DIGITALEUROPE Information Technology Industry Council JEITA

Global Information and Communications Technology (ICT) Industry Statement

Recommended Government Approaches to Cybersecurity

June 2012

Cyber security is a high priority for governments, society, and industry globally. Policy approaches to advance cyber security must meet security needs while preserving interoperability, openness, and a global market. Such approaches will result in enhanced security. In the right policy environment, we can increase security while maintaining the societal benefits derived from the growth and development of cyberspace.

As governments pursue cyber security-related laws, regulations, and other policies, we urge them to adhere to the following principles:

- **Develop cyber security policies in a transparent manner and with relevant stakeholder input.** Governments should ensure that the development of all laws, regulations, and other policies related to cyber security are undertaken in an open and transparent policymaking process. This can include, but is not limited to, publishing draft texts and allowing for public notice and comment procedures.
- **Enable risk management and innovation.** Governments should adopt policy approaches that can adapt to market changes and allow enterprises and consumers to properly understand, assess, and take steps to manage risks. A risk management approach recognizes that private-sector actors are best placed to manage and protect their networks, services, and assets and are incentivized to do so by market forces, corporate responsibility, and ethical standards.
- **Develop and implement cyber security policies in partnership with the private sector.** The ICT industry has extensive experience in providing leadership and resources in every aspect of cyber security. Cyber security policies will be most effective when building upon these initiatives and investments. This can help to ensure that policies are adaptive and effective.
- **Encourage the development and use of globally recognized, industry-led, voluntary consensus security standards, best practices, assurance programs, and conformity assessment schemes.** These approaches will improve security, because 1) nationally focused efforts may not have the benefit of the best peer review processes traditionally found in global standards bodies, 2) proven and effective security measures must be deployed across the entire global digital infrastructure, and 3) the need to meet multiple, conflicting security and conformity assessment requirements in multiple jurisdictions raises enterprises' costs, demanding valuable security resources.
- **Ensure the use of globally standardised tests and certification.** Governments should allow for compliance requirements based on risk assessments, and be supportive of international transportability of test results and certificates.
- **Ensure that cyber security requirements are technology-neutral.** Mandates requiring certain technologies, including a preference for domestically made technologies, decrease security because the country can no longer access leading-edge security solutions that could be developed anywhere in the world.

- **Ensure that cyber security requirements allow for procurement of technologies regardless of the country of origin or the nationality of the technology vendor.** Product security is a function of how a product is made, used, and maintained, not by whom or where it is made. Governments should re-examine their understanding of cyber supply chain risk, acknowledge that ICT vendors are best placed to manage and protect their ICT supply chains, and partner with industry on solutions that build bridges rather than exclusionary trade walls.
- **Ensure that any cyber security requirements avoid forced transfer or review of intellectual property (IP), such as source code.** Such IP is business proprietary information that is essential to companies' ability to innovate and remain economically competitive.
- **Limit any prescriptive requirements to areas of the economy that are highly sensitive, such as government intelligence and military networks.** Many governments may justifiably have very stringent requirements for security technologies sold into intelligence and military networks. Government procurement requirements for such systems should not extend to other government networks, government-licensed networks or to privately run infrastructure or commercial companies**.**
- **Strengthen institutions, and develop contingency plans and cyber security strategies.** Governments should have their own strong, standalone institutions, such as Computer Emergency Readiness Teams (CERTs), to ensure effective cyber security. Governments have an important role to play—working in partnership with the private sector whenever possible—in reflecting overarching national, regional and international security objectives; sharing in preparedness and prevention preparations; diagnosing and responding to incidents; and addressing education and research gaps.
- **Focus on criminals and their threats.** Governments should endeavor to respond to cyber actors, threats, and incidents domestically and internationally, working in cross-border partnerships to the extent possible, when appropriate.
- **Focus on education and awareness.** Governments should make all stakeholders aware of their important roles in helping to address cyber risks. Government efforts should include raising awareness, via education systems, to citizens of all ages about cyber security.

This statement has the full endorsement of DIGITALEUROPE (DE), the Information Technology Industry Council (ITI), and Japan Electronics and Information Technology Industries Association (JEITA).

About DIGITALEUROPE, JEITA, and ITI

DIGITALEUROPE: DIGITALEUROPE represents the digital technology industry in Europe. Our 100+ members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. Together, DIGITALEUROPE's members represent more than 10,000 companies that employ two million citizens and generate €1 trillion in revenues. Our website provides further information on our activities: http://www.digitaleurope.org.

JEITA: The objective of the Japan Electronics and Information Technology Industries Association (JEITA) is to promote the healthy manufacturing, international trade and consumption of electronics products and components in order to contribute to the overall development of the electronics and information technology (IT) industries, and thereby further Japan's economic development and cultural prosperity. Learn more at http://www.jeita.or.jp/english/.

ITI: The Information Technology Industry Council (ITI) is the premier advocacy and policy organization for the world's leading innovation companies. ITI navigates the constantly changing relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. We develop first-rate advocacy strategies and market-specific approaches. And we deliver results. Visit itic.org to learn more.