Project number	Applicant's name	Ctry	Title	Description	Grant
JLS/2007/CEN/001	The European Committee for Standardization - int. org	BE	*Standardization activities on critical infrastructure protection - support to the CEN*	Workshop1Emergency Services Management - ESM- The objective is to improve these servives by enabling the various services to co-operate internally and across the borders on a common basis within a signle master process. Participating stakeholders: Experts from emergency services, e.g. fire fighters, police, embulance personnel, armed forces, specialised disaster services, existing cross border co-operation schemes, procurement officers, certification institutions . The deliverable of the CEN workshop will be a CEN Workshop agreement which will over the following aspects: Co-operation between different services, effective use of emergency services by decision makers; international co-operation of emergency services; a commo basis for the evaluation of the service activities, common recommendations for quality improvement; efficiency of the services and health and safety; interoperability of products and services.Time frame: 22 months Workshop2 Personal Protective Equipment for chemical, biological, radiological and nuclear (CBRN) hazards. The proposed Workshop will allow CBRN PPE issues to be discussed and debated in a dedicated environment, with a view to reaching consensus on a CEN Workshop Agreement, in order to facilitate the manufacture of PPE that protects adequately CBRN hazards. The deliverable for this CEN Workshop will be a CEN Workshop Agreement. Participants: a range of companies producing relevant equipment. It is expected that the Workshop will interest such companies, as well as public administrations and agencies, and companies and associations in critical areas potentially needing to use the equipment. Timeframe: 18 months starting from the kick-off meeting	103,531.00
JLS/2007/CIPS/003	Estonian Public Service Academy (EPSA)	EE	*Safe- and Secure-Innovation in Law Enforcement Education / Safe- and Secure.*	The general objective of the project is to improve National Authorities' and Law Enforcement Agencies' readiness, capabilities and flexible co-operation in prevention and crisis-management of new challenges of acts of terrorism and trans-national crime via innovative curriculas, joint training methods and tools both in national and regional as well as EU-levels.	405,235.00
JLS/2007/CIPS/004	Ministry of Interior Brandenburg	DE	*Wandlungsfähige Schutzstrukturen und Folgenabschätzung zur Prävention, Abwehr und Folgenbewältigung bei Katastrophen*	The project will examine critical infrastructure, the respective protection concepts and the cooperation of relevant organisation in case of a catastrophe, in terms of their adaptability. Adaptability is defined as the capability of a system to adapt and react efficiently and quickly to changing requirements. And is particularly relevant in light of catastrophic events. Moreover, indicators are to be identified and operationalised in order to measure the degree of adaptability and on this basis, make further recommendations to increase the respective adaptability. Furthermore, an integrated process regarding the impact assessment of catastrophe and protection concepts will be developed, which can then be used in a transborder, scalable and participative manner that is independent of domains.	137,109.20
JLS/2007/CIPS/006	Insurance and Bank Consumer Association	ES	*Creation of an European technical catalogue of the fraud at the disposal of the judicial and police authorities on the basis of a net of alerts and information facilitated by entities and citizens*	The project's purpose is the prevention and integral eradication of electronic payment fraud with due regard to supporting the transnational dimension of this phenomenon as well as giving assistance to victims of such crimes. It also aims to improve the association between (among) the public and private sector, the cooperation with NGOs, the judicial and penal system and other professional bodies in order to develop strategies and instruments that could combat crimes in the field of electronic payment.	184,641.68

JLS/2007/CIPS/007	Warsaw Metropolitan Police	PL	*Safe airports in the face of terrorism threats in present Europe*	The project concentrates on a simulation exercise that will be organised during an international seminar in Warsaw. The scope of the seminar is to discuss the security and preparedness system of European airports in face of a potential terrorist attack. Additionally, security and rescue units working at the airport will be engaged into the simulation exercise: Police, Boundary Guards, Fire Guards, Airport Security, Ambulance Service. The simulation will consist of an evacuation procedure generated by a suspected luggage that is left in airport area as well as a rescue procedure against explosion. During the exercise a movie is going to be made. It will contain professional instructions of behaviour in critical situations and cooperation with rescue forces.	42,356.80
JLS/2007/CIPS/008	Telespazio	IT	*Space Infrastructure through Satellite Imagery*	The project foresees activities such as: analysis of the use of EARTH OBSERVATION satellites for monitoring and control human activities around critical infrastructure and borders; Earth Observation satellite based on microwave and passive technologies present status and future development; non-satellite detection system for human activities; data fusion and GIS technology integration; definition, classification and detection requirements of typical human activities around critical infrastructure and borders; coordination with the ongoing project on GMES and GMES approach to security; identification of GMES limitation; general architecture identification and new possible satellite constellations; simulation of sensor detection and feasibility with present technologies and evolution; definition of a viable satellite scenario in the next 15 years: related technologies and cost estimation.	245,885.67
JLS/2007/CIPS/009	Telespazio	IT	*SecureSPACE*	Activities: description [leader, start month – end month] WP110: Analysis of the use of satellite technologies in the overall economy structure [TPZ, 1M-4M] WP120: Analysis of satellite technology in Emergency Operations [DLR, 1M-4M] WP211: Analysis of the Risks on Comm. satellite disruption: Jamming, Earth segment, space segment (Economy) [DIA, 3M-9M] WP212: Analysis of the Risks on Comm. satellite disruption: Jamming, Earth segment, space segment (Emergency operations) [DLR, 3M-9M] WP221: Analysis of the Risks on Navigation satellite disruption: Jamming, Earth Segment, Space Segment (Economy) [DIA, 3M-9M] WP222: Analysis of the Risks on Navigation satellite disruption: Jamming, Earth Segment, Space Segment (Emergency operations) [TPZ, 3M-9M] WP310: Risk assessment of the disruption of Comm. satellite functionalities for the various economy sectors [GMV, 9M-17M] WP320: Risk assessment of the disruption of Navigation satellite functionalities for the various economy sectors [GMV, 16M-24M] WP410: Risk assessment of the disruption of Comm. satellite functionalities for the Emergency Operations [DLR, 9M-17M]	246,012.04

				Deliverables (month): D1: analysis of satellite technologies in overall economy structure and emergency operations (M4) D2: analysis of risks on communications (jamming, earth segment, space segment) (M9) D3: analysis of risks on navigation (jamming, earth segment, space segment) (M9) D4: risk assessment in economy sectors (M17, M24) D5: risk assessment in emergency operation (M17, M24) Milestones/outputs (month) M1: analysis of risks in the defined scenarios (M9) M2: risk assessment in economy sectors (M17) M3: risk assessment in emergency operations(M24)	
JLS/2007/CIPS/010	Symantec LIRIC Limited	UK	*Energy Control Center Risk Assessment and Migration Methodology*	The project's objective is to develop the methodology, the guidelines and tools to assess the overall security risks, including technical, procedural, and infrastructural aspects of Transmission System Operators (TSO) Control Centres. And implement enhancements in a manner that provides resilience, operational availability and survivability. In addition, the applicant will collaborate with two partners, which will support the definition and validation of the necessary methodology together with the implementation of the security plan defined during assessment.	700.000,00
JLS/2007/CIPS/012	FORMIT – Foundation for Technology Migration and Research	IT	*Critical Events Management Model*	The project's aim is to guarantee a more efficient transnational cooperation for the prevention and management of emergency and crisis situations and of their related risks. This will be achieved through an identification and recognition of worldwide already implemented best practices for the management of metropolitan events, which have taken place in the last 5 years and which involved the management of large population masses.	184.340,00
JLS/2007/CIPS/013	FORMIT – Foundation for Technology Migration and Research	IT	*The Vulnerability of Information Systems and its intersectorial, economic and social impacts*	The aim of the proposed project in the context of the protection on Critical Infrastructure is to develop a risk assessment methodology to measure the impact of failures and breakdowns of the information infrastructure on the country economy and more precisely on its production and service processes. By standardising the risk assessment methodology to be shared within the EU countries, this tool will foster an exchange of data and best practices in the EU and may contribute to an enhanced cooperation and coordination among the different actors of crisis management and security actions within the EU.	248.680,00
JLS/2007/CIPS/015	Samarkand	SE	*Assessment and mitigation of risk for disabling control centre of large power networks by international radiofrequency interference*	The overall project objective is to assess the risks for, and take measures to prevent, disabling of the Supervisory Control and Data Acquisition system (SCADA) of electric power control centres via Intentional Radio Frequency Interference (IRFI). At first an IRFI audit of critical control centres and available mitigation technique will be performed. Following that, a resistive sensor prototype capable of identifying an IRFI attack will be developed for integration with other traditional surveillance technology of control centres.	743.753,65
JLS/2007/CIPS/016	The Voivodeship Headquarters of Police in Kraków	PL	*Terrorists at the dam*	The overall objective of the project is to improve co-operation between the Czech, Polish and Slovak Police in the case of an attack on critical infrastructure causing risk for societies on both sides of the border. Furthermore, the specific purposes of the project are the following: development of interagency data exchange on threat of attack; development of risk assessment of consequences from attacks on dams; improving of interoperability during the attack and afterwards (consequence management); exchange of know-how, best practices (transfer of knowledge).	53.956,80

JLS/2007/CIPS/018	National Directorate General for Disaster Management	HU	*Integrated Management for the Protection of the Activities of Critical Infrastructure Technology of Hungary*	The basic aim of IMPACT project is the investigation of the vulnerability of critical infrastructure sectors (water, information-technology and communication). The analysis includes the assessment and analysis of hazards and its visualisation on risk maps as well as drawing conclusions from real case scenarios - with priority to wilfully malignious human behaviour (terrorism).	91.735,35
JLS/2007/CIPS/019	Italian National Agency for New Technology, Energy and Environment	IT	*Definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation / transmission infrastructures*	The project aims to develop a methodological framework to identify and measure the (potentially critical) interdependencies between PS & ICT infrastructures as vital input for network vulnerability and risk analysis. Work streams include: identification of the boundaries and interrelations of the ICT and Power systems; determination of the topological proprieties regarding network structure and nature of interdependency coupling (local, non-local, global), based on the best practices in Graph Theory and Complex Systems Theory; definition of the couplings at service level; analysis and definition of a suitable metric to assess the level of interdependencies for application in network security risk assessment and it's application to the Italian identified practical case study and finally, evaluation of application of the framework to a EU context and dissemination of results.	517.981,00
JLS/2007/CIPS/021	Deloitte	ES	*Octavio: Energy System Control Centres Security, an EU Approach*	Project activities will be focused on: providing an accurate assessment regarding energy sector control centres cyber structure requirements, identifying survivability and resilience requirements for every functionality in electricity and natural gas control centres; defining security audit protocols for different control centre levels; testing audit protocols in at least three different functionality levels; promoting collaboration schemes among energy and ICT network operators and authorities; disseminating results around EU security and energy communities.	475.801,17
JLS/2007/CIPS/022	University of Franche-Comté	FR	*Alert Messages and Protocols*	The project is concerned with the development and transfer of a methodology created by the Coordinator and developed in collaboration with the aircraft industry, the health profession, and with emergency services for establishing standards concerning the writing of messages, alerts and protocols for safety critical applications and which can be easily translated. The project concerns the localisation and application to 4 of the Member States' languages (ES, GB, FR, PL), with the possibility for extension to other Member States.	217.814,08
JLS/2007/CIPS/023	Prefecture of Rome	IT	*Proximity Emergency Network for Common European Communication*	The project's objectives are the study, development and advancement of a European communication strategy, to overcome linguistic obstacles; and the study and development of a communication network architecture (in the following indicated as proximity network) to be used to broadcast to people and operators the contextual multimedia messages.	686.000,00
JLS/2007/CIPS/025	Aston University	UK	*Evacuation Responsiveness: A Preparedness Toolkit for Europe*	The project focuses on methods to "produce well tested plans which can be used to evacuate people from danger zones should an incident occur" (Pidd et al, 1996). Therefore, it develops a 'preparedness toolkit' to support planning/preparation of mass evacuations using models to inform optimal preparedness. It also creates a central knowledge repository for preparedness of the public and Emergency Management Agencies (EMAs) to mass evacuate, and initiates EU-wide collaboration across EMAs (e.g. security, rescue, health).	440.041,59

JLS/2007/CIPS/034	Indra Sistemas, S.A	ES	*Adaptation and roll out of SCEPYLT G-5 "Sistema de Control de Explosivos para la Prevención Y Lucha contra el Terrorismo" (Explosives Control Information System for Terrorism Fight and Prevention) in the 27 EU state members*	The project represents an information system for the control of explosives of civilian use. And is divided in two phases: adaptation and roll out: there are two coordination meetings planned in order to discuss about adaptations, modifications, suggestions; and maintenance and call centre support (6 months). There are two technical visits planned to each Member state to solve technical problems and make suggestions specific to each partner.	680.288,46
JLS/2008/CIPS/001	ISDEFE	ES	*Airport Security Integrated System Evaluation (ASISE)*	The project concentrates on the following activities: assessment of current practices performance, identification and analysis of the gaps in the practices, proposal of best security practices and dissemination to the appropriate audience.	579.284,73
JLS/2008/CIPS/002	Ministry of Interior of the Netherlands	NL	*Cell Broadcast for public warning - Sharing knowledge and experiences and identification and standardisation of (technical) requirements*	The project can be split up into three different activities: sharing knowledge about Cell Broadcast in general, and more specifically sharing knowledge in relation to handsets; compiling functional requirements for handsets used for Cell Broadcast and preparing trials to test the cross-border use of Cell Broadcast.	210.526,51
JLS/2008/CIPS/003	The Swedish Post and Telecom Agency	SE	*Multipurpose Information Management and Exchange for Robustness, Phase 2*	MIMER II is the extension of the MIMER project, its investments and achieved results. The project is built on a combination of methods, technology and common frameworks. Its general aim is to establish a de-facto standard framework for common situation awareness information exchange in the electronic communication sector.	1.068.733,00
JLS/2008/CIPS/004	GENERAL DIRECTORATE OF INTELLIGENCE AND INTERNAL PROTECTION	RO	*Setting-up at the level of Ministry of Interior and Administrative Reform (M.I.A.R.) of an Integrated System for the Management of Terrorist and other Security related Risks to the Critical Infrastructure in the field of Passenger Transport*	The project's overall objective is to conduct evaluation activities in order to improve the legal framework at M.I.A.R's level. In this respect, it concentrates on the identification and definition of terrorist and other security-related risks in the field of passenger transport; setting-up a framework for institutional and inter-institutional cooperation aimed at establishing an integrated management of terrorist risks related to the critical infrastructure of passenger transport. And in accordance with European standards, on the improvement of the analysis and evaluation capacity of DGIPI.	100.990,00
JLS/2008/CIPS/007	Theodore Puskas Foundation	HU	*Framework for Information Sharing and Alerting (FISHA)*	The objective of the project is the framework for the prototype of a European Information Sharing and Alerting System based on already existing national systems. Moreover, the project will set up working groups creating a dedicated web portal, developing and validating a protocol for information exchange and alerting, as well as working out a model for cooperation, project management and dissemination. In this respect, the supporting partners hold a key position.	432.132,64

JLS/2008/CIPS/008	F.S.C. Security consulting, joint stock company	CZ	*Analysis of the Protection of Energy Networks´ Crucial Objects against Terrorism and Proposal of Security Standards*	The project's main focus is on the safety of electricity supply systems. This is an aspect of high importance since failure of such systems in one country as the consequence of crime or terrorist attack can influence significantly the whole economy of the EU. Other sectors of critical infrastructure are depending on electricity supply systems, so these systems must be consider as crucial points. In addition, the project foresees specific activities such as status analysis, security vulnerabilities and risk analysis and subsequently, the proposal for standards regarding security of particular objects categories.	257.834,00
JLS/2008/CIPS/009	The County Administrative Board of Uppsala	SE	*Mass Crisis Communication with the Public Project*	MASSCRISCOM addresses the need for improved protection of the public and infrastructure and two-way crisis communication between authorities and the public. It will build on the high risk conditions in Uppsala i.e. the main highway and rail transport chains between Northern Sweden and Stockholm, a nuclear power plant, several Seveso sites and advanced biochemical and chemical research laboratories.	943.453,70
JLS/2008/CIPS/011	European Chemical Industry Council	BE	*Improve knowledge of effective critical infrastructure protection and facilitate exchange of experiences and best practices*	The project aims at improving critical infrastructure against terrorist attacks. To this challenge, IMPROVE aims at analysing the level of security of industrial installations in Europe and discerning shortcomings and weaknesses. Based on a theoretical and practical analysis, the final objective of this project is to deliver a clear and handy toolkit to be used for filling in existing security gaps in critical infrastructure sites. IMPROVE builds on the SECURE-SITE project carried out in 2006/2007..	604.940,75
JLS/2008/CIPS/012	D'Appollonia SPA	IT	*European Mass-transit System Security Risk Assessment and Audit Methodology*	The EUMASS Project aims at developing an innovative solution for risk assessment and management in Mass-transit System security applications, as part of the EPCIP. The proposed method will draw from the outcomes of the latest programmes developed within the EC, such as COUNTERACT, the EURAM project and the "Protection of Transport Critical Infrastructure at EU Level", the broad experience of the Applicant and its Partners in the engineering of the transport sector. As well as in security and risk assessment projects for transport, defence, and telecommunication applications.	748.674,01
JLS/2008/CIPS/016	Italian National Agency for New Technology, Energy and Environment	IT	*National and European Information Sharing and Alerting System*	The project's objective is the development of a Model and a Pilot Platform for a National and European Information Sharing and Alerting System (NEISAS). This will be based on the results of various EU funded projects; the Information Assurance Messaging Standard (Symantec), the ENISA Study on a European Information Sharing and Alert System, the ENISA Data Collection Framework Study and the Availability and Robustness of Electronic Communications Infrastructures Study (ARECI).	1.034.119,13
JLS/2008/CIPS/018	CESI Ricerca	IT	*ASsessment of resilience to ThReats of cOntrol and data Management systems of electrical transmission network (ASTROM)*	The project's aim is the definition and validation of an innovative methodological framework for the quantitative assessment of the resilience of control and data management systems in electrical transmission networks towards external threats.	990.499,14
JLS/2008/CIPS/022	University Campus Bio-Medico of Rome	IT	*SECUFOOD - Security of European Food supply chain*	The aim of the project is to realise an overview of strategies adopted in the EU in order to prevent terrorist attacks against the supply food chain. To this aim, SECUFOOD proposes to perform such an analysis in a methodological framework that allows the matching of the adopted strategies with the potential threats. This, in turn, gives the possibility to better emphasize best practices, discover dangerous gaps and emphasise those aspects that appear to be under or over estimate.	341.115,00

JLS/2008/CIPS/023	Booz Allen Hamilton Italia LLC	IT	*Development of a Risk Assessment and Countermeasure Audit Methodology for Potential Terrorist Attacks on Mass Transit Systems*	The project aims to develop a framework for a risk assessment and countermeasure auditing methodology capable of assessing the vulnerabilities of mass transit systems (e.g. rail and subways) from potential terrorist attacks. Its specific actions include activities such as analyses of international best practices on risk assessment, audit methodologies and mass transit railway system value chains; identification of potential countermeasures to be implemented; design of a risk assessment and countermeasure audit methodology; testing the risk assessment and countermeasure audit methodology in a pilot area; development and execution of a specific War Game that will involve performing the risk assessment process during a crisis scenario; re-calibration of the methodology based on lessons learned from the pilot and War Game and tailoring the framework to the EU context.	409.000,00
JLS/2008/CIPS/024	TECNUN University of Navarra	ES	*Simulation Exercise to Manage Power Cut Crises (SEMPOC)*	The project relies massively on the involvement of different stakeholders that can provide indispensable tacit knowledge through a Group Model Building (GMB) approach. Therefore, three GMB/SE workshops concerning a large scale power cut will be held with participants from utilities, national and EU regulatory bodies, national emergency management agencies and the EC. Moreover, the project targets first a proof of concept prototype simulation model of an interdependent power production and distribution network, focusing on the ability of agents to deliver society critical services in face of a major power cut. Second, the cascading effects and the asynchronous crisis manifestation. And third, policies to improve the power generation and the system's resilience, response to and recovery from crisis.	762.826,54
JLS/2008/CIPS/025	DNS Infrastructure Resilience Task Force Ltd.	UK	*Initiative for the Development and Coordination of Technologies and Methodologies for Resilience of the DNS Infrastructure in and among European Union Member States*	The project aims to develop and publish a detailed, written analysis of historical DDoS and other coordinated attacks against the DNS infrastructure in Member states, as well as an analysis of vulnerabilities in the DNS infrastructure. Also, to develop and produce a written plan identifying specific technologies for implementation individually or all Member States to aid in the prevention and defence of malicious attacks on the DNS infrastructure. The last aim is to develop and document a secure, web-based methodology that can be implemented in each Member State for the timely sharing of information on attacks, risks, and best practices.	300.000,00
JLS/2008/CIPS/026	Deloitte	ES	*Net Protection: EU Interconnected high voltage electricity grid security approach*	Net Protection project will establish criteria & methodologies to asses and mitigate risks for EU electricity International Interconnections (II) and their interdependent networks. A modelling IT tool will be deployed to evaluate criticality of EU II their vulnerability and assess defence measures.	407.724,66
JLS/2008/CIPS/CEN/001	CEN	BE	*CEN Workshop Agreement for Biosafety Professional (BSP) Competence*	Management of an organisation is responsible and accountable for the safe and secure handling of natural and genetically modified biological agents and toxins handled by the organisation. Therefore it has to ensure the establishment of a bio safety and bio security management program and the appointment of a competent bio saftey professional (BSP). The objective of the project is to develop a standard, through a CEN Workshop Agreement (CWA) process to define the role profile, tasks and skills of a BSP for the adoption at European level.	89.181,00
JLS/2008/CIPS/CEN/002	CEN	BE	*Security of Drinking Water Supply - Guidelines for risk and crisis management*	The project is a standardisation activity to develop a European guideline on risk assessment and crisis management for drinking water utilities. The goal is to improve the security of drinking water supply and to reduce possible effects from security threats.	73.684,75

JLS/2009/CIPS/AG/C1-003	ISDEFE	ES	*Priority Communications for Critical Situations on Mobile Networks*	PROSIMOS assesses the needs for the best suiting technological solution, analyzes and simulates different suitable business models for priority communications to finally disseminate the results to relevant bodies.	385.749,16
JLS/2009/CIPS/AG/C1-010	Police College	HU	*Exch. of best crisis mgmt pract., know-how of The Best Practice of Training Handbook & experiences of EU agencies and participants invd in the set of measures in the fight against terrorism rel. to the protection of electric power plants & the review of security standards and their modification*	The EU-ExTraH is focusing on the prevention of the malfunctions of the European Critical Electric Energy Infrastructures and the prevention of risks related to emergencies (terrorist) attacks in order to provide the continuity of industrial plants and to unify and improve the decision making processes.	116.282,10
JLS/2009/CIPS/AG/C1-013	CYPRUS POLICE	CY	*LEONIDAS - EXERCISE FOR CYPRUS*	Cyprus Police takes the initiative to carry out a large scale national exercise based on the scenario of a real terrorist attack in Cyprus. The attack will supposedly take place during the meeting of the Heads of the Member States during the EuCouncil presidency in Cyprus 2012, as a preparation action for Cyprus Police who is the prime coordinator of the consequent management for all national authorities. Police units such as the Emergency Response Unit (ERU), Counter-terrorism office(CTO), Operat.office, Police Aviation Unit, the Port and Marine Police, Traffic department will take part in the exercise. Cyprus Police takes the initiative to carry out a large scale national exercise based on the scenario of a real terrorist attack in Cyprus. The attack will supposedly take place during the meeting of the Heads of the Member States during the EuCouncil presidency in Cyprus 2012, as a preparation action for Cyprus Police who is the prime coordinator of the consequent management for all national authorities. Police units such as the Emergeny Responce Unit(ERU), Counter-terrorism office(CTO), Operat.office,Police Aviation Unit,the Port and Marine Police,Traffic department will take part in the exercise. The Minister of Justice and Public Order and the Chief of Police will signal the strategy for all operations of this exercise scenario which will include the coordination of other authorities taking part in Cyprus such as Ministry of Health, Fire Dept, the Cyprus Telecommunications Authority (CYTA), the Electricity Authority Cyprus (EAC)and the Cyprus Port Authority (CPA).The crisis centre in Police HQ will operate at the highest level (GOLD).The management and coordination of the exercise will be based on the recommendations of the European Council second peer evaluation mission report on Cyprus(	221.987,34
JLS/2009/CIPS/AG/C1-016	Italian National Agency for New Technology, Energy and Environment	IT	*Modelling Tools for Interdependencies Assessment in ICT systems*	This project is aimed at developing a methodological framework for ICT network inter-dependencies analysis. Special efforts will be devoted to identify critical system inter-dependencies as potential amplifiers of negative impacts upon failures or deliberate attacks. A representative Italian case study will be deeply analyzed, whilst providing general purpose tools. Generally speaking, one expects increases of inter-dependency among the different systems to reduce resilience of the overall system. In this respect, one of the main objectives is to define and implement alert-indicators for crisis prevention and mitigation policy purposes The analysis of indicators may also help CERT's (Computer Emergency Response Teams) to take prompt and effective actions in order to recover an acceptable operational state.	561.260,70

JLS/2009/CIPS/AG/C1-018	FORMIT – Foundation for Technology Migration and Research	IT	*Coordination improvement by Best practices*	The objective of the project is to develop joint exercise scenarios, a conceptual model of coordination and a best practice manual for the coordination among actors in terrorist attacks management. Additionally there will be an analysis of the management of relevant terrorist events in the recent past to identify the best practices and the lessons to be learned.	334.085,85
JLS/2009/CIPS/AG/C1-019	INERIS	FR	*Improving Security with Organization, Limitation of effects and Design*	Protecting critical infrastructure, in particular public spaces such as railway stations, airports, hospitals or high buildings, against terrorist attacks and other antagonistic acts is one of the major challenges of the 21st century. To this challenge, ISOLDE aims at: developing a method for the vulnerability assessment for public areas that may be applicable for new buildings as well as existing ones; developing good practices or codes for the design of new public infrastructures, and also existing ones, considering occurrence and consequences of malicious acts (processes and materials, technical systems, provision of architectural and interior design); developing good practices or codes for the protection of new and existing infrastructures which will integrate technical measures (detection, sensors…) as well as organisational measures (procedures, emergency plans, evacuation…); preparing a specific security documentation; applying this approach to a case study; Three locations are presently proposed: one in London (UK), one in Paris-La Défense (FR) and one in Parma (IT); disseminating the results to security authorities and operators. Based on a theoretical and practical analysis, the final objective of this project is to deliver a clear and handy toolkit being used for filling in existing security gaps in critical public infrastructures. ISOLDE builds on the DG JLS-funded ABVERC project carried out in 2005/2006.	944.450,99
JLS/2009/CIPS/AG/C1-021	Sitep Italia S.p.A	IT	*Maritime Security and Antiterrorism System*	The Maritime Security and Antiterrorism System (MAS) is an integrated, multisensor, turnkey security system designed to reduce the vulnerability of critical infrastructures against terrorist attacks and other threats, e.g. illegal immigration, ecological disasters.	545.580,88
JLS/2009/CIPS/AG/C1-025	ISDEFE	ES	*Modelling of Infrastructure Protection- From Materials To Devices*	Objective: This proposal focuses in protecting critical infrastructure buildings by developing: an evaluation vital areas, an effective modelling tool for structure design able to increase the building resistance to blasts (predictive): including as a solution both, active and passive systems.	517.102,59
JLS/2009/CIPS/AG/C1-026	F.S.C. Security consulting, joint stock company	CZ	*Critical infrastructure protection in energetic sector*	The project builds on the already approved grant project from CIPS program titled "Analysis of the Protection of Energy Networks´ Crucial Objects against Terrorism and Proposal of Security Standards" and now is expanded in the whole field of physical protection of CI in the energy sector, so the proposal of CI protection for whole sector can be created. At the same time it provides support to the EU Member States in the methodology of the CI protection in the field of energy.	345.783,50
JLS/2009/CIPS/AG/C1-028	Inter-department Research Center on Security - University of Modena and Reggio Emilia	IT	*Transport Hub Intelligent video System*	The objective of THIS is to develop new and concrete solutions for handling the human control and identification of people which could create risk situations in crowded scenarios, by means of video analysis. It will propose software tools for people activities and behaviour recognition and surveillance modules, which can be integrated in existing platforms and managed by inspector employers, by means of web interfaces.	468.270,00

JLS/2009/CIPS/AG/C1-030	Indra Sistemas, S.A	IT	*DTN/MANET Routing Study for critical infrastructure protection*	The objective of this project is to define a new communication model capable of improving the security and resilience of critical assets against man made (terrorism) or natural disasters. More specifically, the project proposes to do research on how DTN and MANET technologies can be combined into an hybrid architecture where implementing robust communications systems.	282.203,95
JLS/2009/CIPS/AG/C1-032	The Netherlands National Police Agency	NL	*Modelling against Terrorist Attacks by European Police*	Objectives of the project: To develop, validate, use and maintain knowledge models in order to improve the protection of officials and other individuals in Member States who have special police protection and are under threat from individuals or groups motivated by terrorism. To achieve a better understanding of the resources, preconditions and methodologies needed to develop, use and maintain the models. To develop common European standards ('a common language') regarding models to facilitate their exchange between (police) organisations in Member States.	272.481,22
JLS/2009/CIPS/AG/C1-036	Netherlands Organisation for Applied Scientific Research TNO	NL	*CIP Good practices manual for policy makers*	The objective of this proposal is the development of a manual containing good practices for Critical Infrastructure Protection (CIP) policy makers. The target audience of the manual are Member States, Candidate Countries, and EU-policy makers that are developing or reviewing their CIP programmes or that want to improve their CIP programmes based on effective and efficient CIP approaches developed by other Member States and other nations.	155.143,00
JLS/2009/CIPS/AG/C1-037	Fondazione Ugo Bordoni	IT	*Domino effects modelling infrastructures collapse*	An innovative interdependency methodology and software tool useful to all MSs to perform ex-ante analysis of domino effects due to CI failures will be implemented. Furthermore, an innovative stochastic and socio/economic model will be integrated in the software tool to evaluate the consequences of CI failures in terms of Cross Cutting Criteria (economic impact, casualties and public effects) as stated in the Directive. The models will be scalable, i.e. applicable at European, National and Regional level. The input data to the tool will be gathered through a set of interviews submitted to a sample of operators in each sector. Planning and analysis of interviews will be supported by a robust statistic methodology.	556.694,59
JLS/2009/CIPS/AG/C1-040	FORMIT – Foundation for Technology Migration and Research	IT	*Video intelligence software in Europe*	The output of this phase will be a questionnaire designed to gather useful information to assess the impact of domino effects. Data collected through the questionnaires will be used as input to the models to quantify domino effects	93.793,42
JLS/2009/CIPS/AG/C2-42	GMV Internet Global Solutions	ES	Critical ICT Infrastructures Simulation of Interdependency Models	CRITICISM is to establish a common simulation framework for ICT Critical Infrastructures in order to analyze failure modes, detect critical points, inspect error propagation, mitigate and reduce failure effects, and prevent risks that would cause a major impact on the health, safety, security or economic well-being of citizens or the effective functioning of government. Additionally the project will cover consequence management in topics such as procedures validation, improvement and impact of correction or upgrading plans, and establishment of guidelines and action points to reduce reaction time and ensure an optimal recovery in a minimum time in case of a failure or disaster.	359.796,67
JLS/2009/CIPS/AG/C2-46	Voivodship headquarters of Police in Rzeszow	PL	Stop terrorism - Polish-Slovak initiative in the matter of preventing and fighting the acts of terrorism.	The project focus is on tightening the cooperation between the services engaged in crisis situations management/terrorist attacks. Joint exercises, initiation of situation scenarios and current solving of potential problems will help to prepare for efficient actions in case of a real terrorist threat.	66.871,00

JLS/2009/CIPS/AG/C2-048	European Strategic Intelligence Company	FR	*European Cyber Attack Table Top Exercise*	The Objective of the EUROCYBEX project is to develop and evaluate a joint exercise aiming at the training and improvement of European actors involved in the management of large scale attacks against the Internet. The exercise will consist of a pan-European table top exercise focusing on technical/operational aspects and problems related to the exchange of information.	141.948,00
JLS/2009/CIPS/AG/C2-050	Foundation for Research and technology Hellas - Institute of Computer Science (FORTH-ICS)	GR	*i-Code: Real-time Malicious Code Identification*	The project aims to develop a real-time malicious code identification toolset and an integrated forensic console which will detect, identify, and categorize malicious code spreading through current and next-generation networks. In more detail, the focus is on designing a prototype for network-level real time detection of malicious code propagation, to customize and provide a malware detection infrastructure to categorize and identify captured malware, to facilitate the detection of malware in high-speed next-generation networks by using new execution architectures and finally maximize the impact of the project through aggressive and effective dissemination of the project's results.	539.180,04
JLS/2009/CIPS/AG/C2-055	Ministry of Communications and Information Society	RO	*Study of the development of an Integrated European Cyber security System, by using a pilot demonstrator in some of the main national ISPs.*	The objective of this project is to develop a coordinated set of ICT infrastructure against cyber attacks to protect EU information society services available through the internet and prevent internal information leaking outside private and governmental organisations. Furthermore this project should contribute to the development and dissemination of best practices and methodologies focussing on public-private joint actions and demonstrate them on several country wide networks.	385.711,00
JLS/2009/CIPS/AG/C2-059	Internal Security Agency	PL	*Counter Terrorist Activities during International Sports Events. The Role of National Counter Terrorist Centres*	Overall objective of the project is the development of international cooperation and coordination in the scope of prevention, preparedness and management of consequences of terrorist attacks. The focus is on information exchange about terrorist attack threats, joint exercises and practical scenarios to protect people during international sports events, development of methodologies for assessing terrorist attack consequences, improving the interoperability before, during, and after the attack, and promoting and supporting the development of security standards.	80.665,00
JLS/2009/CIPS/AG/C2-065	Interuniversities Consortium for Supercomputing Applications	IT	*Exchanged Traffic Analysis for a Better Internet Resilience in Europe*	The ExTrBIRE project has the objective to evaluate the overall resiliency of the Internet infrastructure of a Member State and, more generally, to assess the impacts of a coordinated cyber attack on its Internet infrastructure. The final aim of the project is to develop a national Internet contingency plan that will include the identification of processes, procedures, organizational issues and technical countermeasures that Member States and private organizations should adopt and implement to mitigate threats to their Internet connectivity.	345.347,00
JLS/2009/CIPS/AG/C2-067	D'Appolonia S.p.A.	IT	*Interdependency Modelling Tools and Simulation Based Risk Assessment of ICT Critical Infrastructures Contingency Plans*	Interdependencies among critical infrastructures such as ICT, oil, gas and transport are complex to be understood. Contingency plans often exist, yet there has not been an evaluation that takes into account the interdependencies with other critical infrastructure contingency. Thus the aim of the project is to define and develop a methodology and tools for a simulation based risk assessment of critical infrastructures interdependencies and contingency plans.	1.234.357,62
JLS/2009/CIPS/AG/C2-069	INDRA	ES	*Protection of Electrical Grid Infrastructures*	Electrical grids present a critical infrastructure in relation to terrorist attacks. Currently there are no cost effective security solutions for protection and early warning for certain elements of the electrical grid. The project will look at new and adapted sensors on the one hand and look at an innovative concept of georeferenced tracking to increase the reliability of electrical grids.	498.915,52

JLS/2009/CIPS/AG/C2-071	Prime Minister's Cabinet Office of the Council of Ministers - Department for Information and Security	IT	*Semantic Predictive Algorithm Network for Critical Infrastructure Protection*	The project aims at developing a comprehensive critical infrastructure protection (CIP) governance model based on open source intelligence and novel approaches for information collection, analysis, and sharing. A key objective is to establish a common level of understanding, expertise and awareness concerning the protection of CIs in the entire EU. A real case implementation will demonstrate the effectiveness of the approach by offering a software application suite with threat prediction, risk assessment and early warning capabilities.	672.000,00