ESTONIAN SPACE OFFICE / ESA GSTP E3

Space Cyber Security 4th Call for Ideas

Step 1: Request for Information about Estonian Payloads to be Validated in Space

Cover letter

1. BACKGROUND INFORMATION

The growing trend of digitalization of the space sector and the growing number of satellites in orbit creates new cyber threats. Space infrastructure or services, which affect our everyday life on Earth, are vulnerable to hacking by third parties. Therefore, it is necessary to focus on preventing malicious activity on board satellites and ground stations to protect the confidentiality, integrity and availability of system logs, data, and services.

The competence of Estonian companies in developing cybersecurity solutions is internationally recognized. Thanks to Estonian full membership in the European Space Agency (ESA) new avenues are opened for Estonia in the field of **Space Cyber Security**. ESA needs sophisticated new technologies to protect space assets and data. To gather preliminary ideas and recognize motivation for cooperation with ESA, the Estonian Space Office is opening a call for ideas described in more detail below.

2. THE SPACE CYBER SECURITY 4TH CALL FOR IDEAS

The aim of the 4th Call for Ideas is to find payloads developed in Estonia AND use those payloads to validate or test new cyber security technology/application in space and develop cooperation among Estonian companies.

The 4th Call for Ideas comprises two steps, which must both be successfully completed in order to be eligible for funding:

1. **CURRENT STEP 1**: In the first step we are requesting information about payloads or satellite subsystems with a minimum TRL5 developed by Estonian entities that could fly onboard of a satellite to Earth orbit.
2. **UPCOMING STEP 2 (TO BE ANNOUNCED)**: In the second step we are looking for consortiums of Estonian entities that could use the proposed payload to validate or test their technology/application in space.

3. WHAT WE ARE LOOKING FOR IN STEP 1:

i) Description of a payload or satellite subsystem developed by an Estonian entity. The description must include technical information about the payload.
ii) The proposed payload has to be today at least TRL5 with the aim to achieve TRL9 by the end of the project.
iii) The payload can be for example: camera, communication subsystem, command and data handling system, electrical power system, energy storage, etc.
iv) Reuse of existing and mature technologies is accepted as part of the solution but will not be double funded.
v) Existing payload can be improved during the project.
vi) The proposed payload must have potential to be used as part of a cyber security technology demonstration or exercise. In the second step of the 4th Call for Ideas we

will be looking for applications that could be combined with an existing payload from this call.

vii) Feasibility studies are not accepted.

4. SUBMISSION DEADLINE

1st March 2022 (the due date will not be postponed)
Ideas should be presented in free form as a Word document and submitted as an e-mail attachment to the Estonian Space Office.
Please cover:

1. Overview of the entity owning the IP and other entities involved
2. Description of the payload/subsystem
3. Budgets (power, link, etc.)
4. Interfaces
5. Estimated time to deliver
6. Estimated cost of payload
7. Description of potential use case

To: kosmos@eas.ee
Cc: Madis.Vooras@eas.ee; Paul.Liias@mkm.ee; Marily.Hendrikson@mkm.ee

5. WHAT HAPPENS NEXT?

i) All submitted proposals will be reviewed by the Estonian Space Office and all proposals in line with the scope of the call will be forwarded to experts in ESA.

ii) ESA experts look for potential satellite missions which could host the Estonian payloads.

iii) A list of payloads and satellite missions where they could fly will be distributed for the second step of the 4th Call for Ideas. We are looking for cyber security applications that could be combined with payloads (March 2022).

iv) In the second step consortiums of the payload and cyber security application owners are invited to submit proposals to be validated in space. Potential applications are connected to cyber ranges, integrity of data, security monitoring solutions, encrypted communications, cyber threat intelligence (CTI), hackathon missions, etc. (spring 2022).

v) Only payloads with a strong consortium and integrated to an application can fly to space. Payloads without application shall not qualify.

vi) The Estonian Space Office will inform each proposer whether their idea was selected (summer 2022).

vii) If selected, a Statement of Work will be created in cooperation with ESA and the Estonian Space Office. This will be followed by an invitation to tender under ESA GSTP (summer–autumn 2022).

Disclaimer: Ideas are not the subject of Intellectual Property Rights. Submitted ideas will only be shared with persons relevant to the decision-making process. In case your idea is selected for funding, it will also be shared with persons involved in preparing the Statement of Work.