Brussels, November 2018

BSA feedback on European Commission's "Proposal to create a cybersecurity competence network with a European Cybersecurity Research and Competence Centre"

BSA | The Software Alliance ("BSA"[1]), the leading advocate for the global software industry, welcomes the continued efforts of the European Commission to strengthen the EU's cyber resilience and shares its desire to advance cybersecurity research in Europe. The recent proposal to create an EU Cybersecurity Competence Network coupled with a European Cybersecurity Research and Competence Centre has many commendable goals. However, there are a few concerning elements; in particular, the provisions governing funding, procurement, and participation by both the public and private sector.

First, it is critical that the proposal allows for participation from those entities demonstrating the best expertise as well as placing all market players, regardless of their size and origin, on equal footing. The draft Regulation should clarify that all companies and experts, regardless of where they are established would be eligible to participate in the Cybersecurity Competence Community (Article 8.2, 8.3) and potentially receive funding, provided they agree to share the knowledge and development within the Union. Furthermore, to the extent the new Competence Centre will determine how Member States shall define their public procurement practices, we believe that participation should not be limited to companies on the basis of their geographical origins but should instead seek the most effective outcomes to develop and procure sound cybersecurity solutions.

Excellence in cybersecurity cannot be achieved solely at a local level. In pursuing security innovation, European and non-European stakeholders should work together, irrespective of country of origin, and use a technology-neutral approach to increase cybersecurity across the Internet ecosystem. Global companies look forward to actively contributing to this process and we respectfully request that all stakeholders, regardless of their nationality, be allowed the opportunity to participate in future discussions and research.

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the internationals marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*
BSA's members include: Adobe, Akamai, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

A “country-of-origin” approach to security would deprive Europeans of the best available security technologies as some of the best security researchers and products have been produced as the result of collaboration either across borders or nationalities. Coordination and collaboration between governments and the private sector from around the globe are key elements in achieving an effective approach to cybersecurity. All Member States, European and non-European stakeholders should work together to pursue security innovation. The supply chain for cybersecurity products and services as well as the cybersecurity talent pool are global and should remain global.

With regards to the governance of the Competence Centre, the draft legislation foresees that the decision-making process of the Governance Board shall be equally divided between the European Commission (holding 50% of the voting rights), and Member States who financially contribute to the Competence Centre. EU bodies and Member States who do not contribute financially to the Competence Centre will have no voting rights. It thus appears that not all Member States will have oversight responsibilities. It would instead grant only a handful of Member States the authority to shape funding, procurement, research and development decisions across the EU.

This is particularly problematic as technology development and government grant life cycles take several years. As the Competence Centre envisions funding National Coordination Centres, we fear that precluding certain Member States from receiving voting rights would mean that those Member States would be forced to implement requirements developed by only a fraction of Member States.

Also, it is unclear why the option referred to in the Impact Assessment (option 3, discarded at an early stage) to use an existing agency, (European Union Agency for Network and Information Security – (ENISA), the Research Executive Agency (REA) or the Innovations and Networks Executive Agency (INEA)) was not pursued as all of these agencies would be able to cover the aims and actions of the new Competence Centre. We believe that the European Commission’s Impact Assessment fails to explain why the suggested scope of the future Competence Centre falls beyond the mission and mandate of ENISA. If ENISA was chosen to run this new Competence Centre through a new administrative structure or unit, every Member State would enjoy equal voting rights.

Lastly, there should be an emphasis for both the Competence Centre, and the National Coordination Centres to elevate a focus on international standards, which encourages development towards global best practices and has the added benefit of elevating European innovation to compete not just in the EU, but globally.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.131