US Bills on Cyber Security:

- H.R. 3674 of the House of 15 December 2011
- H.R.4263 of the House of 27 March 2012
- Senate Cyber Security Act of 2012

Attached are the front pages and content pages of the above bills.
Because of their length, full versions will be sent to MEPs by email.

112TH CONGRESS
1ST SESSION

H. R. 3674

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 15, 2011

Mr. DANIEL E. LUNGREN of California (for himself, Mr. KING of New York, Mr. MCCAUL, Mr. BILIRAKIS, Mrs. MILLER of Michigan, Mr. WALBERG, Mr. MARINO, Mr. LONG, Mr. TURNER of New York, Mr. STIVERS, and Mr. LANGEVIN) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Select Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011" or the "PRECISE Act of 2011".

112TH CONGRESS
2D SESSION

H. R. 4263

To improve information security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 27, 2012

Mrs. BONO MACK (for herself and Mrs. BLACKBURN) introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committees on Oversight and Government Reform, the Judiciary, Armed Services, and Select Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To improve information security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012" or the "SECURE IT Act of 2012".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

112TH CONGRESS
2D SESSION

S. _____

To enhance the security and resiliency of the cyber and communications infrastructure of the United States.

IN THE SENATE OF THE UNITED STATES

Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, and Mrs. FEINSTEIN) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Cybersecurity Act of 2012".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) COMMERCIAL INFORMATION TECHNOLOGY PRODUCT.—The term ''commercial information technology product'' means a commercial item that organizes or communicates information electronically.

(2) COMMERCIAL ITEM.—The term ''commercial item'' has the meaning given the term in section 103 of title 41, United States Code.

(3) COVERED CRITICAL INFRASTRUCTURE.—The term ''covered critical infrastructure'' means a system or asset designated by the Secretary as covered critical infrastructure in accordance with the procedure established under section 103.

THE CYBERSECURITY ACT OF 2012

The bipartisan *Cybersecurity Act of 2012* was developed in response to the ever-increasing number of cyber attacks on both private companies and the United States government. As the country increasingly relies upon the Internet to conduct business, the critical services upon which we rely have become increasingly vulnerable to cyber threats. The country's most critical infrastructure can now be manipulated or attacked by malicious actors using computers halfway across the globe. The destruction or exploitation of critical infrastructure through a cyber attack, whether a nuclear power plant, a region's water supply, or a major financial market, could devastate the American economy, our national security, and our way of life. Defense and intelligence leaders have called malicious cyber actors an "existential threat" to our country.

Working closely with Senate leadership, the *Cybersecurity Act of 2012* is a joint effort by leaders and senior members of the Senate Committees on Commerce, Homeland Security and Governmental Affairs, and Intelligence to give the federal government and the private sector the tools necessary to protect our most critical infrastructure from growing cyber threats. The bill is a combination of legislation passed by the Commerce and Homeland Security Committees, and it incorporates extensive input from companies and trade associations representing a large swath of the private sector, including the information technology, financial services, telecommunications, chemical, and energy sectors. Other Members of Congress, national security, privacy and civil liberties experts, and government agencies have also provided important input.

To ensure the federal government and the private sector take the necessary steps to secure our nation, the *Cybersecurity Act of 2012* would do the following:

Determine the Greatest Cyber Vulnerabilities. The bill would require the Secretary of Homeland Security, in consultation with the private sector, the Intelligence Community, and others, to conduct risk assessments to determine which sectors are subject to the greatest and most immediate cyber risks.

Protect Our Most Critical Infrastructure. The bill would authorize the Secretary of Homeland Security, with the private sector, to determine cybersecurity performance requirements based upon the risk assessments. The performance requirements would cover critical infrastructure systems and assets whose disruption could result in severe degradation of national security, catastrophic economic damage, or the interruption of life-sustaining services sufficient to cause mass casualties or mass evacuations. The bill would only cover the most critical systems and assets in a given sector, and only if they are not already being appropriately secured.

Protect and Promote Innovation. Owners of "covered critical infrastructure" would have the flexibility to meet the cybersecurity performance requirements in the manner they deem appropriate. The private sector also would have the opportunity to develop and propose