Project number	Applicant's name	Ctry	Title	Description	Grant
HOME/2012/CIPS/AG/4000003747	UNIVERSITY CAMPUS BIO-MEDICO OF ROME	IT	*Security Liaison Officer - SLO*	In the absence of any indications, quite all the ECIs (and also several National CIs) have designed their Security Managers and/or Crisis Managers (SCMs) as LO. However, this generated a jeopardised situation because SCMs often have very different competences, roles and responsibilities inside their organization. This introduces an element that, instead of facilitating the protection of the ECI, might represent a barrier for information sharing and cooperation. In this framework, SLO aims to contribute to define a profile of LO in terms of competences, leadership, responsibilities, skills and roles at organisational level	181.076,75 €
HOME/2012/CIPS/AG/4000003748	FEDERAL HIGHWAY RESEARCH INSTITUTE	DE	*All-Hazard Guide for Transport Infrastructure - ALLTRAIN*	The objective of the project AllTraIn is the conceptualization of a comprehensive and structured all-hazard guide for critical transport infrastructures in Europe. The holistic approach for the identification of threats for transport infrastructures ensures that all kinds of hazards are considered. Furthermore, criteria for the identification of important infrastructures are developed. These criteria are combined with the before mentioned threats into a qualitatively assessed compilation of different threats and different transport infrastructure. The final guide enables the owner/operator of transport networks to identify, on the one hand, the relevant threats for his infrastructure and, on the other hand, the types of infrastructures in his network which are susceptible to a specific threat	644.496,60 €

HOME/2012/CIPS/ AG/4000003750	PORT INSTITUTE FOUNDATION OF STUDIES AND COOPERATION OF THE VALENCIA REGION	ES	*Collaborative Cyber/Physical Security Management System - CYSM*	The main goal of the two year CYSM project is to substantially enhance the protection of the ports' CIIs, on the basis of a holistic approach, which takes into account their dual cyber-physical view. Objectives: -Analyse the whole spectrum of ports' CIIs threats ; Provide a dynamic risk management methodology (CYSM-RM) for the ports' CII considering their physical-cyber nature; Develop a collaborative security management system (CYSM system)	601.951,25
HOME/2012/CIPS/ AG/4000003752	TECNALIA RESEARCH & INNOVATION FOUNDATION	ES	*Resilient Critical Infrastructures for Physical and Cyber Security Convergence - RISC*	The main RISC project objective is to develop a convergence model for cyber and physical security management in the operation of CI. A common collaborative and convergent approach must put the focus on operational resiliency management and develop an overall strategy to deal with risks associated with the business of operating a CI and ensuring that all its services are safely delivered.	243.022,75
HOME/2012/CIPS/ AG/4000003757	PRIME MINISTER'S CABINET OFFICE - DEPARTMENT FOR INFORMATION AND SECURITY	IT	*a Social Network Analysis Platform for the Support of european and HOmeland Threat prevention strategies - SNAPSHOT*	The SNAPSHOT project aims at increasing the global security awareness of critical infrastructure operators (CIOs) by developing a ground-breaking software platform for monitoring and assessment of evolving threats based on premium and exclusive methodologies of open source intelligence. Particular emphasis is brought upon the analysis of online social media, which are considered invaluable sources for intelligence, since they contain evidence of opinion trends, population response to critical events and therefore may provide key elements of policy and decision making in the realm of critical infrastructure security.	912.109

HOME/2012/CIPS/ AG/4000003759	POLITECNICO OF MILAN FOUNDATION	IT	*Multi-level Alignment of Regional Approaches to Critical Infrastructure Resilience by Learning from Experience - MIRACLE*	MIRACLE is a 24 months project, that aims at supporting coherent regional Critical Infrastructure Protection and/or Resilience (CIP/R) strategies, in order to improve existing capacities of the EU Member States to prevent, prepare and protect people against security related risks, including terrorist attacks.	308.986,40
HOME/2012/CIPS/ AG/4000003768	ESTONIAN POLICE AND BORDER GUARD BOARD	EE	Fight and Investigation of Cyber Attacks Against Critical Governmental Infrastructures -FICAACI 2012	The aim of the project is a Simulated Virtual Attack (SVA), in which one of Estonian critical infrastructure will be attacked and where attackers and/or their data will be in different countries. Implementation of counter-measures and at the same time gathering of evidences by different countries agencies, which need co-operation at national and international level and between different bodies	218.004,00
HOME/2012/CIPS/ AG/4000003772	ALLIANDER NV	NL	*Distributed Energy Security Knowledge - DEnSeK*	This project proposal aims at contributing in the improvement of the security of Energy Smart Grids by creating a multi-layered knowledge sharing base on the Cyber Security matters along a three dimensional plan: technical plan, policy plan, inter-national/inter-organizational plan.	763.241,44
HOME/2012/CIPS/ AG/4000003773	PROVINCE OF NOVARA	IT	*Identification of threats against critical infrastructures and decision support- TIDES*	The objective of TIDES is to evaluate the potential of a knowledge based approach to point out, assess and rank potential threats to critical infrastructures (as defined by the Directive 2008/114/EC) and to identify action plans to reduce risk, preventing the occurrence of critical events or at least mitigating their effects through effective management of the subsequent emergency situations.	380.234,61
HOME/2012/CIPS/ AG/4000003774	The urban Planning Institute of Ljubjana	SI	*Risk Management of Transport of Hazardous Substances on the Main Road Network - RMTHS*	The general objective is to develop the methodology of monitoring and management of transport of hazardous substances with proposed scenarios of measures for the risk events on the main road network in real time with GIS application	576.502,54

HOME/2012/CIPS/ AG/4000003777	FORMIT FOUNDATION	IT	*Assessing security awareness and increasing Maturity LEvel of Transport Operators to strengthen Critical Infrastructure Protection - AMLETO*	The AMLETO Project aims at raising awareness and the sense of urgency of Critical Infrastructure Protection (CIP) among operators, in order to fill the gap in wakefulness and preparedness to the threats in different Member States. This main objective is strongly related to the 5 Transport sub-sectors mentioned in the Directive (Road transport, Rail transport, Air transport, Inland waterways transport, Ocean and short-sea shipping and port).	211.291,16
HOME/2012/CIPS/ AG/4000003782	D'APPOLONIA S.P.A.	IT	*Secure Smart Grid - SESMAG*	The arising need for more secure critical infrastructures and the need for a common approach at European on their securitization find their natural expression in SESMAG. In fact, the project will ensure a low cost and replicable study for the evaluation and implementation of a minimum set of security requirements to make the Smart Grids more secure. The study aims at providing a set of guidelines to define how to implement secure smart grids and, on a scenario basis, a set of requirements/measures to be implemented by the stakeholders. Such an approach will allow for a convergent approach across Europe towards a secure implementation of the Smart Grids and the of the energy infrastructures, ensuring a more reliable energy production and distribution across the network. The project outcome will ensure an increased resilience of the energy networks to cyber attacks and physical outages due to misconfiguration of the connected producing systems or unbalanced distribution and production algorithms.	315890,96

HOME/2012/CIPS/ AG/4000003783	UNIVERSITY OF PIEMONTE ORIENTALE	IT	*Formal Methods: Business Impact of Application to Security relevant Devices - FM-BIASED*	FM-BIASED is a study project on the establishment of the business impact of formal methods concerning compliance to the above standards in several industrial and business sectors where such regulations are enforced or will soon be enforced. In most of those sectors, compliance verification may be difficult because most automation are legacy systems, so that industrial stakeholders must face the prospect of either trying to validate ageing systems designed many years ago, or redesigning/re-implementing their functions anew. Although the study project scope will be limited to a few EU countries and some industrial sectors, its conclusive findings will be presented in an international Conference, so as to pave the way to broader uptake across Europe:	373.955,27
HOME/2012/CIPS/ AG/4000003789	SPANISH TECHNOLOGY PLATFORM ON INDUSTRIAL SAFETY	ES	*Increasing Security Awareness of Critical Infrastructure OPerators introducing Intelligence Techniques and focusing on Psycho-social and Human factors- PSOPHIA*	The objective of PSOPHIA is increasing the security awareness of CI operators, applying Human and Artificial Intelligence techniques and focusing on psycho-social factors in order to fill a gap in the operators' general security knowledge as well as their threat perception and alertness. It will also address the lack of coverage of human factors in existing risk analysis and management, integrating security vulnerabilities originated by the operators' specific psycho-social conditions and involving coordination among HR and production or other Departments	311.060,26

HOME/2012/CIPS/ AG/4000003792	SUB-DIRECTORATE GENERAL FOR PLANNING AND INFRASTRUCTURES MANAGEMENT AND MATERIAL FOR SECURITY	ES	*Critical Infrastructure: Improvement of Security Control against the Terrorist Threat - CIISC-T2*	The projects aim to promote information exchange on cyberterrorism and the use of the net for radicalization purposes among European authorities and between public and private sectors. Guidelines will be the result of promoting that information exchange, Exercices will be ran with a view to protect critical infrastructure in cyberspace - mainly from cyberterrorist threats, to raise awareness between critical infrastructure operators,to provide a training environment close to reality, and to foster information exchange among operators and Member states.	523397,5
					6.565.220,49