Replies of the European External Action Service (EEAS) to the European Court of Auditors Special Report

Special Report

The coordination role of the European External Action Service

Mostly working effectively, but some weaknesses in information management, staffing and reporting

Contents

This document presents the replies of the EEAS to observations of a Special Report of the European Court of Auditors, in line with Article 259 of the Financial Regulation that are published together with the Special Report.

I. THE EEAS REPLIES IN BRIEF

The European External Action Service (EEAS) welcomes this Special Report by the European Court of Auditors (ECA). The EEAS considers the report's findings and recommendations a valuable contribution to the improvement of its performance and its general functioning. In fact, the EEAS has already echoed some of the recommendations in ongoing initiatives.

In a climate of multiple global crises, the EEAS must guarantee its "duty of care" towards its staff at all times. This duty does not only include physical security but also secure exchange of information. While always recognising the scale of this challenge, the EEAS, in cooperation with other institutions, places great emphasis on providing the tools for secure exchange of information and strives for interoperability among IT tools, where possible, both in Brussels as well as throughout the network of Delegations. In many countries, the EEAS operations face political challenges (e.g. war, coup d'état etc.) and infrastructure challenges (absence of proper internet infrastructure, bad quality of telecommunications etc.) and must face every obstacle in order to guarantee the Service's smooth operation around the world. This requires continuous engagement from the EEAS and its staff, especially given the IT field's rapidly altering security environment. All while balancing limited budget and resources. Needless to say that in this enormous effort, there will always be room for improvement.

This Special Report highlights the EEAS' efforts since 2019 to implement its Information Management Strategy, which allows for development of collaborative solutions and improvement of communications for EU delegations operating around the globe, both locally and with the EEAS Headquarters. The strategy has allowed the EEAS to set targets and to continuously adapt to new situations. A comprehensive, corporate collaborative platform, HIVE, allowing for much improved cooperation internally in the EEAS is already in pilot and its full-scale rollout is under preparation. In comparison with other EU institutions, the dispersal of staff and political situations in host countries places an extra burden on the EEAS' operations. However, the EEAS recognises the majority of the issues raised in this Special Report and works continuously to ensure that the strategy is properly communicated and implemented.

Increased interoperability among IT systems is mentioned throughout the report. The EEAS recognises that full interoperability among systems that are capable to at the same time to respect security and privacy protocols would be ideal. However, the implications of the many different types of systems, different user groups and audiences, current design of the existing systems, complexity of infrastructure and security and privacy protocols, make this a challenging and expensive undertaking. While the EEAS has made great advances in this regard. The majority of its systems, as illustrated by Figure 5 of the Special Report are interoperable with other systems. The development and implementation of such a fully integrated user experience - although desirable - is far beyond the current resources allocated to the EEAS.

Reporting is a core task of any administration, national or international. Reporting ensures accountability and EU regulations and treaties very often request it. The EEAS complies with the rules binding all EU institutions and requests from its staff the necessary minimum of reporting requirements (requirements stemming from the Financial Regulation, EU treaties etc.). Accountability is enhanced by strategic forward planning and envisaging (to a certain extent) what could be achieved in the future. The report acknowledges the simplification exercises that have taken place in the EEAS and the European Commission to decrease the number of reporting requirements and the 2021 EEAS internal review (EEAS@20) exercise, which helped the EEAS to identify and address weaknesses. Changes in the EEAS' organisational structure, working arrangements and reporting guidelines to staff in Headquarters and in EU delegations were direct results of these exercises.

The Commission is currently discussing at the Council Security Committee the “COM(2022)119 - Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union”. This initiative aims to harmonise the information security policy across the EU in order to facilitate the sharing of information ensuring the security of them. The proposal is currently being discussed by the co-legislators. Until the adoption or rejection of the proposal, the EEAS, and the Commission, cannot implement changes or adopt further measures.

II. EEAS REPLIES TO MAIN OBSERVATIONS OF THE ECA

1. Information management and interoperability of IT tools

As the Special Report notes, rolling out functional and reliable IT tools is key for good coordination and should be based on a solid information management strategy[1]. This principle is at the core of the EEAS' approach towards information and knowledge management. The 2019 strategy focused on identifying challenges in this domain and as a result, the EEAS has focused its efforts towards the implementation of constituent parts.

Since the adoption of the strategy, the EEAS has continuously adapted its action plan to its IT stakeholders' needs. During the audit period (September 2021 until April 2023), the EEAS Information Management Committee met three times. With contribution from all stakeholders at the EEAS, the Committee discussed and agreed on two fundamental policies which led to the Decisions of the EEAS' Secretary-General on the Service's record management and archive policy ADMIN(2022)61, and on Information Sharing Policy ADMIN(2023)32. These Decisions are major steps in the implementation of the strategy. It is necessary to mention that the use of a variety of tools is unavoidable. EEAS supports all tools necessary to interact with all its interlocutors and adapts to the needs of each of them by providing the necessary IT tools and solutions for its staff to be able to carry out their tasks. Some examples of Video teleconferencing (VTC) tools include, Zoom for training with the European Commission's Directorate-General for Budget, Microsoft Teams in general for the all European Commission Directorates-General as well as for the United Nations, Webex for EEAS internal, Webex with some Member States, Skype with others, Zoom with some host countries etc. Given the wide range of interlocutors, the EEAS IT support shows a great degree of flexibility to facilitate the cooperation with all interested parties.

2. Secure communications

RESCOM has been fully rolled out in November 2021 and the system currently has around 1,500 active users. It also contains 150,000 documents and has an average daily traffic of 300 secure messages and 200 new documents. In particular, some user communities, where working with classified information is a daily business, are using the system heavily and there are no significant technical issues with the system. Indeed, as any new tool, the system requires some initial learning curve from users; however the EEAS provides high quality mandatory online training material for all RESCOM users. In addition, a network of RESCOM Community managers (RCM) has been created so that users can have close support even without involving the IT helpdesk for basic RESCOM related issues/questions.

Taking into account the high number of users working with the system without any major issue, the EEAS concludes that the system is suitable to cover the business requirements. RESCOM has been interconnected with the RUE-X system of the European Commission in June 2022 providing a secure interinstitutional file exchange and messaging solution between the two institutions. Likewise, the system is interconnected with the CORTESY system of the Council at EU-Restricted level providing a direct access to incoming COREU messages to RESCOM users (both in Headquarters and EU delegations). The RESCOM system also provides secure, encrypted voice and instant messaging possibilities from security-hardened mobile phones, including accessing restricted documents from these phones. The EEAS is likely to be the only EU institution able to provide a flexible restricted system including full mobility for both the unclassified and the restricted domains.

[1] See ECA observation 29

The EEAS would also like to underline that each EU Institution makes its own decisions with regard to the selection of the IT tools and services based on its business needs, the threat landscape, the risk appetite and the security posture of the institution. Taking into account the nature of its core activities, the EEAS is more conservative regarding cloud-based solutions and security is always a high priority criterion when choosing an IT tool or a system. Furthermore, concerning systems handling classified information, the possibilities of the EEAS (and of other institutions) are very limited as it must comply with the EU security rules and use certain building components for classified systems that are second party approved and available on the Council's list of approved cryptographic devices.

Concerning the perceived cumbersome usage of the ZEUS offline encryption tool, the EEAS is of the opinion that this is partially related to infrequent usage of the tool in a number of delegations. Further integration of ZEUS into RESCOM will reduce to zero the overhead attributable to manual updating of the tool. The total number of EU delegations and Member State Embassies currently provided with ZEUS increased to 1,374 by July 2023, which represents an increase of 20% from January 2022. Using ZEUS eliminates the need for a cumbersome physical exchange of paper documents or USB flash drives between EU delegations and Member State Embassies situated in the same country. The European Union Satellite Centre (SATCEN) can be used as a reference for the use of ZEUS. It functions well for the distribution of their R-UE/EU-R documents: in 2022, SATCEN distributed over 5 000 products to the 27 Member States.

Finally, the EEAS faces huge infrastructure challenges in some countries such as the absence of proper internet infrastructure: this should not be underestimated when discussing communications issues. The EEAS has recently revamped completely its network and upgraded its capacity. In most Delegations, the bandwidth has at least tripled, and in some cases even increased tenfold. In countries with poor quality of internet infrastructure and service providers, twenty new satellite connections have been installed with a remarkable improvement of the latency (decreased by half).

III. EEAS REPLIES TO THE RECOMMENDATIONS OF THE ECA

1. Recommendation 1: Ensure the implementation of the information management strategy

The EEAS should ensure that its collaborative, knowledge management and record-keeping platforms, as well as a corporate search function, become fully operational and provide for streamlined communication when implementing its information management strategy;

(Target implementation date: December 2025)

The EEAS accepts this recommendation.

The missing search function is due to the European Commission' restrictions imposed in ARES[2], whereas for the implementation of its management strategy, reference should be made to the adopted policies[3].

2. Recommendation 2: Improve secure exchange of information

The EEAS should, in coordination with the Commission and Council where relevant:

a) **seek to enhance interoperability of its existing IT tools for secure communication and exchange of documents;**
b) **apply a standard document security classification across the different organisations (EEAS HQ, EU delegations, Commission and Council).**

(Target implementation date: for a) December 2025, **for b) linked to the legislative proposal adoption date.)**

The EEAS accepts recommendation 2a).

In terms of interoperability of classified information systems, the EEAS has completed the necessary steps to interconnect its RESCOM system to the Commission's RUE-X system in June 2022. Interoperability of EU classified information systems at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET is not envisaged in the short term, due to the complexity of the security and interoperability aspects. This will nevertheless be analysed to determine options for future interconnection of the respective classified systems. Unification of the systems is not considered, as the operational requirements of the EEAS are not comparable with those of the Council and Commission.

The EEAS will further investigate how to ensure user compliance with using the existing accredited IT tools for secure communication and exchange of documents to establish the extend of the possible lack of compliance. EEAS will consider implementing stronger rules and measures to manage anyone who would fail to comply with the usage of secure communication tools and the application of information security guidelines.

[2] ECA observation 34

[3] ECA observation 28

The EEAS accepts recommendation 2b).

The EEAS, Headquarters and EU delegations are using the same security classification (security classification marking) for Classified Information (EUCI) as the Commission and the Council. The EEAS security rules are almost verbatim the Council Security Rules.

However, the EEAS (and the Council) has a different approach from the Commission regarding the LIMITE information (Sensitive non Classified information in the nomenclature of the EU). To this extent, an initiative of the Commission (COM(2022) 119 - Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union) is currently under discussion at the Council Security Committee. This initiative aims to harmonise the information security policy across the EU in order to facilitate the sharing of information ensuring the security of them.

Regarding the interoperability of IT tools for secure communication, the EEAS and the Commission's Security Directorate (HR.DS) closely collaborate with the different institutions for the use of common secure communication tools, in particular for classified information.

Concerning a possible standard document security classification, as specified in footnote 11 of the draft report, this is included in the Commission proposal COM(2022) 119. This proposal is currently being discussed by the co-legislators. If adopted, this legislation would address the issue. The Commission and the EEAS cannot therefore implement further measures until the adoption or rejection of the proposal.

3. Recommendation 3: Improve interaction between EEAS HQ and EU delegations

The EEAS should take the following steps to foster coordination between HQ and EU delegations:

a) ensure that all EU Ambassadors receive a mission letter at the beginning of their mandate;
b) in line with the Secretary-General's guidelines, review the timing of the sending of instructions for EU delegations on filling in the templates for their annual management plans and ensure that delegations receive systematic feedback on their plans;
c) ensure that, in line with the Secretary-General's guidelines, EU delegations provide regular political reporting and receive feedback and guidance from HQ.

(Target implementation date: December 2024)

The EEAS accepts the recommendation 3a), 3b), 3c).

The recommendation is being implemented. On point a), the EEAS has put a system in place that verifies that all newly appointed EU Ambassadors receive their respective mission letters, before they take up their duty. In 2022 and 2023, all EU ambassadors received their mission letters.

The Special Report demonstrates that the overall reception of the annual management plans (AMPs) is rather positive from the EU delegations[4], regardless of some individual negative comments. Nonetheless, the EEAS recognises the need to enhance its feedback mechanisms.

Finally, the EEAS welcomes the European Court of Auditor's conclusion on the usefulness of EUDEL as a coordination platform[5].

4. Recommendation 4: Facilitate the follow-up of the 2022 workload assessment in EU Delegations

The EEAS should, in coordination with the Commission, facilitate the follow-up of the 2022 workload assessment as regards the allocation of all staff in EU delegations. This should be done as part of a wider strategic reflection on the EU delegations held at senior level between the EEAS and the Commission. In doing so, it should take into account the principle that the allocation of staff resources to EU delegations should be commensurate with policy and cooperation needs.

(Target implementation date: December 2025)

The EEAS accepts the recommendation.

The recommendation focuses on the EEAS role in supporting and facilitating the implementation of the 2022 workload assessment in EU delegations (WLAD). The need for 'targeted adjustments to the staffing levels' revealed by the workload assessment concerns Commission staff, therefore these targeted adjustments are being implemented by the Commission, with the support of the EEAS.

The findings of the WLAD will feed into a wider strategic reflection on the EU Delegation network to be held at senior level between the EEAS and the Commission. These include: examining the size of EU Delegations against their geopolitical importance, policy demands to deliver the European agenda, resource constraints, and security considerations; finding a balance between efficiency and global reach to maintain diplomatic presence in an efficient manner; ensuring that the EU delivers on the 'European Agenda', including exploring novel forms of diplomatic delivery (e.g. thematic envoys from internal policies services operating from headquarters); considering further strengthening relations with key countries through sub-offices.

5. Recommendation 5: Improve interinstitutional coordination regarding briefing tools for the preparation of Foreign Affairs Council meetings

The EEAS should, in coordination with the Commission and Council, adopt a common briefing tool or, failing this, seek to ensure interoperability and reciprocal access to existing institutional tools.

(Target implementation date: December 2025)

[4] See Figure 8, Figure 9 and ECA observations 51-56

[5] ECA observation 105

The EEAS accepts this recommendation.

It is important to note that the implementation of this recommendation is not solely in the remit of the EEAS. It will require cooperation with the Council and the Commission.

As acknowledged in the report, a partial technical solution between the Commission's IT platform and the EEAS' IT platform already exists. The extension of this technical solution in order to make the two IT tools interoperable is under discussion and its implementation is being assessed in terms of budgetary resources.