Ref. Ares(2022)7302850 - 21/10/2022
With qualified electronic signature(s)

**To: Mr Matthias Oel**
Director
EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION
AND HOME AFFAIRS
Directorate B: Borders, Interoperability and
Innovation

**Subject: [ref: Ares(2022)5461277] Written Question [E-2641/2022], submitted by Cornelia Ernst (The Left) - Security incidents in connection with the Schengen Information System**

Dear Matthias,

In reference to your letter regarding MEP Cornelia Ernst questions on the Security incidents in connection with the Schengen Information System, please find below the necessary elements which I hope will serve the purpose of providing a comprehensive reply to the Honourable Member of the European Parliament.

***Question #1 "What security incidents has the Commission become aware of in connection with the operation of SIS/SIS II since its inception, and which of them are considered serious?"***

Since eu-LISA became responsible for the operational management of the SIS central system, there were no cyber security incidents having impact on data integrity or confidentiality registered. There were few technical incidents impacting services availability, that were fully addressed and the services affected were restored within the minimum required time.

***Question #2 "What instances have there been of SIS/SIS II data being unlawfully downloaded or of national copies being produced?"***

In 2013, an incident related to the unlawful download of data was reported on the Danish national system. This, however, was related to the Schengen Information System first generation (SIS I), which eu-LISA did not have responsibility for at the time.

Furthermore, in accordance with the SIS II Regulation, Member States have the freedom to decide whether or not to create national copies of the SIS database, holding the responsibility and accountability over their respective management, including all data protection and cyber security aspects. eu-LISA has no control or impact on the decision of Member States to create national copies (only a few Member States have decided not to create national copies and are querying directly the central system), neither on how

the Member States will manage their national copies. The Agency only holds the responsibility for the management of the SIS central system, including implementation of the highest standards of data protection and security.

***Question #3 "How often, and for how long, has the SIS/SIS II central system gone down completely, and what was the cause of the most recent incident that has come to light?"***

Since eu-LISA took responsibility for the operational management of the SIS and until the end of 2021, the SIS II central system has been highly available, with an annual availability over 99.75%. The reasons for unavailability of the system through the years concern not only technical incidents related to the Central System, but also incidents related to the underlying secure network infrastructure that connects Member States with the central SIS system.

Since 2013, the start of operations of SIS II, there were 19 cases of unavailability of the SIS II central system with an average duration of around 7 minutes, and exceptionally with the maximum duration of 2 hours and 13 minutes. In addition, there were 14 incidents related to the secure network infrastructure, leading to an average unavailability of 1hr and 7 min. However, it should be emphasised that the availability of the central system was above 99.95% over the last seven years. Additionally, none of the incidents mentioned were related to the security of the system and there was no impact on the data confidentiality or integrity.

The most recent incident with SIS central system was in the period between 30 June 2022 and 5 July 2022. It led to a degradation and partial unavailability of some of the functionalities of the system. The incident had two instances that occurred successively. The first instance occurred after the deployment of a new release and caused a partial unavailability of the Central System for 30 hours and 16 minutes (from 30/06/2022 at 08:15 UTC until 1/07/2022 at 14:36 UTC). The second instance caused a partial unavailability of the Central System for 32 hours and 32 minutes (from 2/07/2022 at 00:25 UTC until 3/07/2022 at 08:57 UTC). It is important to note that the few moments when all services needed to be completely down during that period were under the control of eu-LISA, in order to perform maintenance activities towards the resolution of the root causes of those incidents.

Based on the incident analysis, following the identification of the root cause, it was concluded that the security of the system was not impacted by any external influence. The reasons for the incident were of a purely technical nature related to a failure of a hardware component that severely degraded the performance of the system. It was replaced in due time, restoring the full availability of the system.

eu-LISA remains available to provide further information as needed.

Yours sincerely,

Qualified electronic signature by:
KRUM EMILOV GARKOV
Date: 2022-10-21 08:51:37 +02:00

**Krum Garkov**
Executive Director