



EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology

Sustainable and Secure Society
Trust and Security

Brussels,
CNECT H4/

NOTE TO THE FILE

Subject: Minutes of the first plenary meeting of the Network and Information Security (NIS) Public-private Platform

The first plenary meeting of the NIS Public-Private Platform took place in Brussels on 17 June 2013. A list of participants is attached as an annex.

1. INTRODUCTION

Paul Timmers, Director of DG CONNECT Directorate H, Sustainable and Secure Society, outlined the scope and purpose of the meeting. He welcomed the wide participation, with more than 130 individual companies and public administrations represented and insisted on the need for increased cooperation to improve cybersecurity. He reminded of the importance of the NIS Platform as a key action of the EU Cybersecurity Strategy and remarked the need to align the work of the Platform with the implementation of the NIS Directive. The work of the Platform will have to remain focused, which will be done by ensuring prioritisation.

Evangelos Ouzounis, Head of ENISA Unit on Secure Infrastructure and Services, gave a presentation on public-private cooperation in the NIS area. He described the key factors of success, including trusted information sharing and the need for clear objectives and well-defined themes. In his view, this calls for the establishment of small and focused thematic working groups.

Giuseppe Abbamonte, Head of DG CONNECT Unit H4, Trust and Security, presented the NIS Platform and the related draft issues paper. He stated that the NIS Platform is complementing and underpinning the NIS Directive. It will help implement the measures set out in the Directive, e.g. by simplifying incident reporting, and ensure its convergent and harmonised application across the EU. On top of that, the NIS platform is expected to provide input to the secure ICT R&I agenda. Mr Abbamonte stressed the need to align the work of the NIS Platform with ongoing work in the US, following President Obama's Executive Order on improving critical infrastructure cybersecurity.

Mr Abbamonte guided the participants through the meeting's agenda. He gave an overview of the Platform schedule, including the establishment of thematic working groups shortly after the first plenary meeting, the definition of terms of reference for each working group, the presentation of a progress report at the next plenary meeting in the autumn, and the delivery of a first output in the first half of 2014. The NIS platform will then continue working towards new objectives. The Platform is being set up with an indefinite duration.

2. MORNING SESSIONS: OBJECTIVES AND SCOPE OF WORK OF THE NIS PLATFORM

The morning sessions were dedicated to discussing the objectives and the scope of work of the NIS Platform. The participants made the following comments:

- Many participants pointed to the existence of a complete body of standards covering the envisaged scope of work. Such standards exist at national, European and international level. The Platform should produce guidance in line with these standards. Some participants supported alignment with EU standards, while others insisted on the need to follow international rather than EU-specific standards. Other participants underlined that their organisations comply with national standards and the NIS Platform should also cover these standards.
- Several participants stressed the need for the activities of the Platform to be well-focused. Some participants suggested to first "get the basics right", building on existing practices and standards. Some stressed that what is set out in the issues paper is quite broad and should be narrowed down. One participant however warned against mere compliance with minimum standards, which is not necessarily leading to appropriate focus on the actual risks.
- Many participants underlined the need to link the work taking place in other contexts, including standardisation organisations, national PPPs, activities carried out in third countries (India, Japan, etc.) and international organisations (e.g. NATO) and work undertaken by other bodies (e.g. ENISA) and Commission services (e.g. DG HOME, DG MOVE). The expertise already acquired should be used, e.g. the work led by ENISA in the context of the implementation of Art. 13a of the EU Framework Directive for electronic communications in the telecom sector.
- A number of participants underlined that the NIS Platform should follow a voluntary approach and be separate from the implementation of the NIS Directive, which is still going through the legislative process. They stressed that the output of the Platform should not necessarily lead to regulation, because satisfactory outcomes can also be achieved voluntarily. In general, it should be up to the participants to decide how to implement the best practices identified. Participants also underlined that information exchange in the cybersecurity domain has a wider scope than what is laid down in the NIS Directive.
- A number of participants claimed that the NIS Platform should not only address process-related issues, but also technical issues (e.g. securing DNS or routing systems) and support the development of the appropriate technological input to increase cyber resilience. They stressed the need to support R&D and to liaise with standardisation organisations to address technology standards. One participant mentioned the example of NIST, which is engaged in detailed technical work. Another participant suggested that the work of the Platform should not discourage the adoption of open source technologies, e.g. when promoting kite marks and should take into account of the interest and needs of SMEs and micro companies.
- Many participants supported a strong focus on R&D. One participant mentioned that a key question is how to use cybersecurity building blocks and integrate them into existing systems.
- On risk management, participants underlined the need to develop common practices between industry, government and the EU, but also across the supply chain. One

participant claimed that this is where the issue lies and collaboration is therefore of the essence. Many participants asked to focus on awareness and education, in particular on board-level awareness. Several participants stressed that security requirements should be economically sustainable and allow a level playing field.

- On the question as to whether the Platform should adopt a sector-specific or a horizontal (cross-sector) approach, views were divided. Some participants claimed that the Platform should adopt a sector-specific approach to address the specific cyber security issues encountered in different sectors. Others supported a horizontal approach, at least as a first step. According to those participants, sector-specific guidance would be too difficult to devise in a horizontal Platform, while there is scope for horizontal guidance in the first place.

Mr Abbamonte clarified that the work of the Platform should be as operational as possible. It should follow a bottom-up approach, with participants in the driving seat. As stated in the issues paper, the work should draw from international standards and best practices. Standard organisations should participate in the Platform and their work should feed into the process. However, the activities of the Platform should remain technology neutral, in line with the NIS Directive. The priority will be supporting the implementation of the NIS Directive. The Platform should further help steer the R&I agenda. Mr Abbamonte clarified that there will be no imposition of standards. Adopting identified best practices is in the interest of all stakeholders.

Mr Timmers concurred that we need to be efficient and coordinate the work of the NIS Platform with other related processes. The NIS Platform should first set its own priorities and then broaden the agenda at a later stage.

3. AFTERNOON SESSIONS: ORGANISATION OF THE NIS PLATFORM

Joanne Miller, Department for Business, Innovation and Skills (BIS), UK Government, gave a presentation on organisational measures to improve cyber security in the UK. The UK government follows a voluntary and cross-sector approach to i) raise industry awareness, ii) identify and promote organisational standards to protect against low level threats and iii) share information.

Mr Abbamonte opened the session on the organisation of the working groups by reaffirming that the first priority of the NIS Platform will be to support the implementation of the NIS Directive. The NIS Platform will share the same objective as the Strategy and the Directive, i.e. to foster the resilience of the networks and information systems which underpin the services provided by market operators and public administrations. An ancillary objective is to ensure confidentiality and the protection of personal data. He clarified that the Platform should concentrate on the sectors covered by the Directive, including public administrations.

Following discussion on the organisation of the work, Mr Abbamonte proposed to set up 3 working groups following the various suggestions of the participants:

- WG1 on risk management, including information assurance, risks metrics and awareness raising;
- WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
- WG3 on secure ICT research and innovation.

Mr Abbamonte clarified that the working groups should be cross-cutting, with all relevant sectors represented. Sectors which are less advanced in terms of preparedness will draw from the experience of more advanced sectors. The working groups will seek to identify cross cutting / horizontal best practices. If relevant, sector-specific work could be undertaken at a later stage. Incentives will be addressed in each working group. Secure product and services, included in the draft issues paper for the NIS platform, will be addressed at a later stage.

In terms of the organisation of the working groups, there was a strong call from participants to leave participation open to the members of the Platform rather than be limited in size. Several participants stated that this would allow wide participation, while in effect only a limited number of participants will be contributing to the drafting process. Mr Abbamonte agreed with these suggestions. He clarified that the Commission and ENISA will participate in the working groups and provide support, but will not chair them.

There was consensus on appointing 2 chairpersons (one from the public and one from the private sector) per working group. The question of the selection of the chair persons (by the Commission vs. by the working groups) remains open. The essential role of the chairperson to steer the work and ensure delivery was stressed by several participants.

Mr Abbamonte said he supported double chairmanship and would get back in writing on the selection process of the chair persons.

4. NEXT STEPS

The Commission will launch a call for expression of interest as soon as possible for each working group. As a first task, each working group will be asked to develop and agree on the terms of reference defining the working group's objectives, scope of work and organisation modalities.

The next plenary meeting of the Platform will take place in autumn. On that occasion, each working group will provide a progress report to the plenary. The working groups will actively seek the input of the plenary. Working groups are expected to conclude their work and provide recommendations in the first half of 2014. A third plenary meeting of the platform will take place in the first half of 2014. Future work priorities will be discussed in the next plenary meetings.