Information Technology
Industry Council

ITI Position Paper on the Proposed "Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union"

June 24, 2013

The Information Technology Industry Council (ITI) appreciates the opportunity to provide comments on the Proposed "Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security (NIS) Across the Union," issued February 7, 2013 (herein proposed Directive).

ITI's views are based on 1) our *Cybersecurity Principles for Industry and Government*[1] and 2) the *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity*[2] co-authored by ITI, DIGITALEUROPE, and the Japanese Electronics & Information Technology Industry Association (JEITA). Both documents are important markers for successful cybersecurity policy and we are pleased that many ideas put forth in the proposed Directive align with them. These include proposals to strengthen public agencies, improve Member State and international coordination on cybersecurity, and develop national cybersecurity plans; raise awareness; increase research and development (R&D); and augment public-private partnerships. We also appreciate the flexible, technology neutral approach. Finally, we agree that hardware manufacturers and software developers should not be deemed market operators in the context of the objectives of this Directive.

At the same time, we are concerned with some of the approaches in the proposed Directive, including 1) the scope of what is considered critical infrastructure to include Internet enablers and information society services that are not inherently critical, 2) an information sharing model too focused on the proposed top-down and unidirectional (industry to government) incident reporting framework, when a bidirectional approach including more flexibility for voluntary components would be more effective to understanding threats and improving incident response, 3) the risk of driving a static, "check-the-box" type of compliance regime instead of fostering a proper cybersecurity culture, and 4) the risk of new market access barriers that could result from proposals to draft and use new EU-specific security standards.

Below we detail our positions. Where we have concerns, we describe how alternative approaches would significantly strengthen Europe's cybersecurity. We hope these are taken into consideration as policymakers consider amendments to the proposed Directive.

Areas of Support in Proposed NIS Directive

Raising NIS Levels Across all EU Member States. We welcome proposals in the draft Directive that aim to strengthen public sector agencies and improve pan-European coordination on cybersecurity. This is covered most notably in Chapters II and III, as well as Recitals 9-13 of the Preamble. We agree with many aspects of Articles 4, 5, 6, and 7, including recommendations in

[1] http://www.itic.org/dotAsset/191e377f-b458-4e3d-aced-e856a9b3aebe.pdf
[2] http://www.itic.org/dotAsset/51ad6069-9f1b-4505-b2ff-b03140484586.pdf

Article 5 that Member States that have not already done so adopt national NIS strategies that include education, awareness raising, and training as well as R&D plans. We also support the development of national NIS cooperation plans (Article 5), national competent authorities (Article 6), and national Computer Emergency Response Teams (CERTs, Article 7). Finally, we support the proposed cooperation network in Chapter III, Article 8, which aims to circulate among Member States' competent authorities early warnings and other information, such as that related to cybercrime. We hope that this network can facilitate coordinated responses to incidents, when appropriate, as well.

Additional recommendation: Member States should be explicitly encouraged to involve private-sector stakeholders in the development and implementation of these Strategies and Plans. In particular, the private sector should be involved in risk assessments that are to be undertaken per Article 5. ITI companies work in partnership with many governments globally on such activities and we would be pleased to work in partnership with the Commission and Member States as you commence and strengthen work in these areas.

Public-Private Partnerships. We agree Recital 15's statement that because "most network and information systems are privately owned, cooperation between the public and private sector is essential." Public-private partnerships are essential to improve cybersecurity not only because the private sector owns the majority of critical infrastructure, but also because ICT companies have provided leadership, subject matter experts, technical and monetary resources, and innovation to enable all stakeholders to better manage and mitigate cybersecurity risk for more than a decade. Cyberspace would be much less secure without these initiatives, and we seek to work in partnership with our government colleagues to jointly improve cybersecurity.

Additional recommendation: We encourage Europe to strengthen its public-private partnership commitment, including through the Network and Information Security Platform, the European Public-Private Partnership for Resilience (EP3R), and other appropriate bodies. A commitment, followed by action, by governments to partner with industry at national and EU levels to set and execute on common cybersecurity goals will make Europe's cyber posture stronger. ITI companies will be pleased to be included in these partnerships.

Emphasis on Flexibility. Recital 33 notes that the "Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions." We concur that it is very important to review any cybersecurity-related policies to make sure they remain effective and adjust them as necessary.

Additional recommendation: Any review of the Directive should involve all interested stakeholders, per the public-private partnership model highlighted above.

Technology Neutrality. We highly support the draft Directive's approach to avoid mandates regarding how the ICT industry designs, develops, and manufactures its products (Recital 25).

Emphasis on International Cooperation. We concur with the statement in Recital 21 of the Preamble regarding the need for closer cross-border cooperation to address the challenges of cyberspace. The EU has long been recognized as a global technology leader. European companies have particular expertise in telecommunications network infrastructure, and European technologies led the way in many mobile technologies, such as 3G. We believe that similarly many countries will look to Europe's leadership in cybersecurity policy. Taking a leadership role with regard to one of this decade's pressing technology issues—cybersecurity—is a responsibility that we urge Europe to accept.

Additional recommendation: It is imperative that the EU signal to governments globally about the approaches that will most effectively improve cybersecurity. Per the DE-ITI-JEITA Joint Statement of 2012, this entails a cooperative approach between government and industry; taking approaches to advance cybersecurity that meet security needs while preserving interoperability, openness, and a global market; and allowing industry to innovate and compete. We fear, however, that some of the draft Directive's proposed actions, as described below, diverge from these best practices. The Commission, in particular DG Trade and DG CNECT, has actively worked over the past few years to discourage the governments of China and India from enacting country-of-origin approaches to product security, namely in China's Multi-Level Protection Scheme (MLPS) and India's Preferential Market Access (PMA) policy, respectively, that threaten to shut European ICT companies out of those markets. The EU should set an example for others around the world on how address legitimate cybersecurity concerns without disrupting innovation, competition, and global trade flows. We urge European policymakers to commit to:

- Exercising leadership in encouraging the use of industry-led, globally accepted standards, best practices, and assurance programs to promote security and interoperability.
- Making the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid EU-specific requirements.
- Carefully viewing any EU policies from a global perspective. Any EU policies that are non-globally compatible, whether implemented through a Directive or a Regulation (or sometimes if merely proposed) will be emulated around the world. Some countries also may use such policies/proposals as a starting point for their own additional domestic regulatory intrusions that will balkanize the global marketplace.
- Proactively seeking dialogues with the EU's trading partners about the use and benefits of industry-led, globally recognized standards and best practices that will achieve the requisite levels of security needed to meet national security concerns while preserving interoperability, openness, and economic development.
- Countering other countries' attempts to enact non-globally compatible cybersecurity-related standards, practices and requirements that threaten to balkanize cyberspace and make it less secure.

Keeping Information about Unpatched Vulnerabilities Confidential. Recital 28 of the Preamble states: "In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes." We agree with the importance of keeping vulnerabilities confidential before patches are available.

Additional recommendation: Recital 28 addresses instances when third parties/customers (not vendors) inform competent authorities about vulnerabilities. The Commission should extend that same philosophy to all instances of vulnerabilities, including when vendors identify them.

Policymakers should not require, or even urge, ICT vendors to inform authorities about product vulnerabilities before a patch to a particular vulnerability is designed and deployed. ICT companies take a responsible approach to disclosure of vulnerabilities to protect our customers as well as the integrity of our own systems. Reckless disclosure of unpatched vulnerabilities puts our customers at risk and reduces the effectiveness of security patches. ITI companies have robust processes and procedures in place for timely detection, patching of vulnerabilities, and notification as appropriate.

Treatment of Hardware Manufacturers and Software Developers. We welcome the protection and promotion of innovation in ICT products through the recognition that hardware manufacturers and software developers should not be deemed market operators in the context of the objectives of this Directive. Any security requirements placed on manufacturers or developers would presumably relate to the development and lifecycle of their products, which could stifle product security innovation and isolate Europe from a global approach to such issues. Secure development, product assurance and evaluation are already, and should continue to be, addressed through methods such as globally recognized cybersecurity standards and best practices including the Common Criteria (ISO 15408) and the Common Criteria Recognition Arrangement,[3] and/or telecom standards per 3GPP.

Areas of Concern with Proposed NIS Directive

Scope. ITI believes the term "providers of information society services" as used in Article 3 (8(a)) and Annex II is too broad and risks sweeping in a range of entities for which government regulation is neither necessary nor advisable. Per Annex II, e-commerce platforms, social networks, search engines, application stores, cloud computing services, and Internet payment gateways are all examples of "market operators" which, per Chapter IV, incur a number of obligations. Designating such services in a category that warrants additional regulation from a cybersecurity perspective will cause organizations to divert scarce resources away from areas requiring greater investment towards areas with lower priority.

We understand that one reason European policymakers chose to include "information society services" enablers in this category is the fact that their services underpin so many cyber transactions. While that is true, and losing access to these services would certainly be an inconvenience for many people, we do not believe that interruption of their services would have "catastrophic" results. In fact, the draft Directive itself draws a distinction in the definition of market operators (Article 3 (8)) between "operators of critical infrastructure" and "providers of information society services."

Recommendation: First, any regulation should apply to a narrow subset of systems and assets which are truly critical in nature. In short, the list of market operators relevant to NIS needs to be clearly drawn and carefully targeted so as to maximize the efficiency and effectiveness of the proposed measures. Overly broad or ill-focused definitions could spread resources too thin and capture unnecessary elements of the private sector, rather than focusing on high risk areas we

[3] The CC is an accepted global standard for computer security certification aimed to provide product assurance, as well as a multilateral agreement among 26 countries including 13 EU Member States (Austria, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Italy, the Netherlands, Spain, Sweden, and the UK).

need to keep people safe. Second, designation of which market operators shall be subject to greater regulation should be done in partnership with industry using a risk-based approach.

Security Standards. We are pleased that the Commission affirms in its February 2013 "FAQ" memo that the EU does not intend "to define minimum standards or level of security."[4] However, this appears difficult to reconcile with the intention of the draft NIS Directive to adopt a list of EU-endorsed relevant cybersecurity standards (See Recital 32 and Article 16).

ITI strongly cautions all governments not to set compulsory security standards for the commercial market– whether ones vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause organizations to divert scarce resources away from areas requiring greater investment towards areas with lower priority. To maintain (rather than restrain) innovation and to prevent the development of single points of failure, any standards lists should be purely indicative, their use entirely voluntary, and they should always allow organizations to adopt alternative solutions. Defining new, EU-centric standards has many downsides as they may conflict with global standards currently used, such as the CC and 3GPP, or set new trade barriers. Further, the Directive, read in conjunction with the cybersecurity Communication, could inspire the worrisome misconception that products made in Europe are "more secure," which is neither a true statement, nor a desirable perception.

Recommendations. The global ICT industry is heavily invested in developing standards to address important challenges in security management. We urge the Commission to take a leadership role in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices, make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid EU-specific requirements. We also welcome and encourage European governments to participate in standards development activities, particularly in private fora and consortia. In addition, the Commission and Member States might consider greater action in their own (public sector) use of voluntary, globally accepted standards or generally accepted industry practices for cybersecurity risk management. Indeed, government leadership can demonstrate such standards' importance and may be necessary to overcome economic disincentives to adoption of standards that yield benefits to the network as a whole.

Security Incident Notification.[5] Article 14 allows competent authorities to publicly disclose a security incident involving a market operator when the authority determines it is in the public interest to do so. We are pleased the proposal recognizes that incidents that are reported should relate to the core services provided by the market operator as opposed to incidental services. To draw out the distinction, for example, for an electricity distributor, the core service is provisioning of electricity, not that their public website goes down for a brief period.

[4] European Commission Memo: Proposed Directive on NIS—FAQs, February 7, 2013, p. 5.

[5] We note this part of the draft NIS Directive refers to **security incident notification,** NOT data breach notification.

However, the reporting requirements for security incidents having a significant impact could be overly broad and counterproductive when implemented by individual Member States. Further, this exercise on such a vague standard could cause unnecessary harm both to the reputation and security of the victim companies. Indeed, in many cases public disclosure of an incident could further weaken the security posture of the victim and unnecessarily expose proprietary and other confidential information.

Recommendations. The Directive should include a much clearer and narrower specification of the trigger threshold and substance of any security incident notification requirements. As a general principle, required disclosures from private sector companies to their customers should be limited to those instances where the information is meaningful and actionable. Any other approach would cause companies to expend considerable efforts upon the delivery of notices. In addition, because inconsiderate sharing of information about cyber threats and incidents could unfairly expose companies to new security risks, litigation, regulatory action, or competitive disadvantages, the Directive should provide liability protection for companies that share such information, as well as protections that ensure confidential information is not subject to unauthorized disclosure or unfair use by competitors or regulators.

Security Audits. We believe that market operators should be able to make use of self-compliance mechanisms to demonstrate compliance as opposed to competent authorities undertaking audits. For companies located in several Member States, having to deal with multiple competent authorities to conduct such audits would be a significant, and disproportionate, administrative burden. We also fear the “checklist effect,” where operators might actually degrade their security posture in order to conform to the audit. As such, we believe it is sufficient for the competent authority to require market operators and/or public administrations to provide the information necessary to assess the security of their networks and information systems as opposed to introducing an additional auditing power.

Conclusion

ITI concurs with many aspects of the draft Directive. At the same time, it is imperative that Europe establish a globally compatible cybersecurity policy approach that balances cybersecurity, innovation, and trade. The current cyber-threat environment evolves rapidly and requires a complex and layered approach to security that varies greatly across industry sectors. Further, businesses must adapt their risk management strategies faster than regulatory processes can move, and a static compliance approach risks encouraging some firms to invest only in meeting requirements that are outmoded before they can be published. A one-size-fits-all approach also could divert scarce security resources from areas requiring greater investment towards areas with lower priority. These outcomes could decrease Europe’s collective security.

ITI again thanks European policymakers for tackling the important issue of cybersecurity. We hope our input will receive due consideration. We are available at any time to elaborate on our comments and our suggestions, and our member companies stand ready to work with the EU and Member States to improve cybersecurity not only within Europe, but globally.

For more information contact Danielle Kriz, Director, Global Cybersecurity Policy at dkriz@itic.org