CYBER SECURITY PUBLIC AWARENESS ACT

Mr. WHITEHOUSE. Mr. President, I rise to speak about the Cyber Security Public Awareness Act of 2011, which I have introduced with Senator KYL.

The damage caused by malicious activity in cyberspace is enormous and unrelenting. Every year, cyber attacks inflict vast damage on our Nation's consumers, businesses, and government agencies. This constant cyber assault has resulted in the theft of millions of Americans' identities; exfiltration of billions of dollars of intellectual property; loss of countless American jobs; vulnerability of critical infrastructure to sabotage; and intrusions into sensitive government networks.

These massive attacks have not received the attention they deserve. Instead, we as a nation remain woefully unaware of the risks that cyber attacks pose to our economy, our national security, and our privacy. This problem is caused in large part by the fact that cyber threat information ordinarily is classified when it is gathered by the government or held as proprietary when collected by a company that has been attacked. As a result, Americans do not have an appropriate sense of the threats that they face as individual Internet users, the damage inflicted on our businesses and the jobs they create, or the scale of the attacks undertaken by foreign agents against American interests.

We must not wait for a disaster before we recognize and respond to the cyber threats we face. A false sense of complacency is not a security strategy. For that reason, I believe that raising public awareness of cyber security threats is an important element of the substantial work that we in Congress must do to improve our Nation's cyber security.

The Cyber Security Public Awareness Act of 2011 takes up that challenge. It will raise the public awareness of the cyber threats against our nation in a manner that protects classified, business-sensitive, and proprietary information. By doing so, it will provide consumers, businesses, and policymakers with the continuous flow of information necessary to secure our networks, identities, infrastructure, and innovation economy.

The bill improves public awareness with respect to three key issues: attacks on the government, attacks on infrastructure, and attacks on businesses and consumers.

The bill enhances public awareness of attacks on Federal networks by requiring that the Department of Homeland Security and the Department of Defense submit reports to Congress that detail cyber incidents on the ''.gov'' and ''.mil'' domains. These reports would provide aggregate statistics on breaches, the volume of data exfiltrated, and the estimated cost of remedying these breaches, as well as the continuing risk of cyber sabotage after an incident.

The bill also improves government reporting in two other ways. It requires the Department of Justice and the Federal Bureau of Investigation to submit annual reports on their investigations and prosecutions of cyber crimes, as well as on the resources devoted to cyber crime and on any legal impediments that frustrate those efforts. It also requires the Department of Justice, in consultation with the Administrative Office of the Courts, to study the preparedness of the Federal courts to handle cases relating to botnets or other cyber threats, and to consider whether courts need improved procedural rules, training, or organization to handle such cases.

The bill includes four provisions to enhance the awareness of threats against our nation's critical infrastructure. First, it requires primary regulators to report to Congress on the cyber vulnerabilities in our Nation's critical infrastructure, including our energy, financial, transportation, and communications sectors, and of recommended steps to thwart or diminish cyber attacks in each industry. Second, it requires the Department of Homeland Security to commission reports on improving the network security of critical infrastructure entities, including through the possible creation of a secure domain that relies on technical advancements or notice and consent to increased security measures. Third, it requires the Department of Homeland Security to identify producers of information technology that are linked directly or indirectly to foreign governments. This provision also requires reporting of the vulnerability to malicious activity, including cyber crime or espionage, associated with the use of these producers' technologies in the United States' telecommunications networks. And fourth, the bill requires the Department of Homeland Security, in consultation with the Secretary of Defense and the Director of National Intelligence, to submit a report to Congress describing the threat of a cyber attack disrupting the United States' electrical grid, the implications of such a disruption, the possibility of quickly reconstituting electrical service in the event of a cyber attack, and plans to prevent such a disruption.

The bill also seeks to enhance cyber awareness in the private sector and among businesses and consumers using the Internet. It requires the Department of Homeland Security to report to Congress on policies and procedures for Federal agencies to assist a private sector entity in the event of a cyber attack that could result in the loss of life or significant harm to the national economy or national security. To ensure that our markets properly reflect cyber risks, the bill also tasks the Securities Exchange Commission with reporting to Congress on, first, the extent of financial risk and legal liability of issuers of securities caused by cyber intrusions or other cybercrimes, and, second, whether current financial statements of issuers transparently reflect these risks. Finally, the bill will help enhance consumer awareness of cyber threats by requiring a report to Congress on legal or other impediments to public awareness of common cyber security threats, the minimal standards of computer security needed for responsible Internet use, and the availability of commercial products to meet those standards. This provision also requires the Department of Homeland Security to report on its plans to enhance public awareness of common cyber security threats and to recommend congressional actions to address remaining impediments to appropriate public awareness of common cyber security threats.

The Senate has a lot of work ahead as it seeks to improve our Nation's cyber security. One vital element of this work will be to ensure that we have an appropriate public awareness of cyber security threats going forward. I look forward to working with my colleagues on this important task as well as on cyber security issues more broadly.

I would particularly like to thank Senator KYL for working with me on this piece of legislation. Senator KYL has worked on cyber security issues extensively in the past, and we have worked together on Intelligence issues, so I very much look forward to partnering with him on this and other cyber security bills. As demonstrated by the hearing we held this week in the Crime and Terrorism Subcommittee of the Judiciary Committee, as well as by the important work previously done by the Commerce, Homeland Security, Judiciary, and other Committees, this is a vitally important and urgent national security issue, but one that we can confront in a serious and bipartisan manner.

ARMENIAN GENOCIDE

Mrs. BOXER. Mr. President, I rise today to recognize the 96th Anniversary of the Armenian Genocide—a tragedy that has left a dark stain on the collective conscience of mankind.

What has made this tragedy even more painful—particularly for the Armenian people—is the failure of successive U.S. administrations to acknowledge the deliberate massacre of the Armenians by its rightful name—genocide.

So today, I also rise to reiterate my call to President Barack Obama to finally right this terrible wrong.

In 2008, then-Senator Obama said:

> . . . the Armenian Genocide is not an allegation, a personal opinion, or a point of view, but rather a widely documented fact supported by an overwhelming body of historical evidence. The facts are undeniable.

I could not agree more. And every day that goes by without full acknowledgement of these undeniable facts by the United States prolongs the pain felt by descendants of the victims, as well as the entire Armenian community.