

## Long term recommendations

### Background

The Management Board of the European Network and Information Security Agency (ENISA) is required by the Regulation establishing the Agency (ref) to issue recommendations on appropriate changes to the Regulation. Paragraph 3 of Article 25 states:

“The Management Board shall receive a report on the evaluation and issue recommendations regarding eventual appropriate changes to this Regulation to the Commission. Both the evaluation findings and the Recommendations shall be forwarded by the Commission to the European Parliament and the Council and shall be made public”

The Management Board received the findings of a review of the Agency in January 2007. This review was conducted by IDC and was initiated by the EU Commission. At its Board meeting of 26 January 2007, the Board were able to discuss the recommendations of IDC with representatives of the company's review team.

### The Board's views

The Board reflected on the findings of the IDC report and concluded that :-

- The subject of network and information security was of increasing importance;
- The Agency had achieved a great deal;
- There was a clear lack of clarity among stakeholders about the Agency's role and differing expectations about its contribution;
- There were issues about the way that Regulation might have limited the ability of the Agency to respond and apply its resources in a way best suited to meet its remit;
- The Board and Agency management should address the short terms issues to maximise the contribution the Agency could make within the terms and time period of its current mandate;
- On the basis of this analysis, the Board would produce the Recommendations on appropriate changes to the Regulation as required by Article 25.

### Recommendations

Our recommendations are set out below as responses to the key questions on the future of the Agency.

#### *Should the Agency's mandate be extended ?*

The Board considered three alternative approaches;

- Do not continue with an Agency;
- Continue on the basis of the current Regulation;
- Continue on the basis of a revised Regulation.

#### Do not continue with an Agency

While there were continuing challenges for the Agency, the Board believed that Agency's subject area was of critical importance to the wider European Agenda for the information society.

The Board believed that this fundamental review had occurred early in the life of the Agency and, while the review's findings had value in acting as a reality check on progress to date, it would be imprudent on the basis of the evidence gathered to conclude that the Agency had not merited the resources that the Community had devoted to it. The Board therefore concluded that ENISA could not at this stage be regarded as having failed in any significant way.

Nevertheless, the Board could not conclude that, because the subject matter was important, it must of necessity be addressed by means of an European Agency.

Continue on the basis of the current Regulation

The Board concluded that the years since the passage of the Regulation had allowed certain aspects of the legislation to be assessed critically in the light of experience. In particular, there were issues around the tasks of the Agency, the organisation and resources that need to be looked at afresh. These questions form the basis of several recommendations below.

Continue on the basis of a revised Regulation

The Board therefore had to conclude that the way forward was to extend the mandate of the Agency and revise the Regulation. While acknowledging the difficulties of drafting new legislation, the Board consider that, given the importance of the Agency to the delivery of the political agenda of the EU being a leader in the communications and information areas, there is a clear need to ensure that appropriate legislation is in place to enable the Agency to deliver appropriate solutions in a timely and effective manner. The Board had divergent views on whether the mandate should be time limited. Some argued that we should have sufficient confidence in the importance of the subject matter and the long-term planning needs of the Agency to proceed sine die – that is to remove Article 27 from the Regulation - but others saw value in maintaining a time limited mandate that would compel a fundamental analysis of the need for the Agency. There was consensus that – whatever decision was reached on the life of the Agency – there would be continued value in a review process as embodied in Article 25 of the current Regulation. This review period should be set at a minimum of five years from the start of the revised mandate of the Agency.

### **Recommendation 1**

**The Regulation should be revised to extend the mandate. That mandate should again have a review point.**

*What should the legislation say about the scope and activities of the Agency ?*

In many ways, this was the key question. The current Regulation approaches the operating environment of the Agency from three angles: Article 1 deals with scope, Article 2 deals with the Objectives and Article 3 deals with the tasks.

The Board concluded that the scope of the Agency was appropriate (although some felt the language of Article 1 could be improved). The goal remained to develop a cultural change that would deliver high and effective network and information security.

The Board did, however, feel that the objectives and tasks in Articles 2 and 3 should be reconsidered in the light of experience. In particular, it was felt that the tasks were too tightly defined and reflected the concern that many Member States felt at the time that ENISA should not become an operational centre for European Networks. The upshot of this tight definition of tasks has been to almost demand compartmentalised thinking within the Agency to be seen as making progress against all of the 11 tasks in Article 3.

The Board concluded that the Agency had to become more focused on impacts and less task-oriented. The language of Article 3 therefore was limiting and constrained the ability of the Agency to take a holistic view of how best to deliver outcomes. The Board believed that, as the Agency matured, the process of identifying strategic issues and applying the appropriate resources to address them would become embedded. This would also remove the need for tightly defined tasks in the legislation.

The solution would be to look again at Article 2 to build on the present language to more clearly define the outcomes that we would like to see the Agency achieve in the period of its second mandate. One issue that needs to be addressed is the need for the Agency to respond to requests for advice and assistance. This appears in Article 2.2 and Article 3(b) and the process is further defined at Article 10. The Board's experience is that it is difficult to allocate resources to requests that emerge in year and it is not clear from the Regulation on what basis such requests should be met or rejected. Solutions have been developed – and the Board believes that the Agency should be open to suggestions from other stakeholders - but that such a revision of the Regulation would allow this to be put on a sounder basis. The Board believes that requests should always meet the following criteria:-

- They should clearly fall within the Agency's stated aims and priorities;
- They should be submitted in time to allow them to be taken forward in the following year's work programme (except for the rare circumstance of something being time critical);
- They should benefit Europe as a whole or, as a minimum, more than one Member State.

In addition, requests could be accepted if they meet the following criteria:

- They should contribute to the European Institutions' agenda for the information society (such as requests from the Commission to support legislative or administrative developments); and/or
- They should provide opportunities for the Agency to participate in the practical implementation of guidance it has issued.

#### **Recommendation 2**

**The scope of Agency should not be materially changed.**

#### **Recommendation 3**

**The Regulation should be revised to combine Articles 2 and 3 to set outcome-based key objectives that are realistic and within the scope of the Agency.**

#### **Recommendation 4**

**The Agency should maintain the capability to respond to specific requests for advice and assistance but the nature of these requests and the process for receiving and considering them should be more clearly stated in the Regulation.**

*Should the Governance Structure of the Agency be revised ?*

The Regulation defines clear roles for the Management Board (Article 6), the Executive Director (Article 7), the Permanent Stakeholders' Group (Article 8) and the Working Groups (Article 7.8).

The Board believes that the roles of the Management Board and the Agency are - rightly - in line with those of other Agencies. The Board considered whether the participation of all Member States of the European Union on the Board made it unwieldy as a decision making body. This was not considered a real problem in practice.

The Board did note that there was a large cost associated with having such a large Board but considered that this was a reasonable outlay given the extent to which Board Membership encouraged active participation by Member States in the work of the Agency. The Board could, and has, appointed smaller groups of individual Board Members to carry out specific tasks and this provided opportunities to meet Board objectives more economically.

The Board also noted that the Permanent Stakeholders' Group (PSG) had attracted a high level of participation and this had been one of the successes of the Agency. The Board considered that it was crucial to the success of the Agency that it leverage the resources and expertise of private sector, public

sector, academic and NGO communities. It therefore concluded that the PSG should remain an integral part of the Agency and should represent a balanced cross-section of stakeholder representation.

In the light of IDC's recommendation that the Agency should appoint a high profile "ambassador", the Board concluded that the PSG should not necessarily be chaired by the Executive Director and that if a leading figure from the NIS community took over this role (or in the view of some Board Members, co-chair), it could add credibility and reach to the Agency. Moreover, the Regulation describes (in Article 8.5) that one of the roles of the PSG was "ensuring communication with the relevant stakeholders on all issues related to the work programme". The Board believes that this role should be developed to make the PSG a key two way channel of communication with the stakeholders to help both the Board and the Executive Director in meeting their responsibilities. This should enable a more flexible and effective approach to be taken to stakeholder engagement.

Subject to establishing the principles of impartiality and transparency, the Agency should be encouraged to approach stakeholder in a flexible way as possible – given that this is a technologically literate community. In this regard, we see no need for the Regulation to refer to Working Groups as the way that stakeholders are brought in should be a key aspect of the operation of the Agency and therefore within the discretion of the Executive Director.

#### **Recommendation 5**

**The governance structure of a Management Board, Executive Director and Permanent Stakeholders' Group should not be changed.**

#### **Recommendation 6**

**The Executive Director should be required to appoint – in consultation with the Management Board - a stakeholder to chair the Permanent Stakeholders' Group. In addition to its role in relation to the Work Programme, the Group should be more clearly tasked to contribute to the two way flow of ideas between the Agency (both Board and Executive Director) and the stakeholder community as well as encouraging the commitment of resource by the stakeholder community in support of the Agency's aims.**

*Are the resources of the Agency appropriate to its remit ?*

The Board noted the views of the Executive Director that the Agency needed more professional staff. It also noted with disappointment the high proportion of staff employed on back office functions and the public perception that this was a bureaucratic organisation.

The Board accepted that the high administrative overhead was primarily the result of the need to comply with Commission rules about the management of budgets and the delineation and separation of tasks in that

As part of its process of giving general orientations to the Agency, the Board has asked the Executive Director to put downward pressure on administrative costs - as far as compatible with financial propriety – in order to allow more resource to be devoted to professional staff. The Executive Director was also asked to look at how best to employ professional resources in a non-hierarchical and project oriented manner.

The Board noted the views of IDC that there was, given the high administrative overhead required by financial management rules, a minimum critical mass of around 100 staff. The Board foresaw that any increases in resources would add to the capability of the Agency through the employment of more professional staff. This was clearly an attractive proposition in investment terms. But the Board could not estimate the value for money in terms of additional resource.

Therefore, at this stage we are unable to make any recommendation to the legislators on the appropriate level of resources for an Agency operating under a revised mandate. The Board requested that the Executive Director prepare a business case for additional professional resources - calling on consultancy advice as appropriate - that demonstrates the real impact that could be realised in this way.

The Board would stand ready to comment on that business case by means of a Board Resolution to assist the legislators in their consideration of this point.

Version approved by the Board  
23 March 07