EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 501 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. NEED FOR ACTION

What is the problem and why is it a problem?

Digital technologies and the Internet are the backbones of EU economy and society. Critical economic sectors such as transport, energy, health or finance have become increasingly dependent on network and information systems to run their core businesses. The Internet of Things connects objects and people through communication networks. This new reality creates unprecedented opportunities and also vulnerabilities. Cyber incidents are indeed booming. Their complexity, frequency and the "surface" of their impact - from access to essential services to democratic processes - is set to increase still further.

In this context, the following interrelated problems have been identified:

- A fragmentation of policies and approaches to cybersecurity across Member States.
- Dispersed resources and approaches to cybersecurity of the EU institutions, agencies and bodies.
- An insufficient awareness of citizens and companies of cyber threats and insufficient information concerning the security properties of the ICT products and services they purchase, coupled with the growing emergence of multiple national and sectoral certification schemes.

These problems impact on the overall cyber resilience of the EU and the effective functioning of the internal market.

What should be achieved?

The specific policy objectives of the initiative are the following:

1. Increase capabilities and preparedness of Member States and businesses, in particular regarding critical infrastructures.
2. Improve cooperation and coordination across Member States and EU institutions, agencies and bodies.
3. Increase EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises.
4. Increase awareness of citizens and businesses on cybersecurity issues.
5. Increase the overall transparency of cybersecurity assurance of ICT products and services to strengthen trust in the digital single market and in digital innovation.
6. Avoid fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors.

What is the added value of action at the EU level?

As the digitalisation and interconnection of the economy and society has a global reach, the dimension of the problems goes well beyond the territory of a single Member State. This therefore requires an intervention at Union level. In the current context and looking at the

future scenarios, it appears that individual actions by Member States and a fragmented approach to cybersecurity, and especially its strong cross-border dimension, cannot increase the collective cyber-resilience of the Union.

B. SOLUTIONS

What are the various options to achieve the objectives? Is there a preferred option or not?

This Impact Assessment explores a specific set of policy options, covering the review of the European Union Agency for Network and Information Security (ENISA) and ICT security certification.

ENISA Review

Option 0 - Baseline scenario - This option is about the preservation of the status quo. ENISA's mandate would be extended and the objectives and tasks of the Agency would remain mostly unchanged, while taking into account the tasks entrusted to ENISA by subsequent EU law (e.g. the NIS Directive).

Option 1 - Expiry of ENISA mandate (terminating ENISA). This option would lead to the termination of ENISA at the end of its mandate (June 2020), and possibly to a redistribution of competences/activities at EU and/or national level.

Option 2 - **'Reformed ENISA'**. This option would build on the current mandate of ENISA with a view of adopting selective changes which take the evolution of the cybersecurity landscape into account. The Agency would gain a permanent mandate, based on the following key building blocks: support to EU policy development and implementation; capacity building; knowledge and information; market related tasks; research and innovation; and operational cooperation and crisis management.

Option 3 - EU cybersecurity agency with full operational capabilities. This option implies reforming ENISA by bringing together three main functions: 1. A policy/advisory function; 2. A centre of information and expertise, and 3. A Computer Emergency Response Team (CERT). To a large extent this option would imply the same change in the scope of the mandate as option 2. However, additional tasks would be added in the area of incident response and crisis management, so that the Agency would cover the entire cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.

Certification

Option 0 - Baseline scenario - Do-nothing. Under this option, the Commission would maintain the status- quo and not undertake any policy or legislative action.

Option 1 - Non-legislative ("soft law") measures. Under this option, the Commission would use soft policy instruments (e.g. interpretative communications, support of EU-wide self-regulatory initiatives and standardisation activities) in order to improve transparency and reduce fragmentation.

Option 2 - An EU legislative act to extend SOG-IS agreement to all Member States. Under this policy option, the Commission would propose a legislative act to legally extend the membership to all Member States.

Option 3 - An **EU general ICT security certification framework**. This option implies the establishment of a European ICT Security Certification Framework (including an Expert Group made up of national authorities) by building on existing ICT security certification schemes, as much as possible. In essence, the framework would enable the establishment of EU certification schemes that will be accepted across Member States.

The preferred option is a combination of Option 2 for ENISA and Option 3 for certification.

What are the different stakeholders? Who supports which option?

The vast majority of stakeholders across all categories (Member States, industry, EU institutions, research community) that took part in the consultations appear to welcome the preferred option as they favour the reinforcement of ENISA and the creation of a European ICT security certification framework.

In particular, there is consensus on the need to have (as a minimum) a well-functioning EU agency with a permanent mandate, which is adequately resourced and mandated to face the present and future cybersecurity challenges. There is also broad agreement amongst stakeholders on the creation of a voluntary, scalable European framework.

On the industry side, this solution for certification is supported by businesses which are already subject to certification requirements, and which would benefit from an EU-wide mechanism based on mutual recognition of certificates. It is also supported by SMEs, which would suffer the most if they already have to or would have to embark on different certification processes across Member States. Some Member States, in particular those with fewer resources, and some representatives from industry and EU institutions expressed positive views also regarding option 3 for ENISA.

C. IMPACTS OF THE PREFERRED OPTION

What are the benefits of the preferred option (if any, otherwise of main ones)?

Under the preferred option, the EU would have an agency, focused on providing support to Member States, EU institutions and businesses in areas where it would bring the most added value. These cover: support to NIS Directive implementation; policy development and implementation; information knowledge and awareness; research; operational cooperation and crisis; market. In particular, ENISA would support EU policy in the field of ICT security certification, by ensuring an administrative maintenance and technical management of a European ICT security certification framework. Such a framework will effectively put in place a set of rules on the governance of ICT security certification in the EU, which would promote a system of mutual recognition of certificates issued across Member States. The solution to combine these options is considered the most effective for the EU to reach the identified objectives of: increasing cybersecurity capabilities; preparedness; cooperation; awareness; transparency; and avoiding market fragmentation. This option is also the most coherent with policy priorities, as it is entrenched in the Cybersecurity Strategy and related policies (e.g. the NIS Directive), and the Digital Single Market Strategy. Furthermore, this option would reach the objectives through a reasonable employment of resources.

What are the costs of the preferred option (if any, otherwise of main ones)?

Despite gaining new roles, a 'Reformed ENISA' would remain an agile organisation. The required financial contribution from the EU budget would it be higher than is currently the case but still fairly below other agencies that also operate in critical areas.

The creation of a European ICT security certification framework would not imply additional, upfront costs for the industry (including SMEs). Rather, it would generate significant savings for those firms that already certify their products or are willing to carry out security certification, with beneficial effects on their competitiveness worldwide. On the other side, it would involve some budgetary commitments to ensure the maintenance of the Framework, which would be mainly provided by the 'Reformed ENISA' model, as far as technical and secretarial tasks are concerned.

Will there be a significant impact on national budgets and administration?

No. The costs associated to strengthening ENISA would mostly be borne by the EU budget, while Member States would still be able to provide voluntary financial contributions to the Agency. As for certification, the main impact on national budgets and administration would derive from setting up a certification authority, when appropriate.

Will there be other significant impacts?

No.

Proportionality?

The preferred option includes balanced measures, all deemed necessary to achieve the objectives at stake without imposing excessive burden on the relevant stakeholders. In this light, this initiative is deemed to comply with the principle of proportionality.

D. FOLLOW UP

When will the policy be reviewed?

It is now proposed that the first evaluation will take place five years after the entry into force of the legal instrument. The Commission will subsequently report to the European Parliament and the Council on its evaluation, accompanied where appropriate by a proposal for its review. Further evaluations will have to take place every five years.