IEEE-USA

POSITION STATEMENT

CYBERSECURITY

Adopted by the IEEE-USA
Board of Directors (21 June 2019)

Cyberspace vulnerability is one of the defining technological concerns of our time. Bad actors are endangering our national security. They can take down parts of our national infrastructure, penetrate voting systems, personal financial accounts, financial systems of major corporations, credit systems and ratings, private communications, and most things on our ubiquitous networks.

Robust cybersecurity, especially for the United States of America's critical national infrastructures, is crucial to ensuring economic and national security, as well as for protecting the personal data and welfare of US citizens. IEEE-USA urges all stakeholders to engage in a coordinated public-private effort to enhance the nation's cybersecurity position and resilience. This effort requires strong federal support for cybersecurity research, development of voluntary, consensus-based cybersecurity standards, cybersecurity law and regulation to promote industry adoption of best practice, stimulation of commercial innovation, cybersecurity workforce development, and expansion of cybersecurity training with relevant certification and licensing. Ensuring a robust cybersecurity ecosphere also requires strengthening public awareness of cyber threats and broad adoption of risk-reduction techniques.

The world's citizens now enjoy automation, access to near instantaneous information and personal connections that were not possible a decade ago. There are millions of applications using emerging and developed technologies, including mass and social media, cloud infrastructure, artificial intelligence, signal processing, autonomous vehicles, satellite communication and guidance, visual and sound recognition, predictive analytics and software-defined networks, among many others. These reside on billions of cyber-driven smartphones, computers, cameras, devices, the Internet of Things, or "IoT," and tools that are used daily almost by everyone. Machinery, sensors and processes are increasingly reliant on modern networked communications. These innovative applications are densely woven into critical infrastructures in an integrated, holistic manner that signify the infrastructure's interconnectedness and interdependence and are essential to industrial applications, commerce operations, and citizens' daily lives.

Safeguarding the cyber ecosystem presents significant challenges as cyberattacks and cyber exploits become more massive and complex. Recent cyberattacks often involve nation-states, organized crime, corporate espionage, and political actors. These malicious attacks cause significant disruptions to critical national infrastructures and to people's lives.

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

1) Crucial Cyber Defense Research and Development Efforts:

The federal government should develop and implement a multi-agency coordinated cybersecurity technical strategies as well as necessary supporting research and development programs to meet our national cybersecurity objectives; key elements should include:

a. Ensuring our ability to design, protect, test and verify the security, reliability, and robustness of the cyber ecosphere; including the massive, complex and often unsynchronized and heterogeneous multi-layer and multi-function networks, against continually evolving cyber threats.

b. Establishing an automated and comprehensive cyberattack incident reporting and monitoring system; combined with coordinated partitions and instantaneous self-healing architecture; compliant with national frameworks and employing advanced technologies, such as artificial intelligence, big data analytics, next-generation firewalls and encryption technologies.

c. Fostering new approaches to detect and eliminate backdoors, misconfigurations, imposters and other illicit access to software, firmware, or other embedded system controls, which can be exploited to bypass security mechanisms and to damage, copy, divert, insert or corrupt data, and disrupt networks, system and operations.

d. Commission cybersecurity R&D projects that include identifying attacking traces, signatures and compromising methodologies, and prescribing strategies for responses, mitigation and rapid restoration of the damaged cyber system, networks, software, and components.

e. Propelling advanced and industry-specific infrastructural cyber defense and mitigation systems, including but not limited to the energy grid, 5G services, autonomous transportation, Global Positioning Systems (GPS), satellite communications, aviation navigation, traffic control and communications, public safety and security surveillance, Industrial Control Systems (ICS) and networks, distributed financial transactions, voting system, ID protection, national security, and defense.

f. Supporting cybersecurity modeling, test beds, and demonstration projects.

We recommend that the federal government provide adequate and sustained funding to build United States cybersecurity strengths through on-going collaboration among government, academia and industries to facilitate the rapid transfer of federally funded research results into new cybersecurity solutions. Other than for non-confidential fundamental research, we urge that grant recipients, contractors, sub-contractors and their workers be subject to appropriated security process to reduce insider malfeasance and potential perpetrator concerns.

2) Securing the Cyber Supply Chain: The components used in the system or network, including semiconductors, devices, embedded systems, and firmware are often sourced abroad. They need to be correctly manufactured, tested, handled and stored to ensure the absence of cyber vulnerabilities: insider-attacks through employees, contractors, suppliers and imposters that have known risk cyber paths. In addition to funding malicious and vulnerability detection technologies, we recommend that the Federal government and industry jointly enhance export control and U.S. Customs enforcement for technologies crossing the border, adopt supply chain management standards, impose non-employee access limitations & clearance procedures, regulate process-dependent strong passwords and follow best practices.

3) Uphold the International Cyber Strategy across Country Borders: In recent years, several countries have performed massive cross-border cyberattacks. IEEE-USA supports policies and actions that promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens global security and fosters free expression and innovation. The US Government should cooperate internationally in efforts to increase legal certainty in cyberspace for individuals, corporations and nation states by establishing norms and responsible behaviors that guide states' actions and sustain partnerships.

4) Interoperable Cybersecurity Standards Development: The Federal Government agencies, including and not limited to NIST, DOD, FCC, FAA, NHTSA, and NERC, should work with voluntary standards organizations to facilitate voluntary, industry-led standards and best practices to spur innovation, maximize interoperability and foster wider adoption, thus reducing cyber risks on critical infrastructure, industrial operations, government projects, and the general public.

5) Strengthen Education and Workforce Development: Due to the shortage of talents with modern cyber defense skills, we encourage the government to take a leadership role for developing innovative curricula, accreditation, training, certification, and licensing programs in qualified institutions and offer scholarships in strengthening US cyber security capabilities. IEEE-USA encourages programs that generate interest and focus on cybersecurity careers, such as sponsoring competitions and challenges, and engaging wide outreach and visibility campaigns. Federal hiring and contracting

should require adequate cybersecurity education, certification, and licensing for relevant professionals.

6) Enhance Information Sharing: IEEE-USA recommends public-private information sharing regarding cyber threats and best practices without releasing confidential information. Such processes should be tailored to the needs of stakeholders, both private and public, in each of the relevant infrastructure sectors, and mandate their participation.

7) Protect Privacy: In developing and applying cybersecurity measures, support should be provided to ensure personal data is used only with full consideration of ethical and legal requirements and cultural norms. All parties must work to ensure a high level of importance and protection is established for personal privacy of all cyber users.

8) Cyber Defense with Adaptive Continuity: In a world marked by rapidly changing technologies and continually evolving threats, it is almost impossible for today's IT systems, with widespread communication networks and off-site access, to be 100% secured. The national cyber infrastructure should minimize risks and employ mitigation measures that isolate cyber outbreaks and enable rapid recovery. The continuous monitoring, testing and rapid updating of new adaptive tools are essential for minimizing the chance of cyber breach and enabling lasting reliability and availability.

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 the nearly 180,000 engineering, computing and allied professionals who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.