nuclear weapons program.

Since 2003, Mongolian troops have been deployed in support of coalition operations in Iraq and Afghanistan. In addition, Mongolia has deployed over 3,000 personnel on U.N. peacekeeping missions in approximately 10 countries.

I appreciate this opportunity to convey my appreciation for the personal leadership of President Elbegdorj and his important contribution to the growing of Mongolia-U.S. relations.

JUNETEENTH 2011

Mr. CARDIN. Mr. President, I rise today in celebration of the 146th anniversary of Juneteenth, the oldest continually celebrated commemoration of the end of slavery in the United States. This significant historical event is appropriately observed as an important part of American history. Though the Emancipation Proclamation officially took effect on January 1, 1863, many slaves did not find freedom until Union troops were able to reach the Southern States to enforce the order. Lincoln's order initially directed the Confederate States to end slavery, but allowed the States that remained in the Union during the Civil War to maintain the peculiar institution of slavery. It wasn't until December of 1865 that the 13th amendment marked the complete abolition of slavery in this country. Juneteenth was an important first step toward inclusion in the greater American dream.

It is a time of reflection, healing and an opportunity for our country to have meaningful discussions about our legacy of slavery and inequality and our ambitions for a more perfect Union.

With the breadth of technology we have today, it is difficult for many to conceive of a time where news traveled over days, months and even years depending on where the communication began and ended. The real-time dissemination of information via mobile phones, BlackBerries and Skype video chat makes it easy to forget a time when things moved at a much slower pace. In the 1860s horses were widely used for carrying mail, although parts of the country were building out railroads—with locomotives powered by steam traveling approximately 15 miles per hour.

On June 19, 1865, Union troops arrived in Galveston, TX, to deliver freedom to slaves still held in bondage. Because of the amorphous period between the Emancipation Proclamation and the official implementation of freedom for America's slaves, Juneteenth is celebrated not only on June 19, but the entire month of June, to represent the slow spread of freedom during the war. The culminating reading of General Order No. 3 on June 19 sparked spontaneous and jubilant celebration, and the spirit of that celebration has thrived in every African-American community from that day forward.