

Proposal Evaluation Form



EUROPEAN COMMISSION

Horizon 2020 - Research and Innovation Framework Programme

Security Scrutiny - Evaluation Summary Report

Call: H2020-BES-2015
Funding scheme: Research and Innovation action
Proposal number: 700626
Proposal acronym: iCROSS
Duration (months): 36
Proposal title: Intelligent Portable ContROI SyStem
Activity: BES-05-2015

N.	Proposer name	Country	Total Cost	%	Grant Requested	%
1	European Dynamics Luxembourg SA.	LU			863,000	19.17%
2	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	EL			600,000	13.33%
3	STREMBLE VENTURES LTD	CY			345,000	7.66%
4	THE MANCHESTER METROPOLITAN UNIVERSITY	UK			387,988	8.62%
5	ITTI SP ZOO	PL			276,750	6.15%
6	EVERIS AEROSPAZIAL Y DEFENSA SL	ES			437,000	9.71%
7	BioSec Group Kft.	HU			226,250	5.03%
8	JAS technologie sp. z o.o.	PL			512,250	11.38%
9	GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER	DE			346,640	7.70%
10	Országos Rendőr-főkapitányság	HU			146,250	3.25%
11	Karpacki Ośrodek Wsparcia Strazy Granicznej imienia 1 Pułku Strzelców Podhalanskich w Nowym Saczu	PL			96,750	2.15%
12	TRAINOSE METAFORES-METAFORIKES YPIRESIES	EL			165,000	3.67%
13	EPIVATON KAI FORTIOU AE	LV			99,000	2.20%
	Total:				4,501,878	

Abstract:

iCROSS envisages to enable faster thorough border control for third country nationals crossing the borders of EU, with technologies that adopt the future development of the Schengen Border Management. The project will present an optimal mixture of an enhanced, voluntary form of a Registered Traveller Programme and an auxiliary solution for the Entry/Exit System based on involving bona fide travellers. iCROSS designs and implements a system that adopts mobility concepts and consists of a two-stage procedure, designed to reduce cost/time spent per traveller at the crossing station. It leverages software and hardware technologies ranging from portable readers/scanners, various emerging and novel subsystems for automatic controls, wireless networking for mobile controls, and secure backend storage and processing. The two-stage procedure includes: (A) the registration before the travel to gather initial personal, travel document and vehicle data, perform a short, automated, non-invasive interview with an avatar, subject to lie detection and link the traveller to any pre-existing authority data. Utilizing multifactor analytics and risk-based approach, the data registered is processed and correlated with publicly open data or external systems such as the SIS II. Processing will need the travellers consent as set in EU legislation and national law. (B) the actual control at the border that complements pre-registered information with results of security controls that are performed with a portable, wireless connected iCROSS unit that can be used inside buses/trains or any point. Multiple technologies check validity and authenticity of parameters (e.g. travel documents, visa, face recognition of traveller using passport picture, real-time automated non-invasive lie detection in interview by officer, etc.). The data collected are encrypted, securely transferred and analysed in real time, providing an automated decision support system for the border control officers.

Evaluation Summary Report

Evaluation Result

Status: **Security issues**

Form information

- 1 - No security concern
- 2 - No classification and recommendations for the Grant Agreement Preparation
- 3 - Restreint UE and recommendations for the Grant Agreement Preparation
- 4 - Confidential UE and recommendations for the Grant Agreement Preparation
- 5 - Secret UE and recommendations for the Grant Agreement Preparation
- 6 - Recommendation not to finance the proposal

Security Scrutiny

Status: **Security issues**

Please select one value

No classification and recommendations for the Grant Agreement Preparation

Recommendations or Justification

A Security Advisory Board (SAB) should be set up with representatives from the consortium and end-users with sufficient knowledge of security issues to assess the sensitivity of the following deliverables prior to publication: D2.1, D2.2, D3.1, D3.2, D3.3, D4.1, D4.2, D6.3 and D6.4. The dissemination of any sensitive content should be limited to the consortium.