

POSITION STATEMENT

CYBERSECURITY

**(Approved by the IEEE-USA
Board of Directors, 16 May 2014)**

Cybersecurity, and especially the cybersecurity of the United States of America's critical national infrastructures, is critical to ensuring the economic and national security of the nation, as well as protecting the security and privacy of personal data. IEEE-USA urges a coordinated public-private effort to enhance the nation's cybersecurity, including strong federal support for cybersecurity research, development of voluntary, consensus-based cybersecurity standards, stimulation of commercial innovation, expansion of cybertraining and workforce development, and strengthening public awareness of cyberthreats and risk-reduction techniques.

As part of a comprehensive national cybersecurity strategy, IEEE-USA specifically recommends that action be taken in each of the following areas:

- **Research and Development:** The federal government should develop and implement a multi-agency cybersecurity research and development plan to meet our national cybersecurity objectives. Key elements of the plan include:
 - Ensuring our ability to design, protect, test and verify the security and reliability of complex software-intensive systems, in the face of constantly evolving cyberthreats
 - Mitigating the effects of successful cyberattacks, including an emphasis on design for system resiliency and “self-healing” systems
 - Fostering new approaches to eliminating backdoors and other illicit access to software, firmware, or other embedded system triggers, which can be exploited to bypass security mechanisms.
 - Encouraging and enhancing cross-agency and multidisciplinary collaboration, and using improved techniques and processes

- Coordinating and synergizing efforts among R&D labs, industry, academia and the government
- Conducting research to support cybersecurity curricula development
- Conducting research into technology and techniques for identifying counterfeit or compromised cybersystem software and components
- Supporting cybersecurity modeling, test beds and demonstration projects

Adequate and sustained funding should be provided to meet the plan's objectives.

- **Standards Development:** It is imperative for the federal government and U.S. industry to work together with standards organizations, such as IEEE, to facilitate voluntary, industry-led standards and best practices to reduce cyber risks to critical infrastructure.
- **Integrated Design:** The federal government's cybersecurity program and policy guidance should synergize with the architectures and protocols of the infrastructure systems to be protected in order to assure compatibility and effectiveness.
- **Technology Development and Commercialization:** Working with the private sector, the federal government should facilitate the rapid transfer of federally funded basic and applied research results for technology development, including support for timely commercialization. The goal should be to promote an on-going collaboration among federal laboratories, universities and industry to foster an environment that facilitates the rapid application of technology to new cybersecurity solutions.
- **Securing the Cyber Supply Chain:** The cybersecurity of critical systems and networks requires making sure that the components used in the system or network, such as software, semiconductors and embedded systems, which are often sourced abroad, are properly manufactured, tested, handled, and stored to ensure their quality, reliability and the absence of inadvertent or malicious cyber vulnerabilities. In addition to supporting R&D into counterfeit and vulnerability detection technology and methods, the Federal government should focus its efforts on enhancing customs enforcement and encouraging industry adoption of supply chain management standards and best practices.
- **Education and Workforce Development:** The government should encourage and financially support the development of curricula, as well as instruction techniques and materials, for more effective teaching and training in cybersecurity at all educational levels. Funding should be provided for scholarships to train cyberprofessionals in exchange for public service. The respective roles of education, accreditation, training and certification--in ensuring

a strong, professional, cybersecurity workforce, should be explored and strengthened, where appropriate. IEEE-USA encourages using programs that generate interest and focus on cybersecurity careers, including competitions and challenges. In addition, IEEE-USA advocates authorizing appropriate federal agencies to engage in outreach and visibility campaigns, to increase public awareness of cyber risks and mitigation practices.

- **Continuity:** Cybersecurity policy, standards, best practices, education and research should emphasize continuous daily monitoring, testing and updating cybersecurity processes and protections, to help ensure continuous reliability and availability of critical systems, in light of constantly evolving threats.
- **Information Sharing:** IEEE-USA also believes some mutually acceptable process for sharing public-private information, regarding cyberthreats and best practices, is highly desirable. Such a process should be tailored to the needs of private sector participants in each of the relevant infrastructure sectors, to encourage voluntary participation.
- **Privacy.** In developing and applying cybersecurity measures, all parties should work to ensure that privacy is accorded a high level of importance and protection.

In a world marked by rapidly changing technologies and constantly evolving threats, absolute security from cyberattack is not a realistic expectation. For that reason, a robust national cybersecurity program is essential to minimize the risks and effects of successful cyberattacks that can cause significant damage and societal disruption vastly greater than the scale of the attack.

This statement was developed by the IEEE-USA Committee on Communications Policy, and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good, and promotes the careers and public policy interests of more than 200,000 engineers, scientists and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.