

17 February 2010

The Honorable Robert Byrd  
Office of the President Pro Tempore of the Senate  
S-126 Capitol Building  
Washington, DC 20510

Dear Senator Byrd:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation's infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable Harry Reid  
Office of the Senate Majority Leader  
S-221 Capitol Building  
Washington, DC 20510

Dear Senator Reid:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation's infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable Richard Durbin  
Office of the Senate Majority Whip Leader  
S-321 Capitol Building  
Washington, DC 20510

Dear Senator Durbin:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation's infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable Mitch McConnell  
Office of the Senate Minority Leader  
S-230 Capitol Building  
Washington, DC 20510

Dear Senator McConnell:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation's infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable Jon Kyl  
Office of the Senate Minority Whip  
S-208 Capitol Building  
Washington, DC 20510

Dear Senator Kyl:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation's infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable David Schiappa  
Office of the Secretary for the Minority  
S-337 Capitol Building  
Washington, DC 20510

Dear Senator Schiappa:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation's infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world's largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable John D. “Jay” Rockefeller IV  
Chairman, Committee on Commerce, Science and Transportation  
531 Hart Senate Office Building  
Washington, DC 20510

Dear Mr. Chairman:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation’s critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation’s infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world’s largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc

17 February 2010

The Honorable Ann Bailey “Kay” Hutchison  
Ranking Minority Member  
Committee on Commerce, Science & Transportation  
284 Russell Senate Office Building  
Washington, DC 20510

Dear Senator Hutchison:

I am writing on behalf of the Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA) to ask you to support prompt Senate action on H.R. 4061, the *Cybersecurity Enhancement Act*, which passed the House on 4 February, 2010. The nation’s critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks depends upon networked information systems (NIS) for their operation. Because there is an inadequate understanding of what makes NIS vulnerable to attack or how best to reduce these vulnerabilities, or how to transfer cybersecurity knowledge to actual practice, these systems presently possess vulnerabilities that can be exploited by malicious hackers. In short, it appears that our nation's dependence on NIS has grown faster than our efforts to address cybersecurity vulnerabilities, increasing the potential for disastrous results to the nation’s infrastructure.

The bill will address these cybersecurity vulnerabilities in the federal, private, and public sectors through better coordination and prioritization of U.S. representation in international cybersecurity technical standards development, federal cybersecurity research and development (R&D) activities, and strengthening of the cybersecurity workforce. These efforts will be continued through reauthorization of cybersecurity related programs at the National Science Foundation and the National Institute of Standards & Technology.

To enhance the protection of our cybersecurity resources against a potential, concerted malicious attack, IEEE-USA also strongly supports increased funding for cybersecurity R&D and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems software and hardware. IEEE-USA also urges Congress to support cybersecurity technology transfer programs and to facilitate commercialization, which will create skilled jobs. IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate sufficient and stable funding for cybersecurity R&D, facilitate development and implementation of cybersecurity standards and support cybersecurity education programs.

IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. IEEE-USA is part of IEEE, the world’s largest technical professional society with 375,000 members in 160 countries. See <http://www.ieeeusa.org>. For more information, contact Bill Williams, IEEE-USA at (202) 530-8331, or at [bill.williams@ieee.org](mailto:bill.williams@ieee.org).

Sincerely,



Evelyn H. Hirt  
IEEE-USA President

EHH/BW:bc