



Brussels, 26. 07. 2017
Ares(2017)

Dear Mr Coelho,

Thank you for your letter of 19 June 2017. We would first of all like to thank you for your diligent work as European Parliament rapporteur for our proposals to strengthen the Schengen Information System (SIS).

We took good note of your concerns regarding our proposal to make partial national copies of the SIS mandatory for all Member States.

Let us first reassure you that the central system works well. Query results are delivered to users within the required timeframes, leading to significant operational successes across Europe. Even after the introduction of the systematic checks this April, Member States without a national copy reported that the response time at the borders remained under one second. However, the demands on the system have also clearly grown in recent years. The capacity of the central system is being stretched as a result, and we consider that national copies in each Member State would provide a supportive buffer to the central system. This will become particularly necessary as technological changes such as increased use of Automatic Number Plate Recognition systems will lead to massive increases in the amount of data being processed through the SIS. We agree that this capacity issue could be addressed – at least in part – by significant investment in improving the central system.

The reasoning for our proposal on partial national copies is, as you say in your letter, that this is essential for business continuity in the Member States, ensuring that staff on the ground can access SIS data on a 24/7 basis. Even if further investment is made to bolster the central system's resilience, network outages either centrally or nationally can never be ruled out. Certain system updates require the SIS to be temporarily unavailable, for example.

Mr Carlos Coelho, MEP
European Parliament
Bât. Altiero Spinelli
08E158
Rue Wiertz 60,
1047 Brussels

Allow us to recall that the main objective of the SIS is to improve information-sharing across Europe, to keep our external borders strong and ensure internal security for our citizens. Now, more than ever, there is a clear need for the continued and uninterrupted availability of SIS at external border crossing points and for national policing. There is a risk therefore that if the central system is unavailable to countries that do not have national copies, border management and the security of the entire Schengen area will inevitably suffer. A partial national copy containing alphanumeric data is the best way to reduce the impact of these outages when they occur. This need was also identified in the overall evaluation of the SIS carried out in 2015, in order to improve business continuity arrangements.

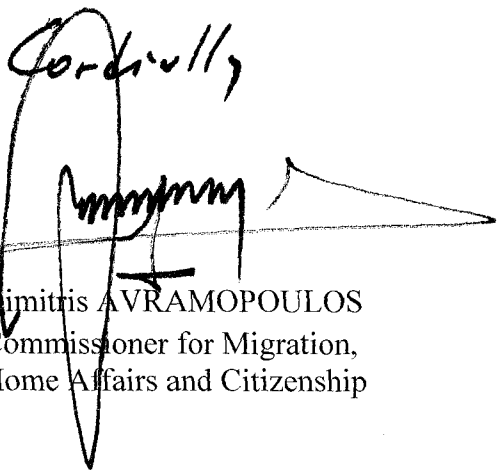
Moreover, Member States have long argued the need, for national security reasons, to retain their national copies of SIS, as it contains millions of records that are relevant in that context. The Commission has taken note of this view and agrees with it, particularly in light of the increased threat posed by terrorism that we face today.

You suggested amended provisions on national copies in your draft report that was discussed at the LIBE meeting on 10 July. The Council, too, has considered the issue in its discussions. In light of this, we recognise that this requires further reflection from the Commission.

We and our experts in DG HOME remain at your disposal should you have any further queries, or if there is anything else we can help with.

Yours faithfully,

Cordially,



Dimitris AVRAMOPOULOS
Commissioner for Migration,
Home Affairs and Citizenship



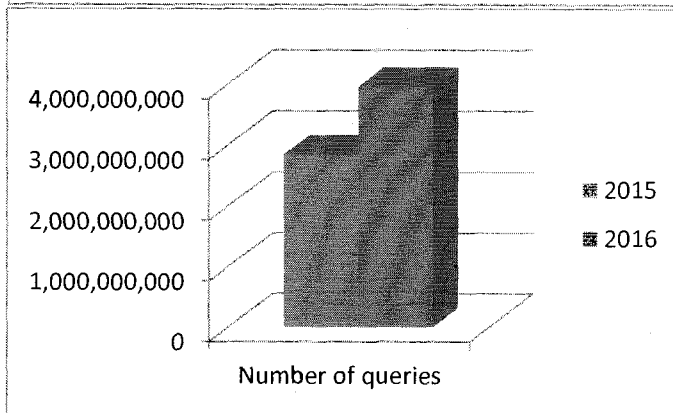
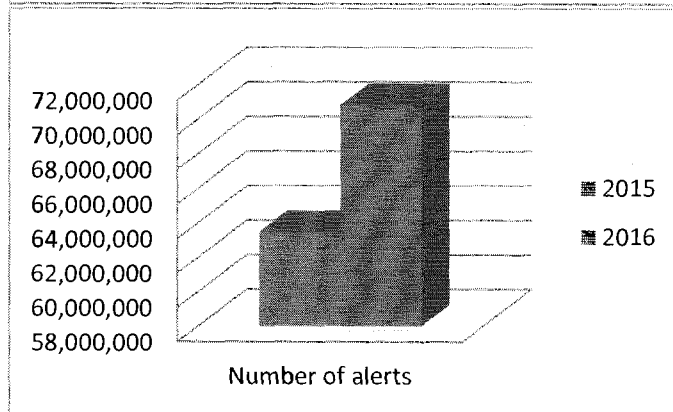
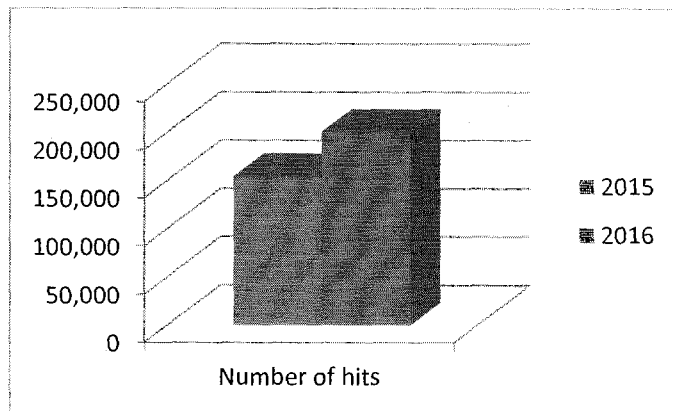
Julian KING
Commissioner for the
Security Union

Annex

Increased load on the system - statistics:

Two new countries – the UK and Croatia – have joined the system since SIS II was rolled out in 2013, and the number of queries, alerts and hits grows year on year. In 2016, there were nearly 4 billion queries of the system, and we expect this to continue to increase.

	2015	2016
Number of hits	154,768	200,778
Number of alerts	63,481,889	70,827,959
Number of queries	2,845,948,679	3,959,957,304



Availability

In your letter, you ask about the availability of the central system and the communication infrastructure. As you will be aware, the SIS legal instruments require 99.99% availability of the central system and the communication infrastructure network.

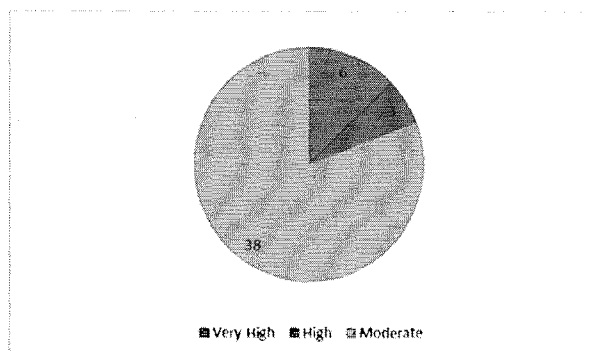
Availability of the central system

Between April 2013, when SIS II became operational, and the cut-off date of the overall evaluation of SIS II (February 2016) the central system has switched to its back-up 5 times, covering 97 hours of operational time in total. The back-up system does not run in parallel to the main system, but has to be activated if a switchover is required, which takes between 30 minutes and 2 hours.

An active-active set-up (the two sites running in parallel and balancing the operations between them) is not possible with the current set-up, due to the geographical distance between the central system in Strasbourg and the back-up system in Sank Johann im Pongau.

Availability of the network

Network unavailability was mainly caused by issues with the second encryption layer due to the use of non-state of art technology. The following chart shows network incidents according to severity:



For most of the time (74%) since SIS II began operating, the network availability between Member States and the central site has been in line with the Service Level Agreements (SLA). A relatively small number of major incidents – mainly outages at central level and incidents affecting the second encryption layer – were responsible for most of the availability issues bringing availability below this level. The presence of an optional second network connection in Member States significantly reduces the time when a Member State has less than the required 99.99% availability, but does not eliminate the risk. Finland and Denmark do not have a second network connection, which can cause total loss of business continuity if there are incidents affecting the central system.