# Cyber Security for SMEs, local public administration and Individuals

Taking into consideration the adequate level of security commensurate with the considered use-case, proposals may address one of the following types of end-users:

- SMEs,
- local public administration,
- individual citizens.

To identify the most wide spread threats and cyber security issues facing end-users, proposals should take into account the guidance documents, best practices and standards issued by International Standardisation Organisations, technical forum and Member State Authorities which are tailored for SMEs or Individuals and actively contribute to their development or improvement.

Proposals should develop innovative solutions with a high degree of usability and automation while ensuring that the end-users retain an adequate degree of cyber situational awareness and control.

Factors going beyond technological solutions and focusing on psychological and behavioural factors (including gender) that affect cyber security at individual or organizational levels should be addressed.

Proposals are expected to validate their work through extensive end-user feedback and participation in the consortium where appropriate.

Proposals have to address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users.

The outcome of the proposals are expected to lead to development up to Technology Readiness Level (TRL) 6 to 7; please see part G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU between EUR 3 and 4 million would allow these areas to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Europe's SMEs, local public administration and citizens face particular challenges in addressing basic cyber security threats.

On one hand, in the case of SMEs and local public administration, their size and budgetary constraints often precludes them from putting in place highly granular organisational structures, retaining dedicated information security personnel and making significant investments in cybersecurity products or services.

Individuals, constantly portrayed as the ""weakest link"" face the daunting task of having to constantly adapt their behaviour at home and in the workplace and the way they use both their personal or work-related IT equipment and devices in order to avoid falling prey to the latest threats and techniques that malicious actors leverage against them.

Moreover, whether addressing SMEs, local public administrations or individuals, few cyber security solutions have been designed with the human factor in mind and therefore present severe limitations in their usability which hampers proper decision making and adequate usage.

- Increased competiveness of European ICT security products and services catering to the needs of SMEs, local public administrations and individuals.
- Increased resilience against widespread cyber security threats facing SMEs, local public administrations and individuals.
- Increased effectiveness of cybersecurity solutions through usability advancements and increased automation.

**Last update:** 12 April 2024

**Permalink:** https://cordis.europa.eu/programme/id/H2020_DS-02-2016