Brussels, 17 June 2013

AmCham EU's position on the Network and Information Security Directive

The American Chamber of Commerce to the European Union (AmCham EU) applauds the European Commission's efforts to give the EU a strong basis to develop its cybersecurity position and address a significant Single Market challenge. We welcome the ambition of the European Cybersecurity Strategy and draft Network Information Security (NIS) Directive to ensure that all Member States equip themselves with adequate resources to facilitate information sharing and cooperation and to inscribe Europe's efforts into the global dimension of cybersecurity. We believe that many of the objectives are well defined, but further improvements are needed to meet these objectives.

The market operators represented at AmCham EU are well aware of the importance of protecting not only our own networks and services, but also those of our customers. We are conscious of the commercial and business value of cybersecurity in a global economy that is increasingly reliant on network and information systems and where failures to meet appropriate security levels would affect trust and confidence of users as well as cause severe reputational damage. With these already very material cybersecurity incentives and operational realities in mind, we will focus our commentary on the requirements of the proposed Directive that will apply to market operators.

Scope of the NIS Directive

Analysis

To achieve a meaningful impact in better protecting Europe's critical information infrastructure, the Directive should focus on truly key networks and services.

AmCham EU believes that it is the combination of the two terms in Recital 24, 'reliant on ICTs' and 'essential to vital functions', that best capture the desirable scope of the Directive.

POSITION STATEMENT

Point of Contact: Roger Coelho, Policy Manager
American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu – www.amchameu.eu

We recognise that the integrity and security of critical information infrastructures must be strengthened to ensure reliable and undisrupted access to information networks for all, and that all actors share responsibility for strengthening security. However, we are concerned that the actual scope of market operators, as defined in Article 3 paragraph 8 and illustrated in Annex II, is not consistent with the criterion of 'essential to vital functions'. The indicative list in Annex II does not bring any clarity, quite to the contrary:

- The non-exhaustive nature of the list raises concerns with regard to long-term legal certainty and potential varying national interpretations of which market players are covered. A clear definition of the criteria for services to be covered would provide legal certainty while maintaining the necessary flexibility.

- Such a broad and legally undefined term as 'cloud computing services' could encompass virtually all online services irrespective of them being essential or vital, which could undermine the very relevance of the Directive by extending its scope to areas without any relation to critical information infrastructure protection.

- Similarly, the terms 'e-commerce platforms', 'social networks', 'search engines' and 'application stores' may be interpreted as referring to particular online services, but their relevance or importance to any vital function is undemonstrated. Indeed, it is questioned why the outage or unavailability of these services should be considered as impacting vital functions, given that for most of them, alternatives are commonly and publicly available at all times.

We are therefore concerned that such a broad, arbitrary and legally uncertain definition of scope leaves unanswered the essential question of who should be covered, and fails to provide guidance as to why a particular operator should be covered. This leaves providers of information society services unsure whether the Directive is applicable to them, and if so, for what reason, to what extent and to what end.

The blanket inclusion of 'providers of information society services which enable the provision of other information society services' should be reconsidered. For this Directive to increase the level of critical information infrastructure protection in Europe, its scope must capture those networks and services that are truly essential to the maintenance of well identified vital functions.

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu – www.amchameu.eu

POSITION STATEMENT

Extending the scope beyond operators of critical infrastructure and providers of key services would dilute effort, lose the focus on critical areas, and unnecessarily burden networks and services that have nothing critical, essential or vital about them. Based on the sheer number of information society services available in the Internal Market – from anywhere in the world – the Directive would end up applying mainly to operators that are simply irrelevant to the policy objective pursued.

At the same time we welcome the explicit exemptions of providers already covered by existing or foreseen risk management and reporting obligations (e-communications providers and trust service providers). Nonetheless the relationship should be further clarified between the various existing frameworks. Indeed, the 'exempted' providers may also provide bundled services falling in the scope of this Directive. This calls for further legal certainty as to what measures apply to what services. More importantly even, they should not be subjected unnecessarily to cumulative or inconsistent burdens. For the sake of efficiency and proportionality, market providers should not have to abide by different requirements depending on the services they provide.

We also welcome that hardware manufacturing and software development are excluded from the scope of market operators. The need to protect and promote innovation in ICT products is rightfully recognised in Recital 24, which states that hardware manufacturing and software development should not be viewed as information society services in the context of the objectives of this Directive. Any security requirements placed on the manufacturing of hardware or the development of software would presumably relate to the development and lifecycle of their products as opposed to the focus on security processes for the market operators included in the scope. Such regulation 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 industry-led codes, the global evaluation methodology, the Common Criteria (ISO 15408) and the Common Criteria Recognition Arrangement.

Suggested solutions

AmCham EU recommends:

- Focusing the scope on critical networks and truly key services;
- Reconsidering the blanket inclusion of 'providers of information society services';

POSITION STATEMENT

- Maintaining the clarification that hardware manufacturers and software developers are not considered to be market operators in the context of this Directive;
- Maintaining the exemption of those operators already covered by other cyber risk management and incident reporting requirements; and
- Clarifying further the relation of the Directive to such other requirements.

Single market, jurisdiction and applicable law within the Internal Market

Analysis

Harmonised and consistent requirements should be the goal

Harmonisation and consistency of requirements on market operators across the EU and, where feasible, in relationships with international partners, is essential. This is key to creating a level playing field for innovative and competitive solutions to be deployed throughout the Internal Market, particularly as these solutions are designed to address risk and threats on a transnational scale. It is equally important for customers and consumers if their overall level of protection is to improve. At the same time, flexibility will be necessary to address the great variety of technologies involved, the diversity of purposes for which they are used, and the broad array of threats facing different sectors.

- **Failing maximum harmonisation, the minimum harmonisation approach needs to be balanced with clear rules on jurisdiction and applicable law for market operators who do business across several Member States**

The effects of network and information security incidents are often cross-border in nature and not necessarily limited to the EU. Therefore a harmonised approach within the EU is essential.

It is also important to create a level playing field for cybersecurity solutions across all Member States. The requirements introduced should not maintain or raise market barriers, lead to intra-EU market fragmentation or discriminate against solutions from third countries.

While accepting that not all aspects covered by the proposed Directive can be fully harmonised, common terms for compliance are essential,

particularly for cross-border and pan-European market operators. However, while Recital 8 and Article 2 lay down the principle of minimum harmonisation, Member States will remain free not only to interpret the Directive when transposing it, but also to go beyond its requirements. As the applicability of the requirements is tied to the service being provided within the EU (Article 14[3]), it becomes important for operators providing services in more than one Member State to know which jurisdiction they fall under. In the interest of efficiency in the case of cross-border incidents, it should be sufficient for the market operator to notify the competent authority in only one Member State.

The issue is especially acute for those market operators whose services do not imply a physical presence, and that is the case in particular of 'key providers of information society services' whose services are provided remotely and across borders, including from outside the EU. For such operators, it is an essential question of legal certainty and compliance to know (subject to further clarifications in section 4 below):

- Which authority must be notified of an incident as per Article 14(2);
- Which authority's requirements, guidance or instructions to abide by as per Article 14 (4) and (6);
- Which authority's implementing measures, investigations and enforcement powers to subject themselves to as per Article 15 (1) and (2); and
- Which Member State's sanctions to be exposed to as per Article 17.

Conversely, Member States and their national authorities need to clearly understand the extent and reach of the supervision, implementation, enforcement, investigation and sanction powers conferred on them by Articles 6(4), 15(3) and 17. This is important because this will also determine their courts' competence for judicial review under Article 15(6), and will influence their role in cooperating with their peers for the consistent application of the Directive across the EU as Article 6(2) and Article 8 rightly require them to do.

Suggested solutions

- Shifting to a maximum harmonisation approach as far as the provisions applicable to market operators are concerned, or, failing that, at least complementing the minimum harmonisation principle of Article 2 with a requirement on Member States to

ensure that the transposition and implementation measures they adopt at the national level are consistent and harmonised;

- Based on experience from other areas of Internal Market legislation, particularly in the area of information society services, a one-stop-shop regime based on the country of origin of the provider should be introduced. The 'country of origin' should refer to the main establishment of the provider in the EU. In the absence of establishment, non-EU providers providing services into the EU should appoint a representative within the EU, and the competent jurisdiction and the applicable law should be those of the Member State where the representative is based. Cross-border investigations and enforcement should be carried out in an effort for enhanced consistency across the Single Market, under the leadership of the competent authority, in the framework of a mechanism to be further detailed within the cooperation network created by Article 8.

Risk management and incident reporting requirements

Analysis

As one of the main objectives of the Commission proposal is to foster the emergence of a culture of cyber risk management, the role of education, training and awareness raising should be better highlighted. Having sufficient attention for these issues will be of paramount importance, so that individuals and organisations can fully grasp the stakes and relevance of network and information security for themselves, the case being that they can better understand compliance requirements, be sufficiently skilled and to protect themselves adequately, as well as meet the requirements in practice. End-user education and awareness campaigns are particularly important considering the threats to security that can arise from uninformed users.

- **Security requirements should enable risk management but should not interfere with product designs**

The current text refers to technical and organisational cyber risk management measures that should be 'state of the art'. This implies an ever evolving process and hence, specific technical mandates need to be avoided. We therefore strongly welcome the clarification in Recital 25 that such measures should not require that ICT products be designed, developed or manufactured in a particular manner. However, we think a

strong reference should be inserted within the actual text. This will allow the necessary flexibility for this Directive to be able to deal with future technological developments.

- **Incident reporting can help improve risk management and security**

Incident reporting can be effective in improving risk management and security if part of a process for preventing and remediating breaches. In many Member States, voluntary reporting schemes are developing and creating the necessary trust between authorities and the private sector to effectively tackle cyber threats. Sensitive information-sharing can develop best in such an environment. AmCham EU strongly recommends properly analysing these emerging schemes, and comparing them to the Directive's suggested framework that segregates the cross-border information-sharing network between authorities on the one hand, and the incident reporting obligations of market operators on the other. Lessons could be learned at the EU level from these evolving best practices, and better ways may be found to tackle the cross-border dimension of information sharing.

The reporting scheme should incentivise sound risk management, facilitate the remediation of breaches, and ensure and contain information sharing to parties who 'need to know'. It should not be a sanction on victims, a factor of reputational risk, or a bureaucratic burden. Most importantly, it needs to be consistent with other notification schemes that may apply simultaneously and cumulatively, notably under privacy law or other existing or foreseen legislation (e.g. in the areas of e-communications and trust services).

- **Incident reporting needs a clear scope: core services and significant material impact**

AmCham EU welcomes the recognition that only incidents having a 'signification impact' should be reported, i.e. only incidents relating to the core services provided by the market operator. However, legal certainty can be increased by inserting a definition of core services under Article 3. In addition, further enhancements to the text could clarify that only incidents involving an actual penetration of information networks resulting in a significant negative impact on those core services would need to be reported. The current text talks about an actual adverse effect that is difficult to quantify. Improvements on this point would also help avoid the risk of 'over-reporting' which would increase the pressure on resources and competent authorities, damaging the effectiveness of the system.

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu – www.amchameu.eu

POSITION STATEMENT

- **Incident reporting should not lead to exposing vulnerabilities**

The underlying reasons of a cyber incident may include the exploitation of a vulnerability in the network and information infrastructure of the market operator. Indeed the intelligence generated is not only valuable but also sensitive. Market operators need the assurance that the information will be kept appropriately confidential and will not expose them to increased risk of undue liabilities. The reporting of such vulnerabilities should not be the main objective of the reporting scheme. When such a vulnerability is reported by the market operator, any information relating to it should be kept strictly confidential not only before a fix is found, but also until it has been deployed and implemented in the wider ecosystem. We welcome the clarification in Recital 28 to take these points into account.

- **The implementation of the requirements needs to be practical**

With regard to practical implementation, many questions remain. The European Commission will define in a subsequent delegated act the circumstances for reporting and the format and procedures will be set via implementing acts. At the same time, Member States can also provide guidelines. The text of the Directive should be as clear as possible to ensure that compliance is realistically possible, and that requirements are consistent across the Member States. For example, real time or unduly hasty notification before the consequences of a breach could even be investigated and determined would not help remediation at all, may even create unnecessary concern or panic, and should therefore be avoided.

It should also be noted that many cybersecurity incidents do not actually involve the breach of systems belonging to the victim organisation. For example, the widely-publicised Denial of Service attacks against US banks have not breached their systems, but rather prevented access to them. Similarly, fraudsters often do not target banking systems, but rather the customers' systems. It is unclear how the mandatory reporting would be applied in these circumstances, or whether it should even be applicable in all of these cases, hence our insistence on focusing the reporting requirements on incidents that significantly impact the integrity or continuity of the market operator's core services.

Moreover, the notification requirement must be consistent with – and must not duplicate – other notification schemes that already exist or will be created (e.g. Telecom Framework, e-Privacy Directives, General Data Protection Regulation, Digital Trust Services Regulation).

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu – www.amchameu.eu

- **The competent body**

As for which body or authority should be the prime recipient of breach notices, AmCham EU warns of the risk of Member States inconsistently appointing a broad variety or even several competent authorities. AmCham EU insists on the importance for compliant organisations to be faced with straightforward and clear administrative procedures, as much as possible through one-stop-shops, as explained in section about jurisdiction and applicable law. This would help streamline a potentially overly burdensome and complex process that otherwise could eventually defeat the purpose of the initiative.

Suggested solutions

To address the concerns raised above, AmCham EU recommends:

- Introducing an explicit reference to the technology neutrality principle, stressing the importance of not imposing any product design requirements;

- Clarifying in Article 14 that incident reporting requirements should only apply to incidents significantly affecting the integrity and continuity of market operators' core services, to help incident remediation and prevent further incidents, and that it should not lead to disclosing or otherwise exposing vulnerabilities, in any case not before they have been comprehensively patched across the ecosystem;

- Ensuring that the incident notification requirement is compatible with other existing and potentially applicable breach reporting regimes, as rightly suggested in Recital 31; and

- Making sure that the landscape of competent authorities across Member States is consistent so that compliance is equally straightforward for all market operators.

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu – www.amchameu.eu

Enforcement powers and audits

Analysis

- **Greater focus is needed on effective coordination between Member States**

AmCham EU welcomes the development of national NIS strategies as a means of increasing levels of network and information security across the EU. Given the national security prerogatives of the Member States, we understand the choice of a Directive as the legal instrument for achieving convergence in NIS. However, Member States will need to remain vigilant to ensure that the minimum harmonisation principle does not lead to inconsistent or conflicting approaches to the supervision of market operators operating in more than one Member State.

Inconsistency is possible at multiple levels, including in the definition of the roles and responsibilities of actors (Article 5(2)b), and cooperation mechanisms between the public and private sectors (Article 5(1)c). Greater emphasis needs to be placed on coordination of national NIS strategies via the cooperation network, to pre-empt inconsistency and to resolve conflicts of supervision should they arise. Market operators need certainty as to which supervisory authority has competence to give them instructions (see earlier comments in section 2).

- **Greater involvement of market operators is needed in all information sharing processes**

The text is not clear about the exact involvement of market operators within the cooperation network (Article 8), the early warning mechanism (Article 10), the co-ordinated response process (Article 11), the Union NIS cooperation plan (Article 12), or the international cooperation procedures (Article 13).

Recital 15 offers the important insight that:

> As most network and information systems are privately operated, cooperation between the public and private sector is essential… Market operators… should… cooperate with the public sector and share information and best practices in exchange of operational support in case of incidents.

Carefully crafted information sharing procedures involving the public and private sector will be critical in developing a culture of risk management. The trust needed to make this work cannot be mandated. Information sharing should be as far as possible voluntary, bi-directional,

and restricted to stakeholders that meet minimum security requirements. Market operators should not be obliged to share information, for example under a national NIS strategy or legislation, unless there are sufficient guarantees that the information shared will not be misused. A greater role is, in particular, needed for market operators alongside ENISA within the procedures for developing delegated and implementing acts, which touch on matters that fundamentally affect market operators.

- **Supervision by Member States should never dictate the design of a product or service**

Under Article 15(2), competent authorities can issue 'binding instructions' to public administrations and market operators. This appears difficult to reconcile with Recital 25 which states that 'technical and organisational measures imposed on public administrations and market operators should not require that a particular… technology product be designed, developed or manufactured in a particular manner.' NIS is very broad and can capture many types of incidents, the causes, frequency and nature of which vary according to the different types of infrastructures and services concerned, and their unique risk profiles. There is no one size fits-all approach. Market operators by definition are best placed to know how to appropriately protect their network and services. Therefore greater clarity is needed over the scope of binding instructions that can be issued to market operators, and ensure that such instruction will not be technology specific or interfere with product design.

- **The conditions permitting an investigation by a competent authority need clarification**

Article 15 hands Member States the powers to investigate 'cases of non-compliance' with the security and incident reporting requirements of Article 14. This formulation provides no safeguards for market operators on the due process to be followed, neither does it define the threshold of evidence needed to trigger what could be a highly intrusive investigation. As currently drafted, this power is too broadly framed and leaves market operators open to the discretionary intervention of 27 different authorities.

- **The information requirements under Article 15(2)(a) are too broad**

As currently formulated, this Article could allow any competent authority to request any information it considers necessary to assess the security of information systems. There is no balancing requirement that regulates, for example, the protection of intellectual property or other commercially sensitive data. Market operators would only have a right to judicial redress after the fact.

- **Audit requirements under Article 15(2)(b) are too broad**

Member States may unilaterally require a market operator to undergo a 'security audit' carried out by a 'qualified independent body' or national authority. These powers are exceptionally broadly framed and offer little protection for market operators, and raise a number of concerns. The conditions that might justify and trigger an audit are not defined. The scope of 'security audit' is not clear and the definition of a 'qualified independent body' is also vague. As a result market operators could be obliged to open up their commercially sensitive information to a broad range of stakeholders at the discretion of any competent authority. Moreover, promoting an audit culture could weaken security by encouraging operators to adopt a checklist approach – implementing security to meet the audit as opposed to adopting the most appropriate security measures.

- **Exemption for micro-enterprises should be subject to a criticality test**

Security is a collective concern, and the size of a market operator does not necessarily bear any relation to the security risk it poses. Rather than a blanket exemption for micro-enterprises form the security and incident reporting requirements of Article 14, some form of criticality test should be applied to determine whether a micro enterprise should be exempt.

- **Divergence in national sanction-setting powers could distort the market**

Article 17 requires Member States to provide for 'effective, proportionate and dissuasive' sanctions. There is no requirement, however, for national sanctions to follow similar criteria or to be consistent with each other in any way. Nor is there apparently any form of judicial redress foreseen for sanctions applied under Article 17 – which is particularly problematic given the absence of objective criteria triggering the enforcement actions outlined in Article 15. This creates a significant risk for market operators in countries that apply stricter sanctions. Much greater emphasis should be placed on ensuring consistency between Member States provisions, and ideally, this could be achieved through maximum harmonisation for the part of the Directive that applies to market operators.

Suggested solutions

In order to avoid market barriers, Article 8(3)d should include a requirement for Member States to cooperate with each other in order

ensure consistency of transposition, implementation, supervision, enforcement and sanctions across borders.
Increased involvement of market operators should be foreseen both in the information sharing mechanism and in the definition of the delegated and implementing acts that will flesh out in practice the actual requirements applicable to them.

The provisions of Article 15 should define more accurately the circumstances in which national authorities exert investigation, information request and audit powers, and market operators should get reassurance that these powers will not be exerted disproportionately, unnecessarily or to the detriment of their services.

The *de minimis* clause exempting micro-enterprises should be tailored not according to the operator's size, but to the lack of criticality of its services.

Standards and market access

Analysis

- **Encouraging the use of standards is a laudable principle**

Caution is needed, as formal compliance to technical standards could be counter-productive. Indeed, technical standards take time to develop and cannot keep pace with the dynamic threat environment. Formal requirements would encourage a 'box ticking' compliance culture at odds with genuine risk management. It could even create a false sense of security, although compliance with even the most stringent technical standards may not be sufficient for effective risk management.

- **Flexibility over security standards is welcome**

AmCham EU welcomes the formulation of Article 14, whereby market operators are required to maintain a 'level of security appropriate to the risk presented'. Market operators are best placed to know how to protect their networks and services. Mandated technical standards create single points of failure and their relevance is heavily time bound. Similarly, the formulation of Article 16, which requires Member States to encourage rather than require adoption of security standards, provides needed flexibility. More formal recognition of the concept of equivalence – whereby a market operator can adopt any standard that delivers an equal or superior level of security, whether or not it features on a list drawn up under Article 16 – would help ensure that an EU-mandated standards list

can never become a barrier to market access or stand in the way of the deployment of more advanced security solutions.

- **The EU should always adopt global, market-driven standards**

Article 16 proposes a standardisation process in order to implement risk management requirements. The corresponding Recital 32 suggests that it may be necessary to draft harmonised standards to this end. Such standards are by their nature European as opposed to international. Given that standardisation in the cybersecurity space is an international process, and that bodies such as ISO and IETF have already developed many effective standards, it would be more appropriate to reference international standards.

This would also be consistent with the imperative for any new standards to build on international expertise. Moreover it would also avoid provide leverage to other countries or regions that have contemplated introducing local standards that hinder market access. At the same time, the concept of equivalence should also be introduced, so as to effectively allow the market to propose alternative, innovative, and the case being even superior approaches.

Suggested solutions

An explicit provision should be added in the articles of the Directive to:

- Require that referenced standards be international;
- Spell out the voluntary nature of standard adherence;
- Secure sufficient room for technological neutrality and innovation by granting market operators the possibility of demonstrating equivalency or superiority to established standards; and
- Acknowledge the international scale of the cybersecurity challenge and the market-driven nature of standardisation efforts, explicitly foresee the active involvement of market operators in the definition of standards and technical specifications.

Relation of the NIS Directive to the privacy framework

Analysis

- **Managing cyber risk, notifying incidents and exchanging information should happen lawfully under data protection law**

Addressing cybersecurity threats involves processing data and sharing information with competent authorities and among market operators, often across borders within the EU, as well as with stakeholders in third countries. Some data processed or exchanged in this context may qualify as personal. Recital 39 and Article 1 paragraph 6 rightly recognise that such processing and exchange should be viewed as lawful under the applicable data protection rules. Further discussion and fine-tuning of the proposed provisions may be needed to clarify what this means in practice. It will be important for market operators to fully understand the extent to which processing data for cyber risk management, incident reporting and information sharing purposes can be viewed as lawful under privacy rules, and how such processing can be accommodated and reconciled with the provisions of data protection law, notably with respect to data subject rights. It will be important to ensure that cybercriminals' privacy rights do not trump the ability of organisations to comply with the proposed Directive and to protect themselves from cyber threats.

- **Cyber incident reporting and personal data breach notification should be coordinated, but not confused**

Recital 31 suggests that where a cyber incident reported under the NIS Directive also constitutes a personal data breach to be reported under the e-privacy or the general data protection rules, the NIS authorities should exchange information with the data protection authorities. While certainly well-meaning, this is very worrisome because the liability for notifying personal data breaches under privacy rules rests with the so-called data controller (the notifying organisation), and not with any third party or intermediary (such as the NIS authority). This is especially important as the draft General Data Protection Regulation includes heavy sanctions for non-compliance with notification requirements. Although we welcome the aim of Recital 31 to harmonise and streamline single notification templates both for security incidents and for data breaches, further clarity is needed to ensure that information on data breaches is not exchanged, even between authorities, outside the control or knowledge of the data controller concerned.

- **Reassurance must be given to organisations that complying with security incident reporting under the NIS directive does not expose them *ipso facto* to sanctions under privacy rules**

Article 17 paragraph 2 suggests that where a security incident happens that involves personal data, sanctions should be imposed as a matter of course, and they should be consistent with the privacy sanctions foreseen in data protection law. This is unhelpful in many respects. It clearly

POSITION STATEMENT

disincentivises the reporting of security incidents and suggests that falling victim to a cyber incident involving personal data is in itself a cause for sanction, even though this is not foreseen as a grounds for sanction in the Regulation itself. It also opens the door to multiple sanctions in breach of the fundamental *ne bis in idem* principle by implying not only that 'cybersecurity sanctions' should be consistent with 'privacy sanctions' (i.e. potentially very heavy), but that the two could even be cumulatively imposed. If this provision stays as is, it risks completely undermining the whole principle of incident reporting, as no organisation would be willing – or could be forced – to 'testify against itself' by reporting an incident that would inevitably lead to a sanction being imposed.

Surely the objective is not to create what can only be described as a 'sanction for compliance', whereas the purpose of sanctions should precisely be to punish non-compliance. AmCham EU assumes that what is meant is that in case where demonstrated non-compliance with NIS requirements has contributed to a personal data breach, then the sanction for non-compliance should be as dissuasive as foreseen under data protection rules. This needs to be clarified in the Article, including by spelling out the *ne bis in idem* principle, i.e. the same event should not be sanctioned twice, once on NIS grounds, and once on privacy grounds.

Suggested solutions

To address the concerns described above, AmCham EU recommends:

- Extending the recognition of the lawfulness of processing personal data to the extent strictly necessary to comply with the NIS directive from information sharing and incident reporting also to cyber risk management itself;

- Specifying that where such data processing takes place, those provisions of privacy law, notably in relation to data subjects' rights, which could compromise the effective ability of organisations to implement robust cybersecurity, should not apply;

- Clarifying that in the context of incident reporting, the consistency sought between cybersecurity breach notifications and personal data breach notifications should not lead to NIS authorities either substituting themselves for data controllers in their relations and liabilities towards data protection authorities, or otherwise interfering with these relations; and

POSITION STATEMENT

- Rewording Article 17 paragraph 2 so as to avoid the creation of a systematic 'sanction for compliance' each time a security incident is reported which also involves the breach of personal data.

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate U.S. investment in Europe totaled €1.7 trillion in 2010 and directly supports more than 4.2 million jobs in Europe.

* * *

POSITION STATEMENT

American Chamber of Commerce to the European Union – Avenue des Arts/Kunstlaan 53, B-1000 Brussels, Belgium
Telephone 32-2-513 68 92 – Fax 32-2-513 79 28 – info@amchameu.eu – www.amchameu.eu