ALEC American Legislative Exchange Council
LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

DRAFT STATEMENT OF PRINCIPLES FOR CYBERSECURITY

WHEREAS, it is the mission of the American Legislative Exchange Council (ALEC) to advance the principles of free markets, limited government and federalism; and

WHEREAS, effective cybersecurity is essential for the proper function of government and continued growth of the economy in cyberspace; and

WHEREAS, cyber challenges could pose an existential threat to the US economy, our national security apparatus and public health and safety;

THEREFORE, LET IT BE RESOLVED, that ALEC supports the following principles in formulating effective government policy regarding cybersecurity:

1. ***Effective cybersecurity measures reflect the global, borderless, and interconnected nature of cyberspace***

Cyberspace is a global and interconnected system of networks and users that spans geographic borders and traverses national jurisdictions. While recognizing government's important role to protect its citizens, the state and the U.S. governments should exercise leadership in encouraging the use of bottom-up, industry-led, and globally-accepted standards, best practices, and assurance programs to promote security and interoperability. We must also collaborate with trusted allies both to share information and to bolster defenses.

2. ***Effective cybersecurity measures are capable of responding and rapidly adapting to new technologies, consumer preferences, business models, and emerging threats***

Cyberspace is full of innovation and dynamism, with rapidly changing and evolving technologies. Cybersecurity measures must be equally dynamic and flexible to effectively leverage new technologies and business models, and changing consumer preferences, and address new, ever-changing threats.

3. ***Effective cybersecurity measures focus directly on threats and bad actors***

In cyberspace, as in the physical world, adversaries use instruments (in this case, technology and communications) to carry out crime, espionage, or warfare. Cybersecurity measures must enable governments to better use current laws, regulations, efforts, and information sharing practices to respond to cyber bad actors, threats, and incidents domestically and internationally.

4. ***Effective cybersecurity measures focus on awareness***

DRAFT

Cyberspace's owners include all who use it: consumers, businesses, governments, and infrastructure owners and operators. Cybersecurity measures must help these stakeholders to be aware of the risks to their assets, property, reputations, operations, and sometimes businesses, and better understand their important role in helping to address these risks. Industry should lead the way in sharing information with the appropriate government entities following an attack and collaborating with others in the private sector to share best practices.

5. ***Effective cybersecurity measures emphasize risk management***

Cybersecurity is not an end state. Rather, it is a means to achieve and ensure continued trust in various technologies and communications networks that comprise the cyber infrastructure. Cybersecurity measures must facilitate an organization's, whether it is the government or a private entity, ability to properly understand, assess, and take steps to manage ongoing risks in this environment.

6. ***Effective cybersecurity measures build upon public-private partnerships, existing initiatives, and resources***

Partnerships between government and industry has provided leadership, resources, innovation, and stewardship in every aspect of cybersecurity since the origin of the Internet. Cybersecurity efforts are most effective when leveraging and building upon these existing initiatives, investments, and partnerships.

DRAFT