EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Sustainable and Secure Society
Trust and Security

NOTE TO THE FILE

Subject: NIS Public-Private Platform – Draft issues paper

The following outline is provided as a scene setter and input in view of the first plenary meeting of the NIS Public-Private Platform on 17 June 2013. The final scope of work and the organisation of the Platform will be discussed and agreed upon together with the Platform participants at the first plenary meeting.

1. MISSION AND OBJECTIVES

The establishment of the NIS Public-Private Platform was announced in the Cybersecurity Strategy of the European Union[1].

The Strategy "*calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions*". The Platform is tasked to develop "*incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally*".

As a first objective, the Platform will focus on fostering the adoption of effective risk management practices. Businesses and public administrations are often unaware of the actual level of cybersecurity risks they face. Many of them rely solely on deploying basic ICT security solutions, an approach that has been repeatedly proved to be inadequate. Meanwhile, even though there is a sense of growing concern, as evidenced for example by the nascent 'cyber insurance' sector, this has not necessarily led to an increase in cybersecurity performance, which ultimately requires organisational and procedural changes. For example, according to Eurostat, as of January 2012, only 26 % of enterprises in the EU-27 had a formally defined ICT security policy with a plan for regular review.

Businesses and public administrations need to invest in NIS to protect their key assets and ensure the continuity of the services they provide. As a starting point, they should implement proper risk management processes, including dynamic risk assessment and risk mitigation, but also participate in the exchange of information on threats and vulnerabilities while recognising the potential benefit of collaboration in incident

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/01 final.

response. These practices are essential safeguards to cope with a rapidly evolving threat and technology landscape. The adoption of risk management processes will largely determine the development and the adoption of secure ICT solutions.

The findings of the Platform on risk management will help companies and public administrations to increase their preparedness and cooperate more effectively, thereby enhancing cyber resilience in the EU. They will feed into Commission recommendations on cybersecurity to be adopted in 2014.

The NIS Platform will complement and underpin the proposed NIS Directive. In particular, through best practices identification, it will help the relevant companies and public administrations implement in a consistent manner the general risk management and incident reporting obligations proposed under the Directive. It will also feed in the process leading to the development of the implementing measures set out in the proposal, for example by helping simplify the reporting process.

In addition, the NIS platform is expected to provide input to the secure ICT Research & Innovation agenda at national and EU level, including H2020.

2. SCOPE OF WORK

The NIS platform will as a matter of priority aim to:

1. Identify and facilitate the up-take of risk management practices, including standards, to enhance cybersecurity; such practices should be process-related and technology-neutral;

2. Develop incentives to adopt the identified practices.

The Platform may focus on the following areas:

- Organisational measures: practices to define, guide or evaluate an organisation's cybersecurity, specifically its capability to identify, assess and mitigate cybersecurity risks, and to deter and handle incidents;

- Secure products and services: practices to demonstrate the ability of products or services to provide a "good" level of cybersecurity performance as part of the ICT value chain;

- Metrics, measurement and language / taxonomy for cyber risk: practices for measuring, describing and evaluating cyber risks, impacts, threats, controls, etc.

- Information exchange: practices for the exchange of cyber incident information, to allow cyber incident reports to be understood and acted upon in the framework of complex cooperation schemes; to facilitate a high level view of all cyber incidents which facilitates spotting trends and directing resources;

- Cybersecurity resources: practices to manage and develop cybersecurity knowledge, skills and resources within an organisation or a sector.

The Platform should take into account all types of threats, be they accidental or intentional. It should seek to promote actionable practices, based as far as possible on

internationally recognised best practices and standards and addressing the dynamic nature of cybersecurity risks.

The Platform will have to consider a number of questions in relation to the identification and the implementation of risk management practices, including:

- Whether a sector by sector and/or a horizontal approach should be followed when identifying such practices; while some practices may apply across sectors, others may prove relevant only in certain sectors, due to sector specificities or criticality;

- How to ensure a high level of cybersecurity in complex value chains and ecosystems, encompassing many interconnected players and strongly interlinked information systems;

- How to remove the barriers to the adoption of risk management practices and help less advanced stakeholders to progressively increase their level of NIS; whether the use of a Capability Maturity Model, guiding entities to progressively improve their risk management processes, would prove useful in this regard;

- How to raise awareness and obtain C-level engagement;

- Whether minimum security requirements could be identified to help companies and administrations counter basic threats, on which a large part of successful breaches are based, while serving as a basis to progressively implement more sophisticated risk management practices;

- How to build innovation in risk management to be able to cope with the changing nature of threats and permanent technological evolutions;

- Whether cybersecurity risk management should be addressed as a standalone function or as part of business risk management/business continuity and what should be the interplay between the business and cyber risk management frameworks;

The NIS Platform will in parallel discuss economic, legal and technological incentives which could be set at EU, national or sectorial level to adopt risk management practices and adopt secure ICT solutions. Incentives are warranted to motivate the decision of businesses and administrations to improve their cybersecurity capabilities beyond immediate business and operational considerations. This is important to increase the overall level of cybersecurity in a fully interconnected world and serve the public interest. Importantly, by contributing to creating stable and harmonised demand for secure ICT solutions and risk mitigating technologies, incentives for end-users will also foster R&D investment and innovation by ICT suppliers.

In the EU Cybersecurity Strategy, the Commission calls upon governments and private sector to develop incentives, such as:

- Developing security labels or kite marks to enable informed purchasing while facilitating companies with a good cybersecurity performance to make it a selling point;

- Leveraging public procurement schemes to stimulate the development and deployment of security features in ICT products and services;

- Developing harmonised metrics for calculating insurance risk premiums;

- Making CEOs and boards more accountable for ensuring cybersecurity.

Other incentives that could be considered by the Platform are:

- Liability reduction and/or safe harbour protection in cases where an adequate level of cybersecurity performance is demonstrated, for example based on (certified) implementation of best practices; conversely increased liability could be the consequences of poor cybersecurity performance;

- Tax incentives in cases where an adequate level of cybersecurity performance is demonstrated;

- The use of public funding to foster risk management and the adoption of secure ICT solutions, for example by making certain public grants or loans conditional on the adoption of adequate cybersecurity measures by beneficiaries;

- Fostering the development of cybersecurity insurance schemes, for example through tax incentives, transfer of risk to public authorities for low-probability high-impact events, providing reinsurance to cyber insurance companies; cyber insurance could be a useful vehicle to improve cybersecurity performance of insured entities by linking the insurance premium to the implementation of risk management best practices;

- The participation in information sharing platforms, where participants are able to share up-to-date information on threats and vulnerabilities;

The Platform should assess the requirements to implement such incentives, including whether they would require new legislation at EU or Member State level, discuss their benefits, cost-effectiveness and the barriers to their implementation.

3. ORGANISATION OF THE NIS PLATFORM

The NIS Platform will be an inclusive and multi-stakeholder endeavour. The objective is to mobilise goodwill and energies to deliver increased cybersecurity in Europe.

The NIS Platform will be structured between:

- Plenary meetings, composed of senior government and company representatives, held 2 to 3 times a year and aimed at steering the work of the Platform and validating the output of the working groups or taskforces

- Thematic working groups or taskforces composed of experts, meeting on a regular basis to conduct technical discussions and produce draft consensus papers.

The Commission has called the first plenary meeting of the NIS platform on 17 June 2013. The main objective of this meeting will be to decide together with the Platform members on the precise scope of the activities and a roadmap setting out milestones and deliverables. 2 additional plenary meetings are envisaged before the Platform delivers its first output, to be integrated in the 2014 Commission recommendations on cybersecurity:

- An intermediary plenary meeting in Q4 2013 to follow up and steer the work of the Platform;

- A meeting in H1 2014 to agree on the first deliverables.

The Platform will have to produce results fairly quickly. At the first meeting it will be important to create a sense of urgency. The Platform will continue to operate after it has delivered this first output and the work programme will have to incorporate both short-term and longer-term objectives and milestones. The work programme will be regularly updated during plenary meetings, as part of the steering of the Platform.

The bulk of the work of the platform will take place in the working groups, which will meet on a regular basis to conduct technical discussions and provide draft consensus papers on specific topics. Such meetings and the work of the groups could be organised essentially in a remote or virtual way (with secure portal and teleconference facilities provided by the Commission and/or ENISA) in order to ensure swift delivery. The working groups will start working as soon as possible after the first plenary meeting, with a view to provide the first draft deliverables in early 2014. The precise organisation of the working groups and their individual scope will depend on the agreed scope of work.

Work in the Platform will be carried out with the following principles in mind:

- Be results-oriented and focused on impact. The objective is to improve the level of cybersecurity in Europe; metrics of success and measures of impact will be defined;

- Be of value to the stakeholders. The main objective of the Platform is to help companies and public administrations to increase their level of preparedness and to cooperate more effectively. For that reason, participants should not only carry out but also steer the work of the Platform;

- Follow a bottom-up approach involving practitioners, in order to make progress on operational issues;

- Adopt a deadline-driven approach, where working groups are asked to deliver specific deliverables in a short timescale;

- Ensure active participation and continuity in the participation, in order to build trust and ensure progress in the work of the Platform;

- Confidentiality rules and supporting tools (e.g. secure platform to share documents) will be implemented as appropriate;

The Commission and ENISA will organise the coordination of the Platform with similar and related initiatives in the field of cybersecurity, including standardisation, with a view to avoid duplication of work.

The Commission will manage Platform membership with a view to ensuring a balanced and manageable representation of the different stakeholders and to secure participation of the relevant stakeholders in the different working groups. New participants could be accepted or called to participate after the first plenary meeting.

Membership in the working groups will be voluntary. It will be validated by the Commission on the basis of individual expression of interest from Platform members. Working groups will be kept small and closed after they have been set up to allow for swift progress. Input from non-Platform members will be sought as appropriate.

The outputs of the Platform and regular progress reports will be made publicly available to ensure appropriate dissemination of the work of the Platform and allow entities not directly involved in the work of the Platform, including political bodies and the general public, to follow closely its activities.