1. On 14 June 2020, the GSC was invited to undertake the studies necessary to allow Coreper to decide on the provision of a secure physical and virtual meeting facility for Heads of State and Government and ministers, capable of operating with full language interpretation (doc. 9457/21).

2. Since then, the GSC has worked on two separate initiatives placed under a joint internal governance framework, with a view to:

   i) adding full language interpretation to the ongoing project of creating a secure VTC system (up to classification level SECRET UE/EU SECRET);

   ii) studying the feasibility of offering a secure physical meeting room (up to classification level SECRET UE/EU SECRET), suitable for Heads of States and Government and ministers and capable of operating with full language interpretation. This room could also be used for meetings of Coreper and other Council preparatory bodies as appropriate.

3. As a first outcome, GSC competent services have drafted high-level business requirements and high-level security requirements (attached). The latter are based on the Council Security Rules and the corresponding implementing policies and guidelines.

4. While the possible options identified for locating the secure room in the GSC premises are still under examination, including to check if they meet all those requirements, a location has
already been identified for the secure interpretation facility. This facility would be securely connected to both the secure room and the secure VTC system, thus allowing full interpretation to both physical and virtual meetings up to up to classification level SECRET UE/EU SECRET.

5. Depending on the options retained, estimated costs could reach up to M€ 6, including around M€ 2 for the secure interpretation facility. Once a decision is made, and the corresponding budget secured, the completion time is estimated between 18 and 24 months.

6. On that basis, the GSC recommends that Coreper:
   
i) takes note of the work accomplished by GSC services and invites the GSC to continue work in consultation with other relevant Council preparatory bodies such as the Budget Committee and Council Security Committee;

   ii) approves the high-level business requirements and high-level security requirements;

   iii) invites the GSC to work further on the identification of possible suitable locations for installing the secure meeting room and provide options with forecast of the associated costs to Coreper by 30 November 2022.
HIGH-LEVEL BUSINESS REQUIREMENTS

High-level business requirements

The “High-level business requirements” provide a high-level description of the business requirements of the European Council and the Council to be covered by the secure meeting room capabilities including the following:

1. a capability of holding classified discussions at the level of CONFIDENTIEL UE/ EU CONFIDENTIAL or SECRET UE/EU SECRET or their national equivalents;

This room would not provide facilities to hold public or non-classified sessions or sessions below the indicated classification levels. This exclusive use of the room for classified discussions should not impact the overall capacity of GSC meetings rooms.

2. Available for meetings of the Member States’ Heads of States or Governments (European Council meetings) or ministers and officials, and EU institutions, bodies or agencies’ staff (Council meetings) in the context of the EU decision-making process or broader EU collaboration;

Availability for classified meetings of Coreper, PSC or other Council preparatory bodies should be considered.

3. a capability of holding meetings in 1+1 format (i.e. 34 places around the table plus backbencher places and note takers in the second row);

4. Causing the least possible disturbance when meeting participants need to transit from the non-classified meeting room to the secure room and thus facilitating its frequent use, whilst taking into account intrinsic characteristics of the building where the facilities will be located;

5. The secure room should be VTC-compatible.

6. Equipped with easily visible optical indicators for video camera or microphone activation, with a hand raising tools and individual or shared big screens;

7. This room should not provide recording (audio/video, including pictures) options.

8. providing a suitable level of comfort for VIPs (furniture, chairs, etc.) and appropriate fixed decorum (e.g. flags, but no flowers or other frequently replaceable items);

**Note:** Decorum and catering services will induce additional security measures in a SECRET UE/ EU SECRET environment.

9. providing simultaneous interpretation at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET with full linguistic regime.

Remote interpretation in a secure environment at the level of CONFIDENTIEL UE/ EU CONFIDENTIAL and SECRET UE/EU SECRET should be preferred. The interpretation facility should be usable for secure VTC meetings.
10. the secured interpretation environment (or secured interpretation “hub”) should offer enough room to install 30 standard mobile interpretation booths in one single area – including access to booths and safety and fire precautions. Booth dimensions ISO 4043:2016 for a 3 seats (interpreters) are 2,40m (width) x 1,60m (depth) x 2,00m (height) each. All booths should be equipped with interpretation desks (inside) and video screens (inside or outside). 11. In order ease the use of the secure meeting room during summits without movement of interpreters, the feasibility of combined interpretation should be analysed. Combined interpretation is understood as using the secured interpretation hub to interpret classified meetings taking place in the secure meeting room or to interpret non-classified meetings taking place in the usual room of the summits. Appropriate facilities and technical assistance will be provided in the secured perimeter (as defined in paragraph 10 the security requirements) for the support functions of the meetings (space for drafters, copy machines);

12. The secure meeting room project should be considered in light of the planned JL renovation. It is in particular advisable to avoid unmounting the facilities for the renovation (e.g. eventual changes for HVAC) and to avoid proximity with a public access zone.
ANNEX II

HIGH-LEVEL SECURITY REQUIREMENTS

1. The "basic principles and minimum standards of security for protecting European Union Classified Information" (EUCI) are defined by the Council Security Rules\(^1\) and their underlying policies and guidelines.

2. Any meeting room or interpretation facility where European Union Classified Information (EUCI) is handled or discussed shall be compliant with these standards, which differ according to the level of designated classification of the EUCI concerned\(^2\).

3. The following high-level security requirements correspond to the level SECRET UE/EU SECRET, i.e. for a meeting room and interpretation facility where the EUCI handled or discussed is "information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States\(^3\).

4. They are based on the assumption that the discussions concerned would require the use of electronic devices (microphones, cameras, computers, etc.) and could not be held with only voice and paper, from a business point of view.

Physical and personnel security

i. The meeting room and interpretation facility shall not be used for any other purpose than classified meetings at level SECRET UE/EU SECRET or CONFIDENTIEL UE/EU CONFIDENTIAL.

   Justification: the integrity of the meeting room and the interpretation facility shall be protected at all times. Any access outside times of meetings shall be authorised, justified and registered. Any change of the physical arrangements shall be approved. Permanent access rights shall be exceptional and the list of their beneficiary kept updated and regularly reviewed.

ii. To avoid additional security measures (safes, surveillance mechanisms), the meeting room and the interpretation facility should not be used to store EUCI.

iii. The enclosure of meeting room and the interpretation facility shall resist any effort to penetrate until security personnel can be present after the intrusion attempt has been detected (e.g. using intrusion detection system IDS).

iv. The meeting room and interpretation facility shall be equipped by an access control system.

v. Enough space shall be available at the entrance of the meeting room and

---

\(^1\) Decision 2013/488 of the 13 September 2013.

\(^2\) RESTREINT UE/EU RESTRICTED, CONFIDENTIE UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET.

\(^3\) The potential value of information and material at that level being very high, corresponding protection and security measures shall ensure a protection against state-level threat actors with extensive resources, including those necessary to hack communication and information systems, exploit unintentional radio or electrical signals, sounds, and vibrations or recruit insider agents.
interpretation facility to execute a proper access control and accreditation.

*Justification:* the meeting room and the interpretation facility being Secured Areas with EUCI directly accessible during meetings, require that any access during meetings is limited to persons with a need-to-know\(^4\) and SECRET UE/EU SECRET level valid security clearance, including by the virtue of a function/office and is explicitly authorised, registered and controlled.

vi. There should also be enough space outside the meeting room to install storage areas (soundproof lockers) for personal electronic equipment.

*Justification:* Non accredited personal and professional phones and laptops, but also personal smart devices like smart watches, hearing aids or other electronic/electric devices or equipment including RFID badges shall not be accepted in the meeting room or interpretation facility.

**Communication and Information Systems (CIS)**

vii. CIS installed in and used into the meeting room and interpretation facility shall be authorised, security accredited and monitored using network defence techniques.

viii. The transmission of EUCI by electronic means shall be encrypted with EU approved cryptographic products. Subject to the approval of the Security Accreditation Authority, this obligation may be lifted based on a risk management process if the transmission remains confined within the same Secured Area or passes through a controllable Administrative Area between two Secured Areas.

ix. All IT maintenance and support capabilities shall be located within the GSC premises.

x. Only wired communication may be installed and used. Wireless communication facilities outside the secured perimeter shall be unreachable. Any wireless solution (cellular networks, wifi, etc.) shall be deactivated in the secured perimeter (to be specified after field audit).

**Protection against eavesdropping and TEMPEST spying activities**

xi. To mitigate the risk of exploitation of compromising emanations, the meeting room and interpretation facility shall be either equipped with TEMPEST equipment, or enclosed in a shielded enclosure\(^5\). In the first hypothesis, the level (A, B or C) of TEMPEST attenuation required for that equipment will be determined on the basis of technical measures of the level of exposure to such exploitation in the zone(s) (0, 1 or 2) where the meeting room and interpretation facility will be located.

xii. The design of the meeting room and interpretation facility should facilitate technical security counter-measures (TSCM) inspections (sweeping), to take place before and after the meetings to detect, locate and neutralize any eavesdropping device. The use of radio frequency monitoring should also be facilitated.

xiii. Any new furniture, technical equipment or accessory (flowers, decorations, As well as specifically authorised catering personnel, technicians, interpreters and any other support staff.

See IASG 14006/13 on selection and installation of TEMPEST equipment (R-UE/EU-R). No facility with natural electromagnetic attenuation can be considered TEMPEST-proof at the level SECRET UE/ EU SECRET. Facility Zones 2 are considered as compatible with the use of commercial off-the-shelf equipment at the level CONFIDENTIEL UE/EU CONFIDENTIAL.
beverages utilities etc.) shall undergo a TSCM inspection.

xiv. Any technical intervention (maintenance or equipment) shall be coordinated with the GSC TSCM team.

 xv. Depending on the location and environment, it is recommended as good practice that no acoustic signal may leave the meeting room or interpretation facility. If needed, sound attenuation in building and technical systems such as HVAC should be implemented.

Other requirements

xvi. Security operating procedures shall be established to ensure compliance to these requirements.

xvii. Any EUCI created in the facilities shall be registered in compliance with the CSRs.

xviii. All IT operations shall follow the four-eye-principle, preferably by SMART and ORG.5.

xix. All emergency and contingency concepts and plans shall ensure the confidentiality, integrity and availability of EUCI to the extent possible.

xx. All implemented security measures shall be subject to regular tests.