



Council of the
European Union

006401/EU XXVI. GP
Eingelangt am 19/12/17

Brussels, 19 December 2017
(OR. en)

15901/17

INF 252
API 158

NOTE

From: General Secretariat of the Council
To: Working Party on Information
Subject: Public access to documents
- Confirmatory application No 31/c/01/17

Delegations will find attached the:

- request for access to documents sent to the General Secretariat of the Council on 6 November 2017 and registered on the same day ([Annex 1](#));
- email from the General Secretariat of the Council dated 15 December 2017 ([Annex 2](#));
- confirmatory application dated 18 December 2017 and registered on 19 December 2017 ([Annex 3](#)).

[E-mail message sent to PUBLIC INFO on 6 November 2017 - 13:09]

First Name: **DELETED**

Family Name: **DELETED**

Postal Address: **DELETED**

Email: **DELETED**

Phone: **DELETED**

Initial question:

Requesting a copy of this document please: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - examination of the revised text

Thank you,

DELETED



Council of the European Union
General Secretariat
Directorate-General Communication and Information
Knowledge Management
Transparency
Head of Unit

Brussels, 15 December 2017

DELETED

Ref. 17/2305-ld/jg

Request made on: 06.11.2017
Deadline extension: 27.11.2017

Dear **DELETED**,

Thank you for your request for access to documents of the Council of the European Union.¹

I regret however to inform you that access to document **8946/17 REV3** cannot be given for the reasons set out below.

Document **8946/17 REV3** is a note of 20 September 2017 from the Presidency to Delegations related to the "Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities - examination of the revised text"

¹ The General Secretariat of the Council has examined your request on the basis of the applicable rules: Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43) and the specific provisions concerning public access to Council documents set out in Annex II to the Council's Rules of Procedure (Council Decision No 2009/937/EU, OJ L 325, 11.12.2009, p. 35).

This note reflects the discussions in the relevant Council Working Party of 4 September 2017 as well as written comments provided by the Member States afterwards.

These "Implementing guidelines" follow-up the Council Conclusions on a framework for a Joint EU Diplomatic Response to malicious cyber activities ("Cyber Diplomatic Toolbox") which were adopted by the Council on 19 June 2017 and which are publicly available on the Council's Website. Preparatory work on this framework instrument started in parallel with the preparations for the Council Conclusions but is still ongoing.

As you may learn from the Council conclusions, document **8946/17 REV3** relates to the Common Foreign and Security Policy. The document is by nature very sensitive since it reveals proposals for diplomatic actions in an area which is also under discussion in other international fora such as the UN, NATO, WTO as well as in bilateral dialogues.

Release of the information and positions contained in this document could provide misleading information on provisional positions which ultimately have not been agreed. It may also lead interested third parties to take strategic positions to weaken the EU's and Member States' negotiating powers and have a negative impact on the relations between the European Union and its Member States and international organisations and third countries concerned.

Disclosure of the document would therefore undermine the protection of the public interest as regards international relations. As a consequence, the General Secretariat has to refuse access to document **8946/17 REV3**.²

Furthermore, the content of document **8946/17 REV3** is still under discussion in the preparatory bodies of the Council.

Disclosure of the document could therefore lead to misperceptions and/or create expectations which may not be confirmed. This may however incite stakeholders to intervene on an issue on which a final decision has not been taken.

² Article 4(1)(a), third indent, of Regulation (EC) No 1049/2001

Release to the public of the information contained in this document would therefore affect the Council's negotiating process and diminish its chances of reaching an agreement as it is likely to put delegations under additional pressure. Disclosure of document **8946/17 REV3** would impede the proper conduct of the negotiations and compromise the conclusion of an agreement on this subject and would therefore seriously undermine the decision making-process of the Council.

As a consequence, the General Secretariat has also for this reason to refuse access to document **8946/17 REV3** ³.

The General Secretariat has weighed your interest in being informed of progress in this area against the general interest that progress be made in an area that is still the subject of negotiations.

Having examined the context in which the document was drafted and the current state of play on this matter, on balance the General Secretariat could not identify any evidence suggesting an overriding public interest in its disclosure.

You can ask the Council to review this decision within 15 working days of receiving this reply (confirmatory application).⁴

Yours sincerely,

Ramón CHISMOL IBÁÑEZ

³ Article 4(3), second subparagraph, of Regulation (EC) No 1049/2001.

⁴ Article 7(2) of Regulation (EC) No 1049/2001.

Council documents on confirmatory applications are made available to the public. Pursuant to data protection rules at EU level (Regulation (EC) No 45/2001), if you make a confirmatory application your name will only appear in related documents if you have given your explicit consent.

[E-mail message sent to access@consilium.europa.eu on 18 December 2017 - 17:56]

From: **DELETED**

Sent: Monday, December 18, 2017 5:56 PM

To: SECRETARIAT DGF Access

Subject: Re: Ref. 17/2305-ld/jg

Thank you for your response.

It is deeply problematic that a draft document in redacted form cannot be provided. As an accredited cyber-crime researcher, published author of peer reviewed papers related to the subject matter discussed, I find it disconcerting that no attempt to disclose the course or intent of these discussions is forthcoming.

Given the second addition of the Talinn Manual, NATO's announcement of a focus on cyber defense in 2016 (<https://www.nato.int/cps/en/natolive/75747.htm>) and the US Army revisions to its Field Manual relating to the deployment of cyber weapons (<https://www.c4isrnet.com/c2-comms/2017/04/21/army-releases-new-cyber-ew-field-manual/>) A response from the EU is long overdue.

I would submit with the body of work currently published it is very much in the public interest to identify where EU policy will align or depart from the presidents and direction outlined in the three referenced works.

Please register my appeal relating to the full or redacted disclosure of **8946/17 REV3**

Thank you,

DELETED