

Il Presidente

D 202098 02.10.2018

Ms Marietje SCHAAKE,
Member of the European Parliament
Altiero Spinelli Building, 08G253
European Parliament
Brussels

Dear Ms Schaaake,

Thank you very much for your letter of 6 July regarding the digital security risks for Members and staff of Parliament, especially in the context of the upcoming European elections.

I fully share your concerns. Let me assure you that Parliament has already taken important steps to mitigate these risks and will further increase its resilience and preparedness.

In particular, the Secretary-General has initiated a work stream of the Member States' cybersecurity authorities, which led to the publication of a Compendium on cybersecurity of election technology to be applied by electoral bodies of Member States during the 2019 European elections. Parliament will publish a brochure based on the Compendium for a wider audience and will carry out awareness raising events for Members, Political Groups, EU political parties and Member States' electoral bodies.

In co-operation with other EU Institutions, Parliament is also actively tackling the issue of fake news and disinformation.

As regards the risks linked to ICT equipment and services offered by certain providers, Parliament has carried out a detailed analysis of the legal framework for public procurement and will take all available measures to avoid buying equipment and services that may compromise Parliament's information security and integrity.

In order to enhance the digital security specifically during official missions, Parliament has already introduced a mandatory password protection of emails from portable devices and protection of webmail services with tokens. Hard disks of laptops and hybrid computers can be encrypted on request. The services organise regular cybersecurity trainings and awareness raising activities.

In addition, the responsible services of Parliament will implement the following measures:

- a 'hands-on' cybersecurity mission guide with tips on how to protect information before, during and after the mission;

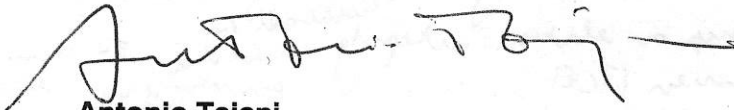
- tailor-made cybersecurity trainings for Members and staff travelling to specific countries. This course will present available protective solutions and could include a cybersecurity test;

- a mission feedback form for Members and staff to communicate any suspicious events during the mission not yet covered by the cybersecurity mission guide;

- an ICT equipment kit for every person going on mission to specific countries.

I hope that the information provided is useful for you. I will invite the services to continue and intensify measures to improve digital security.

With kind regards,



Antonio Tajani

Copie: Petras Austrevicius (ALDE)
Tunne Kelam (EPP)
Renate Weber (ALDE)
Liliana Rodrigues (S&D)
Dietmar Koster (S&D)
Helga Stevens (ECR)
Matthijs van Miltenburg (ALDE)
Laurentiu Rebega (ECR)
Godelieve Quisthoudt-Rowohl (EPP)
Clare Moody (S&D)
Nils Torvalds (ALDE)
Reinhard Butikofer (Greens/EFA)
Ramona Manescu (EPP)
Tibor Szanyi (S&D)
Patricia Lalonde (ALDE)
Hilde Vautmans (ALDE)
Gerben-Jan Gerbrandy (ALDE)
Pascal Durand (Greens/EFA)
Arndt Kohn (S&D)
Ramon Tremosa i Balcells (ALDE)
Indrek Tarand (Greens/EFA)
Anna Fotyga (ECR)
Julie Ward (S&D)
Sophie in 't Veld (ALDE)
Nathalie Griesbeck (ALDE)
Julia Reda (Greens)
Anna Maria Corazza Bildt (EPP)
Danuta Hubner (EPP)
Ivica Tolić (EPP)
Ana Gomes (S&D)
Bas Belder (ECR)
Neena Gill (S&D)
Eva Kaili (S&D)
Nadja Hirsch (ALDE)
Josef Weidenholzer (Greens)
Miapetra Kumpula-Natri (S&D)