SURVEY PART II

Questionnaire for potential GOVSATCOM users who have little to no experience in the use of secure SatCom services

STRUCTURE OF THIS DOCUMENT AND TYPE OF QUESTIONS

- *This survey includes questions divided into the following sections:*

ENTITY INFORMATION

A. GENERAL INFORMATION

B. USER CAPABILITIES AND TECHNOLOGY

C. GENERAL USER NEEDS AND REQUIREMENTS

D. USE CASES

E.1. USE CASE SPECIFIC REQUIREMENTS

E.2. BUSINESS IMPACT ASSESSMENTS

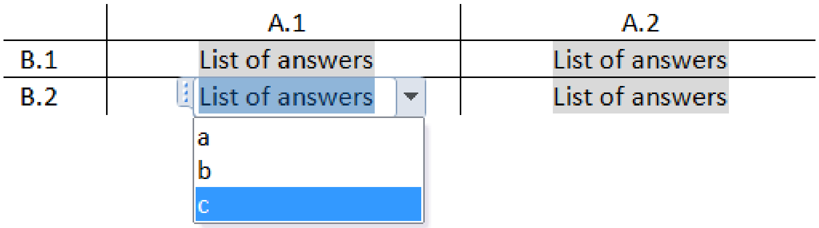
SURVEY ACRONYMS

- *Where necessary, the questions provide short instructions on the content of the fixed lists and scales, definitions of concepts and graphs.*

- *Most of the questions require multiple choice selection of answers e.g.:*

B.1	☒
B.2	□
Other, which?:	□

- *There are also matrix type questions were the respondent will be asked to choose his answers from the drop-down list in relation to column A and row B e.g.:*



	A.1	A.2
B.1	List of answers	List of answers
B.2	List of answers	List of answers

- *In many cases there is a possibility to provide an answer to an open question or option e.g.:*

Other, which?:

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

GOVSATCOM USERS' SURVEY

ENTITY INFORMATION

INSTITUTION AND PERSONAL DATA

a. **Name**

b. **Job function**

c. **Activity domain**

d. **Organisation**

e. **Country**

f. **E-mail address**

g. **ENTRUSTED PoC**

h. **User community** *(if you mark more than one community, please mark the checkbox of your main area of activity)*

	Activities your entity is involved in:	*Is this your main area of activities? (please, select only one)*
Border Authorities	□	□
Maritime Authorities	□	□
Civil Protection	□	□
Humanitarian Aid	□	□
EU External Action	□	□
Law Enforcement Bodies	□	□
Military Forces	□	□
Key Infrastructure Operators	□	□
Other, please specify here:	□	□

CLASSIFIED INFORMATION

Please read the survey first. Dependently if the answers to survey would contain classified information. Please mark the relevant box and proceed accordingly?

NO □ *Please proceed to answer the survey.*

YES □ *Please inform your PoC who will indicate you how to proceed.*

GENERAL REGULATION ON DATA PROTECTION

□ *The collection of personal data is the sole responsibility of ENTRUSTED project consortium members, who guarantee their protection in compliance with the General Data Protection Regulation (EU) 2016/679 and regulation (EU) 2018/1725, and arises within the scope of the project and activity to which this questionnaire reports to. To learn more about the ENTRUSTED Survey Data Privacy Policy, please refer to the document distributed with this questionnaire.*

□ *By completing this form, I consent the ENTRUSTED project PoC to process my personal data in order to process and evaluate the questionnaires, and to contact me via email to request information about my answers or to provide more information about the project. I have read and agree with the ENTRUSTED Survey Privacy Statement.*

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

A. GENERAL INFORMATION

1. For the technologies your entity currently uses when communication has to be ensured (i.e. reliable communications), please indicate the level of satisfaction:
0 – Technology not used; 1 – not very reliable; 5- very reliable when it comes to reliability of the service in your normal operations:

Public mobile phone networks (e.g. 4G, 5G)	Choose from 0 to 5
Bubble (virtual) networks (e.g. tailored networks to specific areas)	Choose from 0 to 5
Private radio networks (e.g. UHF/VHF)	Choose from 0 to 5
Wireless networks	Choose from 0 to 5
Customised mobile applications	Choose from 0 to 5
Satellite Communication (SatCom) services	Choose from 0 to 5
Push-to-Talk services	Choose from 0 to 5
TETRA networks	Choose from 0 to 5
Other, please specify	

2. What are the main barriers that prevent your entity from using SatCom services or to extend its usage?

User specific obstacles

We do not have available technical and/or procedural know-how or necessary equipment □

There are no people trained to deal with the technology □

Lack of knowledge about benefits of SatCom for our activities □

Other, which? □

Legal and institutional external obstacles

National procurement rules, if so which? □

Agency procurement procedures, if so which? □

National infrastructure limitations, if so which? □

National legal constraints, e.g. national radio landing rights, if other which? □

National technical constraints, if so which? □

Other, which? □

Service specific obstacles

There is not enough information about SatCom benefits □

There is not enough information about access to SatCom □

There are delays to procure/deploy services □

The cost of the services is too high □

The catalogue of services is not easy to access □

The services are too difficult to use □

The service that we need is cannot be supported by SatCom □

Quality of service □

Other, which? □

3. In general terms, which of the following telecommunication services would be of interest for your entity?

Voice-only services □
(including in remote locations, fixed and on-the-move)

Transmission of content in one direction (Broadcast services) □
(e.g. TV)

High-speed data connection (Fixed Broadband services) □
(e.g., high-speed internet, B2B, OTT, DHT)

High-speed data connection on the move (Mobile Broadband services) □
(e.g., onboard airplanes, vessels, trucks or other vehicles)

Low data-rate services □
(e.g. IoT, machine-to-machine (M2M) services, fixed and on-the move)

If other, which?:

4. What high-level information security aspects would be important for your entity?
Please indicate the level of importance of each security aspect: 1- not very important; 5- very important

Confidentiality
(i.e. protecting sensitive and private information from unauthorized access, file encryption, access level permissions) Choose from 1 to 5

Integrity
(i.e. information is not corrupted, nor modified by unauthorised parties) Choose from 1 to 5

Availability
(i.e. ensure service continuity, including access to authorized users) Choose from 1 to 5

Authenticity
(i.e. ensure the genuineness of physical or electronic documents, communications, transactions, and data) Choose from 1 to 5

Non-repudiation
(i.e. services providing proof of the integrity and origin of data, as well as authentication mechanisms that can be said to be genuine with high confidence) Choose from 1 to 5

B. USER CAPABILITIES AND TECHNOLOGY

5. **Please select the current and expected use of secure SatCom services over your current communications systems (traditional, not SatCom means):**

	Today	Medium-term (after 2027)
Expected use of secure SatCom services with respect to non-SatCom services	Select Use	Select Use

6. SatCom systems can be owned by commercial or governmental entities. Please select your preferences in respect to the ownership of the systems, and thus the service provision.

	Today
Expected use of secure SatCom services by ownership	Select Provider

7. With respect to user terminals, what requirements would you consider important?

Certification / standardisation	☐
Reliability	☐
Weight	☐
Waterproof	☐
Battery duration / power consumption	☐
Interoperability	☐
Cybersecurity related to the access to terminal use	☐
Cost	☐
Multi-band capabilities	☐
Multi-orbit capabilities	☐
Easy-to-use and easy-to-deploy technology and interface	☐
Encryption	☐
Quality of service	☐
Other, which?	☐

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

8. **Are you aware of any initiative (including Research & Innovation) related to (secure) SatCom ongoing within your entity? If so, could you list them?:**

9. **Are you aware of any initiative (including Research & Innovation) related to (secure) SatCom ongoing at national or EU level? If so, could you list them?:**

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

C. GENERAL USER NEEDS AND REQUIREMENTS

10. Which of the following information protection aspects would your entity expect while using secure and guaranteed SatCom services?

Please choose your answer according to the following scale: 1 – not important, 5 – very important.

[confidentiality] Possibility to transmit EU Classified Information (EUCI)	Choose from 1 to 5
[confidentiality] Possibility to transmit National Classified information	Choose from 1 to 5
[confidentiality] Levels of security guaranteed by accreditation entities	Choose from 1 to 5
[confidentiality] Protection of user location	Choose from 1 to 5
[integrity] Integrity and non-repudiation of transmitted information	Choose from 1 to 5
[integrity] Resilience and protection against jamming and interference	Choose from 1 to 5
[integrity] Monitoring of communication link status (Link status service)	Choose from 1 to 5
[availability] Geographical coverage and ensured capability	Choose from 1 to 5
[availability] Tailored access by type of user community	Choose from 1 to 5
[authenticity] Authenticity	Choose from 1 to 5
[non-repudiation] Non-repudiation	Choose from 1 to 5
Other, which?	Choose from 1 to 5

11. What of the following customer services would be of interest for your entity?

365/7/24 Customer support (Help Desk) □
Tailored Service Level Agreement (SLA) □
Online technical assistance □
On-site/In-field technical support □
Lease/Logistic & supply of pre-configured SatCom terminals □
Training services □
Reference materials (e.g. handbooks on secure communications) □
Framework agreement (Pooling and sharing platform) □
Other, which?: □

12. How would you expect to get access to future GOVSATCOM services?

This question refers to the way users expect to put in place a service request.
Please, select as many options as you consider relevant.

Via website, directly contracting services from there □
Via phone call, directly contracting services by calling to a unique service access point □
Having access to a catalogue of pre-defined services and prices □
Having access to multiple offers for the same service request (i.e. competitiveness) □
Other, which?: □

ENTRUSTED project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 870330.

13. Which means would you expect to interact with the potential support service of secure SatCom services?

This question refers to the expected interface with the potential customer support service of the SatCom service provider, once the SatCom service is in place. Please, select as many options as you consider necessary

Via website (e.g. live chat)	□
Via direct contact by phone	□
Via email	□
Other, which?:	□

D. USE CASES

14. The ENTRUSTED project has preliminarily identified a set of Use Cases for secure SatCom services. Based on the tasks, duties and activities of your entity, please select from the following list the Use Cases relevant for your entity:

The use cases are grouped by 3 Fields of Application (FoA): (1) Surveillance, (2) Crisis Management and (3) Key Infrastructure, and respectively in Use Case Families within each FoA.

There are also 3 Specific Use Cases: (a) Polar regions users, (b) UAV/RPAS/Beyond Line-of-Sight Communication – Aerial SatCom and (c) Machine to Machine communications and IoT.

S. SURVEILLANCE

S.1. Border surveillance

S.1.1. Sea border scenarios □

S.1.2. Land border scenarios □

S.1.3. Pre-frontier scenarios □

S.1.4. Military missions and operations (CSDP & national) □

Other, which?: □

S.2. Maritime surveillance & control

S.2.1. Maritime safety and surveillance □

S.2.2. Maritime security: illegal activities □

S.2.3. Fisheries Monitoring Control and Surveillance □

S.2.4. Protection of shore and maritime resources □

S.2.5. Protection of subaquatic cultural heritage □

S.2.6. Military missions and operations □

Other, which?: □

C. CRISIS MANAGEMENT

C.1. Maritime Emergency

C.1.1. Maritime Search and Rescue (SAR) □

C.1.2. Response to maritime disasters – civil □

C.1.3. Response to maritime disasters – military □

C.1.4. Telemedicine (onboard ships) □

Other, which?: □

C.2. Humanitarian Aid

C.2.1. Assistance in case of disasters and armed conflicts □

C.2.2. Telemedicine □

C.2.3. Refugee camps main communication □

C.2.4. Refugee camps welfare services (e.g. videoconference) □

C.2.5. Peacekeeping mission communications □

Other, which?: □

C.3. Civil Protection

C.3.1. Response to natural and man-made disasters □

C.3.2. Ambulance and fire risk rescue response within EU □

C.3.3. Information dissemination (e.g. open messages comms) □

C.3.4. Forest fires early-warning video surveillance □

C.3.5. External Public protection □

Other, which?: □

C.4. Law Enforcement Interventions

C.4.1. Fight against international drug traffic □

C.4.2. Fight against international Organized Crime Groups (OCG) □

C.4.3. National police missions within EU □

C.4.4. Fight against environmental crimes (e.g. illegal waste dumping). □

Other, which?: □

C.5. EU External Action

C.5.1. Civilian CSDP missions □

C.5.2. Election observation □

C.5.3. EU Diplomatic representation in foreign countries □

C.5.4. Intelligence □

C.5.5. UN missions □

C.5.6. NATO missions □

Other, which?: □

C.6. Forces deployment

C.6.1. Defence National Territory □

C. 6.2. Support Air Defence systems □

C.6.3. Joint military C2 network resilience – secondary links □

C.6.4. Support to other governmental bodies □

C.6.5. HQ Operations connection □

C.6.6. Air alternative communications □

C.6.7. Maritime military research – ship communications □

K. KEY INFRASTRUCTURES

K.1. Transport infrastructures

K.1.1. Air traffic management □

K.1.2. Rail traffic management □

K.1.3. Road traffic management □

K.1.4. Maritime traffic management □

Other, which?: □

K.2. Space Infrastructures

K.2.1. Space segment infrastructure protection and service enhancement □

K.2.2. Ground segment infrastructure protection and service enhancement □

K.2.3. Launch segment infrastructures enhancement (e.g. CGS) □

K.2.4. Service synergies (e.g. Copernicus, Galileo, SSA) □

K.2.5. Military space segment infrastructure protection and enhancement □

K.2.6. Military ground segment infrastructure protection and enhancement □

Other, which?: □

K.3. Institutional Communications

K.3.1. National diplomacy (e.g. connectivity between HQ and remote sites, dedicated secure lines of communication) □

K.3.2. EU delegations out of the EU □

K.3.3. Connectivity to the ECHO field offices out of the EU □

K.3.4. EU High & Special Representatives □

K.3.5. EUROPOL network □

K.3.6. Police routine operations □

Other, which?: □

K.4. Other Critical Infrastructures

K.4.1. Energy grid infrastructures – backup communication link □

K.4.2. CBNR Infrastructures – backup communication link □

K.4.3. Financial Infrastructures (e.g. National or EU institutions) – backup communication link □

K.4.4. Telecommunications Infrastructure (e.g. secure backup link, interconnection between systems) □

K.4.5. ICT infrastructure □

Other, which?: □

SU. SPECIFIC USE CASES FOR CIVIL AND MILITARY USERS

SU-P. Polar Regions

SU-P.1. Surveillance services □

SU-P.2. Diplomatic activity e.g. international actions □

SU-P.3. Protection of space infrastructure □

SU-P.4. Air Traffic Management (ATM) □

SU-P.5. Crisis management missions □

SU-P.6. Military operations in the Arctic □

SU-P.7. Dissemination of space data in the Arctic regions □

Other, which?: □

SU-R. UAV/RPAS Beyond Line-of-Sight Communication – Aerial SatCom

SU-R.1 UAV/RPAS Command & Control communications □

SU-R.2. UAV/RPAS sensor data transmission □

Other, which?: □

SU-M. M2M & IoT communication

SU-M.1. Secure and cost-effective M2M communications □

SU-M.2. IoT secure applications □

Other, which?: □

Other use cases:

Please, provide details on other use cases of GOVSATCOM services not identified above that might be of intersest for your entity.

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

E.1. USE CASE SPECIFIC REQUIREMENTS

The following questions should be answered considering the specific Use Cases of interest for your entity selected in previous section D, for which specific requirements are needed.

(please duplicate Sections E.1 and E.2 if you need to answer for more than one use case family)

USE CASE FAMILY
Please choose from the list,
or indicate other:

15. For this particular use case, which services do you expect to use?

Voice-only services □
(including in remote locations, fixed and on-the-move)

Transmission of content in one direction (Broadcast services) □
(e.g. TV)

High-speed data connection (Fixed Broadband services) □
(e.g., high-speed internet, B2B, OTT, DHT)

High-speed data connection on the move (Mobile Broadband services) □
(e.g., onboard airplanes, vessels, trucks or other vehicles)

Low data-rate services □
(e.g. IoT, machine-to-machine (M2M) services, fixed and on-the move)

If other, which?:

16. What type of data or application would you like to transmit/use in this specific use case?

Real-time video streaming □
Video conferencing (2 directions) □
Video non-real time (e.g. TV) □
Voice calls (e.g. teleconference, phone) □
Voice over IP □
Radio services (e.g. voice messaging, push-to-talk) □
Real-time content sharing (e.g. images, messaging) □
Other non-real time data transmission (e.g. email, Internet access) □
Inter-systems data transmission □
(e.g. satellite/UAV payload data transmission, satellite/UAV telemetry and telecommand links)
Remote and secured access to specific information systems or databases □
IoT applications □
Network backhauling (e.g. satellite backhaul for 5G networks) □
Other, which? □

17. What parameters would be key to using the secure SatCom services for this use case?

Please choose from the options presented for each parameter.

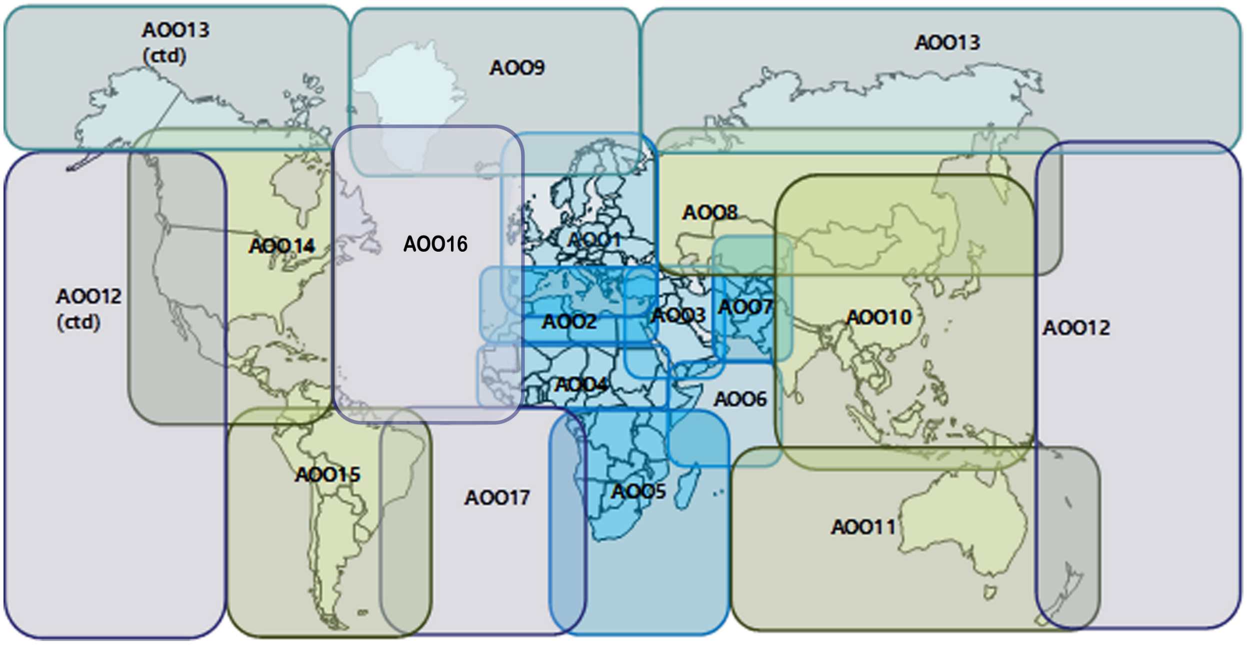


Figure 1- Geographical areas of operation (© EDA)

Geographical coverage *(please, refer to Figure 1 to select the areas of coverage or, if more than 3, specify in "other" the coverage expected for the use case)*	Area of interest: Choose geographical area, Area of interest: Choose geographical area, Area of interest: Choose geographical area. If other (e.g. global, continent), which?:
Capacity (Data rate (Mbps))	Choose capacity need
Frequency band (if known)	Choose frequency band If other, which?:
Seamless continuous service (i.e. handover)	No ☐ Yes ☐
How long do you need the system/service to be deployed for?	Choose service duration
Do you need static terminals or mobile ones?	Static ☐ Mobile ☐ Both ☐
Is occasional data loss in transmission acceptable, or is it vital that every message get through reliably?	Occasional data loss: Acceptable ☐ Not acceptable ☐
Do you need to have the data in real time or some delay is acceptable?	Real-time ☐ Some delay acceptable ☐ Do not know ☐
Expected deployment time of the service (i.e. time from service ordering to the service being operational)?	Select the deployment time

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

18. Is there any specific security requirements for this use case?

	Check if relevant	Required classification level in operations
Resilience and protection against jamming and interference:		
- resilience *(technical and procedural means for quick remedy any interference and interruption occurring on a service)*	□	
- robustness to interference *(elimination of unwanted signals during communication)*	□	
- anti-jamming *(prevention against signal disruption)*	□	
Cyber resilience and protection *(elimination of entry points for cyberattacks on users' information systems)*	□	
Data encryption	□	Select EUCI level.
Controlled access to services	□	Select EUCI level.
Controlled access to infrastructures and control centres	□	Select EUCI level.
Non-dependence from third parties	□	
Authenticity	□	
Non-repudiation	□	
Others, which?:	□	

In case your use case is linked to safety related applications, please provide any specific security aspect to be considered (e.g. EGNOS (ARAIM), ATM (SESAR)):

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

19. **What is / would be the minimum acceptable level of security for the use case and for each of the following services? In case that you need to exchange EUCI, what is / would be the classification level for each of the following services?**

    Please select the minimum acceptable level of security:

    - *Not Applicable*
    - *Authorization & Access Control (e.g. DAC, FBAC, MAC, RBAC),*
    - *Authentication e.g. Password, Challenge-Response, Biometric, Kerberos /Auditing ,*
    - *Communications Layer Security (e.g. VPN, IPsec, SSL/TLS, S/MIME, Firewalls),*
    - *Cryptography (e.g. Hashing, Ciphers, Digital Signatures, Certificates),*
    - *if other, please indicate, which?:*

	Today	
	Level of Security required	**EUCI level need**
Real-time video streaming	Select the level of security.	Select EUCI level.
Video conferencing (2 directions)	Select the level of security.	Select EUCI level.
Video non-real time (e.g. TV)	Select the level of security.	Select EUCI level.
Voice calls (e.g. teleconference, phone)	Select the level of security.	Select EUCI level.
Voice over IP	Select the level of security.	Select EUCI level.
Radio services (e.g. voice messaging, push-to-talk)	Select the level of security.	Select EUCI level.
Real-time content sharing (e.g. images, messaging)	Select the level of security.	Select EUCI level.
Other non-real time data transmission (e.g. email, Internet access)	Select the level of security.	Select EUCI level.
Inter-systems data transmission (e.g. satellite/UAV payload data transmission, satellite/UAV telemetry and telecommand links)	Select the level of security.	Select EUCI level.
Remote and secured access to specific information systems or databases	Select the level of security.	Select EUCI level.
IoT applications	Select the level of security.	Select EUCI level.
Network backhauling (e.g. satellite backhaul for 5G networks)	Select the level of security.	Select EUCI level.
Other, which?	Select the level of security.	Select EUCI level.

E.2. BUSINESS IMPACT ASSESSMENTS

The purpose of these questions is to assess the impact in case of service disruption or in case of performance degradation for a certain period of time, for the specific use case selected in section E.1.

20. How do you rate the impact criticality of service interruption for your mission/operations?

e.g. is SATCOM a back-up communication means or a primary one? Do you have redundancy?
Please choose your answer according to the following scale: 1 – not critical, 5 – catastrophic.

For 1 hour	Choose from 1 to 5
For 12 hours	Choose from 1 to 5
For 24 hours	Choose from 1 to 5
For more than 24 hours	Choose from 1 to 5

21. How do you rate the impact criticality of service degradation for your mission/operations?

e.g. is SATCOM a back-up communication means or a primary one? Do you have redundancy?
Please choose your answer according to the following scale: 1 – not critical, 5 – catastrophic.

For 1 hour	Choose from 1 to 5
For 12 hours	Choose from 1 to 5
For 24 hours	Choose from 1 to 5
For more than 24 hours	Choose from 1 to 5

22. In case of service interruption or degradation, what is the most critical service element for your mission/operations?

Please choose your answer according to the following scale: 1 – not important, 5 – very critical.

Accessibility	Select the level of criticality.
Confidentiality	Select the level of criticality.
Integrity	Select the level of criticality.
Availability	Select the level of criticality.
Bandwidth	Select the level of criticality.
Resilience to jamming or spoofing	Select the level of criticality.
Other, which?:	Select the level of criticality.

23. What is the overall impact for you mission/operations in case of service interruption or degradation?

Safety of citizens (e.g. people's life or health at risk)	□
Economic impact (e.g. mission costs, assets at stake, etc.)	□
Disruption in critical service provision (e.g. critical infrastructures)	□
Security (e.g. uncontrolled borders)	□
Interruption of critical communications (e.g. loss of critical data)	□
Risk of accident (e.g. loss of control links)	□
Political (e.g. diplomacy)	□
Other, which?	□

E.3. ADDITIONAL INFORMATION TO BE CONSIDERED

The purpose of this section is to give the users the possibility of including any additional information considered relevant to specify the future secure SATCOM services in the context of GOVSATCOM Space Programme component.

Click or tap here to enter any additional input that you consider relevant for future GOVSATCOM services definition.

Your inputs can be related either to the specific use case identify, or to general aspects.

Thank you.

ENTRUSTED project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870330.

CLARIFICATIONS AND REFERENCES

- **Information Protection:**
  In the present context, it shall be understood as the preservation of confidentiality, integrity and availability of information (known as the CIA triad). In addition, authenticity and non-repudiation shall be ensured.

  Questions related: Q10

- **Security Aspects of SATCOM services:**
  This term makes reference to potential threats and vulnerabilities of the system in different segments, including space, ground (control and data) and user segments.

  Questions related: Q18

- **(Network) Level of Security:**
  These are security levels related to the physical implementation of the services. Therefore, when answering to this question, the user shall consider the needs and requirements related to the future systems to access the services. The levels considered include:
  - Authorization & Access Control: this level includes control to access the system/service, and determines what this user is allowed to do, once logged into the system/service.
  - Authentication: this levels requires proving the identity of a system user.
  - Communications Layer Security: this is a physical layer of security to protect data traffic streams. Examples of implementation of this level include VPN, IPsec, SSL/TLS, S/MIME, Firewalls, etc.
  - Cryptography: this level includes methods to protect information through the use of codes, so that only those for whom the information is intended can read and process it. Examples include methods and tools as Hazing, Ciphers, Digital Signatures, Certificates, etc.

  Questions related: Q19

- **EUCI Information:**
  The Council decision[1] on the security rules for protecting EU classified information (EUCI) stipulates that communication and information systems need to handle EUCI in accordance with the concept of information assurance. Information assurance in the field of communication and information systems is defined as the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective information assurance must ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity.

  Questions related: Q18, Q19

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN

- **EUCI Classification Levels:**
    - TRÈS SECRET UE/EU TOP SECRET: unauthorised disclosure could cause exceptionally grave prejudice to essential EU or member state interests
    - SECRET UE/EU SECRET: unauthorised disclosure could seriously harm essential EU or member state interests
    - CONFIDENTIEL UE/EU CONFIDENTIAL: unauthorised disclosure could harm essential EU or member state interests
    - RESTREINT UE/EU RESTRICTED: unauthorised disclosure could be disadvantageous to EU or member state interests

Questions related: Q18, Q19

- **Radio spectrum and Frequency bands for SATCOM:**
The radio spectrum is the part of the electromagnetic spectrum with frequencies from 30 Hz to 300 GHz. Parts of the radio spectrum are allocated by the International Telecommunications Union for different radio transmission technologies and applications.
In this questionnaire, it is considered the parts of the radio spectrum allocated to satellite communication services, with the following frequency bands classification (IEEE radar-frequency bands, modified to include Q band and Ka-band military):

HF	0.003 – 0.03 GHz
VHF	0.03 – 0.3 GHz
UHF	0.3 – 1 GHz
L	1 – 2 GHz
S	2 – 4 GHz
C	4 – 8 GHz
X	8 – 12 GHz
Ku	12 – 18GHz
K and Ka	18 to 40 GHz (Ka-band military 30 – 31 GHz uplink, 20.2 – 21.2 GHz downlink)
Q	36 – 46 GHz
V	40 – 75 GHz

Questions related: Q17

ENTRUSTED project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 870330.

SURVEY ACRONYMS

ARAIM	*Advanced Receiver Autonomous Integrity Monitoring*
AOO	*Area Of Operation*
ATC	*Air Traffic Control*
ATM	*Air Traffic Management*
BLoS	*Beyond Line-of-sight*
BW	*Bandwidth*
CBNR	*Chemical Bacteriological Nuclear and Radiological*
CFSP	*Common Foreign and Security Policy*
CSDP	*Common Security and Defence Policy*
CSG	*Centre Spatial Guyannais*
DHT	*Direct-to-home TV*
EC	*European Commission*
EGNOS	*European Geostationary Navigation Overlay Service*
ESOC	*European Satellite Operation Center*
EU	*European Union*
EUSST	*European Space Surveillance and Tracking*
FoA	*Field of Application*
GNSS	*Global Navigation Satellite System*
GOVSATCOM	*Governmental Satellite Communications*
HLUN	*High-Level User Needs document*
HQ	*Headquarters*
IoT	*Internet of Things*
M2M	*Machine to Machine*
MS	*Member State*
OTT	*Over-the-top messaging*
PoC	*Point of Contact*
RBAC	*Role-based access control*
RPAS	*Remotely Piloted Aerial System (same as UAV)*
SAR	*Search and Rescue*
SATCOM	*Satellite Communication*
SESAR	*Single European Sky ATM Research*
SLA	*Service Level Agreement*
TBC	*To Be Confirmed*
TBD	*To Be Defined*
TT&C	*Telemetry, Tracking and Command*
TV	*Television*
UAV	*Unmanned Aerial Vehicle*
URD	*User Requirements Document (this document)*
VSAT	*Very small aperture terminal*