NATIONAL STANDPOINTS PROPOSAL

Project name - Resilience of Critical Infrastructure Protection in Europe (RECIPE)

Project is funded by the Directorate-General for Humanitarian Aid and Civil Protection (ECHO), 2014.

Date of update: August 27. 2015.

Humanitarian Aid
and Civil Protection
ECHO/SUB/2014/696006

CONTENTS

ABBREVIATIONS

CI	Critical Infrastructure
CoESS	Confederation of European Private Security Services
EU	European Union
EC	European Commission
FB	Faculty of Security Studies, University of Belgrade
NCCI	National Centre for Critical Infrastructure
RECIPE	Resilience of Critical Infrastructure Protection in Europe

1. PROJECT DESCRIPTION

Project Coordinator: National Protection and Rescue Directorate, Republic of Croatia (DUZS),

Project Partners:

- Faculty of Security Studies, University of Belgrade (FB), Republic of Serbia
- University of Applied Studies Velika Gorica (VVG), Republic of Croatia
- Swedish Civil Contingencies Agency (MMB), Kingdom of Sweden

Area of Implementation:

- Republic of Croatia
- Republic of Serbia
- Kingdom of Sweden

Project Aim: Strengthening the resilience of critical infrastructure protection systems both at national and European level by filling the gaps in the management and protection of critical infrastructure.

Source of co-funding: European Committee - Directorate-General for Humanitarian Aid and Civil Protection (DG ECHO http://ec.europa.eu/echo/).
In line with the Agreement of Funding, the total Project value is 408.675 €, with the co-funding of 75% (306.506 €).

Funding instrument: Financial Instrument for Civil Protection - 2014 Call for Proposals for the preparedness and prevention projects.

Project Duration: 01.01.2015. - 30.06.2016.

2. PROJECT PURPOSE AND OBJECTIVES

Failure in functioning of basic support systems of our society such as energy, traffic, transport, healthcare, financial and telecommunications, and shortage of necessities such as food and water contain the possibility of a massive adverse impact on:

- ✓ Welfare of population and environment,
- ✓ Functioning of industry and economy,
- ✓ Freedom and capacity of governments to respond and act.

The field of Critical Infrastructure Protection (hereinafter CIP) is among the EU key priorities. From the EU aspect, CI is defined as: " an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[1]

The Republic of Croatia in 2013 adopted the following CIP related legislation: Law on Critical Infrastructure, Rulebook on methodology for risk assessment for critical infrastructure operations, and Decision on designation of sectors from which central state administration bodies identify national critical infrastructure and CI sector sequence list.[2]

In May 2014, the Consortium composed of partners from the Republic of Serbia, Republic of Croatia and Kingdom of Sweden, participated at the European Commission call for proposals for projects in the field of civil protection and marine pollution, with the proposal on the topic of critical infrastructure protection - „Resilience of Critical Infrastructure Protection in Europe“ (RECIPE).

The Project is implemented in the Republic of Croatia, Republic of Serbia and Kingdom of Sweden, with the Consortium partners being: National Protection and Rescue Directorate, Republic of Croatia (project coordinator), University of Velika Gorica, Faculty of Security Studies of the University of Belgrade, and Swedish Civil Contingencies Agency. The project has started on January 1st 2015, and will end on June 30th 2016. The Project website is www.recipe2015.eu

---

1 Article 2. Council Directive 2008/114/EC of December 8.2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (SL L 345/75, 23.12.2008.).

2 Law on Critical Infrastructure of the Republic of Croatia (Official Gazette RH, 56/13); Rulebook on methodology for risk assessment for critical infrastructure operations (Official Gazette RH, 128/13); Decision on designation of sectors from which central state administration bodies identify national critical infrastructure and CI sector sequence list (Official Gazette RH, 108/13).

Given that CI is the backbone of the development of contemporary society, its deficient or inadequate protection may pose a threat to the national, regional and European security, economy and stability. Notwithstanding various efforts done by the European Commission and member states in this respect, there is no uniform level of development throughout the EU, nor is there consensus on the model of protection of European CI.

The aim of the RECIPE project is to facilitate establishment of a platform for exchange of experience and 'best practice' between experts and countries that are on different levels of development of CIP.

This will be achieved through: improvement of communication and cooperation between relevant public and private sectors stakeholders, more active involvement of the academic community, as well as strengthening of the scientific research activities in the field of CI risk management.

The project's main objective is development of several applicable and efficient models for:

- ✓ **Public-private partnership in the field of CIP,**
- ✓ **Establishment of mechanism for classified information/data exchange in the CIP system,**
- ✓ **Setting of preconditions for the establishment of National CI Centres.**

Project approach and expected results

The project "Resilience of Critical Infrastructure Protection in Europe" is divided into four components/activities:

- ✓ Panel discussions,
- ✓ Joint workshops,
- ✓ International scientific conference,
- ✓ Follow up strategy.

Since the project start date, four one-day panel discussions were organized – two in Belgrade and two in Zagreb. The results of panels are National Standpoints documents related to the analysis of current national legislation and practice, their strengths and weaknesses, possibilities for their improvement and the analyses of regulations and practice in the field of identification and interdependencies of CI with regard to the requirements of the Directive 2008/114/EC.

National Standpoints will be the basic document for international stakeholders participating at the ***joint workshops*** where they will exchange their experiences and best practices. The results of joint workshops will be used for *Instructions/Guidelines* for better and more efficient management of CI.

International conference will integrate all the results of the efforts throughout the project and provide conclusions for the follow-up strategy on CIP in general and on the following topics in particular: public-private partnership in the field of CIP; mechanisms of classified information/data exchange in the CIP system; setting of preconditions for the establishment of National CI Centres.

The Follow-up strategy will define future cooperation models on any other needs in the CI management system (e.g. training etc.).

Expected results of the project:

- ✓ Facilitated exchange of knowledge, experiences and best practices among Member States and beyond,
- ✓ Increased awareness of and knowledge base on disaster risks threatening critical infrastructure and disaster prevention,
- ✓ Enhanced stakeholder communication both at national and international level,
- ✓ Strengthened mutual support and collaboration between all relevant public and private sector partners,
- ✓ Boosted scientific and research activity in the field of critical infrastructure risk management,
- ✓ Guidelines for the establishment of an optimal risk management system related to CIP in the project partner countries,
- ✓ Guidelines made available to the EC for further dissemination and use;
- ✓ Increased resilience and level of protection of European critical infrastructure resulting from improved coordination and cooperation between stakeholders and from the exchange of best practices,
- ✓ Assessment methodology for CIP established based on the system approach,
- ✓ Defined long-term follow-up strategy on CIP in the project partner countries,
- ✓ Assessed and defined needs for further education and training of public and private sectors in the related area (educational programmes, exchange of experts).

3. ANALYSIS OF THE CURRENT SITUATION

The concept of 'Critical Infrastructure' has only recently appeared in Serbia, for the first time in 2011, in the Regulation on the Content and Methodology for the Development of Protection and Rescue Plans in Emergency Situations (Official Gazette of RS, No. 8/2011). The Article 8 of the Regulation highlights the assessment of CI from the standpoint of natural disasters and other major accidents. However, neither this nor any other document gives a definition of the concept.

Furthermore, 'Guideline on Methodology for Preparation of Vulnerability Assessment and the Protection and Rescue Plans in a State of Emergency' (The Official Gazette of RS No. 96/12), establishes criteria for the assessment of ten CI sectors with regard to their vulnerability to natural disasters and other accidents. Although the methodology contains the most comprehensive approach to the CIP in the national legislation, it is focused on identifying sources of threats and particularly on the consequences that a disturbance or interruption of the facility operation has on the economy and ecology. However, this methodology does not include 'all-hazard approach', nor the measures for improving resilience that could reduce the adverse effects of natural and other disasters on the infrastructure, including the cascade effects caused by interdependencies.

There is a particular need to develop models and methods for improvement of resilience of CI system in order to improve its capacity to minimize the consequences. It is necessary to define criteria for the identification of potential threats/hazards and generation of hazards and interdependencies tailored to different CI sectors in line with international, European and national standards.

Therefore, the first step in the regulation of this field would be to adopt the Law on Critical Infrastructure, thus establishing the legal framework for definition, identification and protection of national and European CI. After the adoption of the Law, it will be necessary to develop and adopt the bylaws that would provide practical solutions and criteria for identification of CI sectors and systems.

It should be added that the identification of CI will not start from scratch, as some existing legal acts give a solid starting point. In particular, the Law on Defence ("Off. Gazette of RS", no. 116/2007, 88/2009, 88/2009 - ot. Law 104/2009 - other. Law 10 / 2015) with its related bylaws should be observed. The Law refers mainly to the defence industry of Serbia, but also to other industrial and infrastructure objects, which during war, state of emergency or mobilization of the Serbian Army primarily provide the services and operations stipulated by the Ministry of Defence.

Other laws, bylaws and strategic documents relevant for the CIP are: the Law on Emergency Situations ('Official Gazette of RS' no.111/2009), National Strategy of Protection and Rescue in

Emergency Situations ('Official Gazette of RS', no. 86/2011), Law on Private Security ('Official Gazette of RS', no. 104/2013), Law on Environmental Protection ('Off. Gazette of RS', no. 135/2004, 36/2009, 36 / 2009 – other law 72/2009 and 43/2011 - Decision), Data Secrecy Law ("Off. Gazette of RS", no.104/2009), Law on Planning and Construction ("Off. Gazette " no.72/2009), Law on Water (Official Gazette. Gazette no.30/10, 93/12), and other relevant documents.

In the following steps it will be necessary to prioritize the identified CI sectors and regulate the aspects of the CIP that have shown to be particularly problematic in the European and global practice – public-private partnership (PPP) and exchange of classified information.

4. DEFINITION, IDENTIFICATION AND LEGAL REGULATION OF THE FIELD OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SERBIA

Based on the international experience and 'good practice', the partners agree that the definition of critical infrastructure and its content cannot be identical in each and every country, therefore its definition and content should be determined at the national level.

Therefore, in order to be sure about the content and the boundaries of the CI concept, it is crucial to adopt the Law on Critical Infrastructure. The Law would establish a regulatory framework for defining, identifying, and protecting national and European CI in Serbia. In addition, its bylaws should provide practical solutions and criteria for the identification and prioritization of CI.

The adoption of the Law on CI (or CIP) is among the obligations of the Republic of Serbia in the process of EU accession. The Action Plan for Chapter 24 for the EU accession recognizes the Ministry of Internal Affairs of the Republic of Serbia as the authority responsible for the future Law. Within the Ministry of Interior, the Sector for Emergency Management is the body that shall coordinate the activities on the establishment of an interdepartmental working group that will define a national CIP policy.

The future Law on CI, but also other laws relevant to the CI should contain the provisions of the European Directive on the Protection of Critical Infrastructure (Directive 2008/114 / EC). In this regard, it is necessary to make amendments in the CIP related parts of the National Strategy for Protection and Rescue in the Emergency Situations and in the Law on Emergency Situations. For effective CIP and comprehensive legal regulation of this area it will be necessary to implement the existing Data Secrecy Law, which, according to some experts, exists only on paper. In addition, the Law on Information Security (the work on its draft commenced more than three years ago), the Regulation on Encryption and Cyber Security Strategy should also be adopted.

During the identification of CI sectors and facilities it would be desirable to start from international, or at least from the regional level. While many developed countries identified over ten CI sectors (including the Republic of Croatia - eleven sectors identified), it is suggested that lawmakers in Serbia should be realistic and not make a list of sectors that is too broad, taking into account the limited state budget, due to which not all identified sectors and belonging facilities could be protected in an optimal manner. The next step would be to identify CI facilities at lower levels, in addition to regional and national. CI facilities can also be identified at the city, local, and even at the sectoral level. Preliminary identification and classification of CI facilities may be done even before the law is adopted, provided the criteria and departmental sector analysis are defined.

The following infrastructure sectors appear in almost all countries with the developed CIP policies and can be used for creation of a wider list of CI sectors in Serbia:

- Energy (production, transmission, distribution and storage of energy supplies (oil and gas) and electricity)
- Information and communication technologies (electronic communication, data transmission, information systems, audio and multimedia services)
- Transport (road, rail, air, water)
- Health (hospitals, pharmaceutical industry)
- Water (drinking water supply, dams, wastewater treatment, water protection)
- Food (production, food supply, food security, commodity stocks)
- Finance (banking, stock exchanges, investment, insurance and payment systems) and
- Public services (preservation of public order, protection and rescue, emergency medical assistance).

Various ministries, sectors and departments have different criteria and classification of objects and facilities under their jurisdiction. The Law on Defence provides the definition of facilities that are of special importance for the national defence: large technical and technological systems; facilities in which products of importance for defence purposes are produced, stored or kept, or facilities that provide service for defence purposes; buildings occupied by public authorities and legal entities of special importance for the national defence, as well as certain infrastructure facilities. The Plan of Defence mentions hundreds of technical and technological systems, with the respective plans of defence, whilst the Instruction on Creation of Plans of Defence from 2013 provides a methodology for identification of those technical and technological. Therefore, it is possible that future CIP plans will be included in plans of defence. In addition to the Law on Defence and Plans of Defence, the following bylaws are also relevant for future identification and classification of CI in Serbia:

- Decision on Types of Investment Facilities and Spatial and Urban Plans of Importance for National Defence ("Off. Gazette FRY", no. 39/95).
- Decision on Facilities of Particular Importance for National Defence ("Off. Gazette of RS", no. 112/2008)
- Decision on Identification of Large Technical Systems Important for National Defence ("Off. Gazette of RS", No.41 / 2014 and 35/2015)
- Decision on Identification of Products and Services of Special Importance for the National Defence of the Republic of Serbia ("Off. Gazette of RS", no.58 / 2008);

The abovementioned documents primarily refer to defence industry in Serbia, as well as other industrial and infrastructure facilities that in time of war or state of emergency, as well as during the mobilization of the Army of Serbia primarily provide those services determined by the Ministry of Defence.

Another relevant law for the identification of CI is the Law on Planning and Construction, and its associated plans: Spatial Plan of the RS, followed by regional and local plans. Particularly

important are the spatial plans of special purpose areas, which almost completely coincide with critical infrastructures.

Conclusion

As the first step towards establishment of an efficient protection and resilience CI system, the legal regulation of this field is of key importance. First of all, it is necessary to adopt the Law on CI and its bylaws that will more precisely regulate the particular challenges such as the identification of CI sectors, identification of CI facilities in specific sectors, classification and prioritization of identified CI, public-private partnerships and the exchange of classified information. This procedure will not start from scratch as the existing legal framework provides a solid base for the inclusion of certain provisions in the new law and accompanying bylaws. The term „critical infrastructure "should be included in the existing relevant laws and bylaws, which will further need to be harmonized with the Law on CIP when it comes into force.

5. PUBLIC-PRIVATE PARTNERSHIP IN PROTECTING CRITICAL INFRASTRUCTURE

Abstract

The aim of the proposal is to establish a platform for public-private partnership in the field of the critical infrastructure protection and resilience that will provide the logic and principles for the following: the concept of cooperation; projects; security; creation of a new and improvement of existing legal and normative framework; identification of critical infrastructure; prioritization of vital critical infrastructure; development of programs and tools for achievement and improvement of resilience and security.

Public-private partnership (hereinafter - PPP) is among the key factors of the CIP process. In the majority of developed countries around 80% of CI is privately owned. Although for Serbia and the Western Balkans region precise figures do not exist, that percentage is undoubtedly lower. However, the increase of the percentage of privately owned CI facilities is expected, taking into account global trends of market liberalization. According to the Communication from the European Commission on the principles of the PPP "Public Private Partnerships (PPPs) can provide effective ways to deliver infrastructure projects, to provide public services and to innovate more widely in the context of these recovery efforts. At the same time, PPPs are interesting vehicles for the long-term structural development of infrastructures and services, bringing together distinct advantages of the private sector and the public sector, respectively."[3]

In the contemporary "risk society", where we are exposed to an increasing number of security threats and challenges - from climate change to organized crime and terrorism - the cooperation, including the exchange of knowledge and experiences between the private and public sectors is crucial. The state and state "institutions of force" do not always have sufficient capacity for meeting the security needs of society, which is especially noticeable in the field of protection. Indeed, PPP appears to be the mechanism of choice for cooperation between the factors that may impact the efficient resolution of security challenges. PPP as a model of relations between the public and private sectors is established on the premises of recognizing the benefits for both public and private sector from the pooling of resources and expertise (knowledge), for the purpose of meeting community needs. This partnership combines the expertise, resources and strengths of both sectors, harmonizes social and public accountability and effective management of the public sector with financial capabilities and the "entrepreneurial spirit" inherent to the

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 November 2009 - Mobilising private and public investment for recovery and long term structural change: developing Public Private Partnerships [COM(2009) 615 final – Not published in the Official Journal].

private sector. This may result in better and more efficient protection of public interest in the field of CIP. Therefore, the priority should be given to those joint initiatives of the public and business sectors in which each entity contributes with specific resources and cooperates in the planning and decision-making process.

Certainly, one should take into account that in PPP there must be some differences in the "approach" to the concept of cooperation between the partners. For example, private companies will often manifest "profit motives“, whilst the public sector can impose "bureaucratic" thinking and decision making thus demotivating the other side. In order to overcome potential differences, it is important to concentrate on wider picture. If it is correctly designed and implemented, PPP can bring palpable benefits in terms of helping governments to finance infrastructure investments in a more efficient manner, as scarce resources may be channelled to other national priorities (e.g. meeting the basic needs of citizens in the fields of education, health care) with better value for money.

According to the “Best Practice” analysed, PPP should meet the following criteria: open dialogue between the responsible public authorities and service providers of private security, clear guidelines on the role of each partner, clear legal and contractual framework, regular assessments and the necessary corrections and improvements when and where necessary. In addition, the interaction must exist within the framework of specifically established and formally bound joint structures.

In order to meet these criteria and optimize the effectiveness of the partnership between the public and the private security sector in CIP arena, it is vital that each partner fully understands its role, responsibilities and limitations. The Confederation of European Security Services (CoESS) believes that due to the lack of knowledge of these elements, the partnership between the public and private sectors in the field of CIP across Europe is still underdeveloped and far from reaching its maximum potential.

It should be added that, when considering policy cooperation with private security companies in the field of CIP, the necessary attention should be paid to the quality of service. CoESS therefore recommends that national regulations concerning private security services include provisions on special licenses or authorizations for the CIP services. This can be achieved through additional licensing and setting of work criteria for private security companies or through compulsory special training programs for the staff of private security in this field.

It should be stressed that the private security sector in Serbia is very active and a proponent of the large number of initiatives on the adoption and improvement of legislation and national standards.

Private security sector companies are engaged in the CIP projects through the process of public procurement. It is essential that private security sector reaches a certain level of competence for such operations, as is necessary in the case of state security institutions - the army and police. It was noted that major problems arise in the process of public procurement of private security

services, since the only criterion is the lowest available price, even though the EU Directive provides clear guidelines that mandatory criteria are the most economically advantageous tender, and the competitive dialogue. As the price of private security services in Serbia is the lowest in Europe, the quality of services is questionable if the cheapest offer is chosen. This can have serious consequences for the CIP, since many of CI facilities are protected by companies characterized by a low level of service quality, personnel training, equipment and others.

The National Security Strategy of the Republic of Serbia and the public-private partnership

The National Security Strategy of the Republic of Serbia identifies PPPs as a matter of a huge importance to the national security. "An important prerequisite for achieving and improving protection of life and property of citizens, human and minority rights is the cooperation of state bodies with the entities from the field of private security and other institutions, local governments, professional associations, churches and religious communities, the media, minority communities, civil society organizations and citizens, thus developing relationships of trust, building and strengthening security and solving security problems."[4]

The National Security Strategy of the Republic of Serbia also addresses the issue of private security companies by stating that: "Along with government and other bodies and institutions, the entities in the field of private security services have increasing responsibility for the implementation of internal security policy, whose activities include security protection of individuals, objects and other material goods not covered by the protection of the competent state authorities. Of particular importance is that the social activities of the entities in the field of private security are entirely normatively and doctrinally regulated."[5]

Law on Public-Private Partnership and Critical Infrastructure

It is to be expected that certain provisions of the future Law on CI will be based on the Law on Public-Private Partnership, adopted in 2011 ("Official Gazette of the RS" no. 88/2011). Certainly, the Law on PPP does not recognize the term 'critical infrastructure", due to non-existent legislation on CI. However, it is clear that many facilities and services of public interest mentioned in this Law will enter the framework of the prospective Law on CI and future bylaws and regulations in this area.

According to this law, the PPP is a long-term cooperation between a public and a private partner for the purposes of providing financing, construction, reconstruction, management or maintenance of infrastructure and other facilities of public interest and provision of services, of

[4] National Security Strategy of the Republic of Serbia, p.27.
[5] Ibid, p.26

public interest, which may be contractual or institutional (Article 7) The period for which the public contract is concluded may not be less than five, nor more than fifty years (Article 18).

Article 4 of the Law defines public partner as one or more public bodies, or a legal person who according to this law is in charge of approving the concession, which enters into a public contract with the private partner or the SPV, or one or more public bodies that are linked with the private partner through membership in some joint enterprise.

The private partner is defined as a natural or legal person, national or foreign, with local or foreign share or without it, or a consortium of one or more such natural and legal persons which have been selected in a public procurement procedure or concession granting procedure and which have signed with the public partner a public contract, or which is establishing for that purpose an SPV, or which is establishing with the public partner a joint enterprise.

It is interesting to note that Article 3 states that the Law does not apply to PPPs if the subject of that partnership was the use of a public telecommunications network or the provision of telecommunications services. Paragraph 2 of the same article also points out non-application of the law in the event that the establishment of such PPP would require enabling access to the information whose disclosure would endanger the security of the Republic of Serbia

Article 5 of the Law sets out Principle on environmental protection as one of the basic principles for conclusion of public contracts. According to the Article 6 **The principle of environmental protection** includes the principles defined by the law regulating environmental protection, such as: the principle of integrity, the principle of prevention and precaution, the principle of preservation of natural values, sustainable development, the polluter-pays principle and other.

The private partner has an obligation to take over from the public partner the design, construction or reconstruction of public infrastructure or a facility of public interest, as well as the maintenance of public infrastructure or provision of services of public interest including one or more of the following obligations: financing, management and maintenance, for the purpose of providing services of public interest to final beneficiaries from within the competences of the public partner, or for the purpose of ensuring the necessary preconditions for the public partner for the provision of services of public interest within his competences, or provision of services of public interest from within the competences of the public partner to the final beneficiaries

Also, each partner is to undertake responsibility for the risk which it can better manage or which it can affect, or risks are divided in a balanced manner, all for the purpose or ensuring optimal risk management for the duration of the PPP project, with the use of management, technical, financial and innovative capacities of the private partner, and by improved exchange of skills and knowledge between the public and the private partners.

The concept of ‘concession’ which regulates relations in various infrastructure sectors will surely be relevant for the PPPs in the field of CI. According to this Law, the concession is a PPP with

the elements of concession in which a public contract regulates the commercial use of natural resources or assets in general use which are publicly owned or the performance of an activity of public interest which the competent authority transfers to a national or foreign person, for a specific period of time, under specially prescribed conditions, against the payment of a concession fee by the private or the public partner, with the private partner bearing the risk associated with the commercial use of the subject of concession. (Article 10)

Among other things, the concession may be given for exploration and exploitation of mineral resources and other geological resources, in the area of energy, for construction and maintenance of ports, public roads, public transport, airports, railways, health care, etc. (Article 11). It should be noted that not all areas of public interest are explicitly mentioned in the Law, so some of them remain open to interpretation. The concession granting authority may be the Government of the Republic of Serbia, the Government of an autonomous province, the local assembly or a public company. (Article 13) As far as the private partner, participant in the award of a public contract may be any domestic or foreign natural or legal person (Article 14).

According to the Law, the state PPP Commission gives professional assistance in the implementation of PPP projects and concessions. The chairman of the Commission's is the representative of the Ministry of Economy and Regional Development, whilst his deputy is a representative of the Ministry of finance (Article 65). The Commission, as the most important state body for the approval of PPP projects determines whether the project proposal is in the public interest and whether it is submitted by a public body. As the Commission is composed of representatives of various ministries, under whose competencies are areas that will belong to future CI sectors - such as the Ministries of energy, transport, mining, etc., their representatives will be directly involved in projects related to CI belonging to their competencies.

The Commission for PPP in the Security Sector, organized within the Serbian Chamber of Commerce, is identified as an important subject in the CIP related PPP projects. Its members are representatives of private security associations and companies, representatives of ministries with an interest to cooperate with private security sector, representatives of the academic community and various citizen associations (NGOs).

National and International Standards

Some provisions of international and national standards give an insight into the "good practice" of PPP. For instance, draft ISO 22397 Standard (Societal security - Public private partnership - Guidelines for establishing partnership agreements among organizations) from 2012 mentions critical values of the assets and disruptive events.

According to this draft, the first parameters for the establishment of a partnership agreement are the identification and classification of common critical assets, as well as the identification and evaluation of potentially disruptive events. It is proposed that these activities are executed in accordance with the guidelines of ISO 31000: 2010 (Risk Management). For the same purpose, in

Serbia the national standard SRPS A.L2.003 2010, Social security - Risk Assessment in the Protection of Persons, Property and Business (Official Gazette of RS, no. 92/2010) can be used.

When identifying critical assets, the parties should provide a comprehensive list of all relevant resources, and also identify any vulnerable targets. Information about critical assets (facilities, systems, equipment, services, processes, people, etc.) should be made in accordance with the mission, confidentiality and expectations set out in the partnership agreement. Analysis and prioritization of identified assets can be a useful input for the next phase of classification.

During the classification process the contracting parties should jointly establish a list of identified critical assets. The contracting parties should also define the method of evaluation, which may include the correlation between the protected assets. The level of detail of mathematical modelling should be determined by the expectations of the parties. Audit and 'field' evaluation can also be used to gain insight on particular assets and/or for the validation of previous criticality assessments.

Identification of disruptive events involves identification and description of the sources of risk, and the potential consequences for the identified critical assets. Risk identification must be comprehensive and should include interdependencies, cascade and cumulative effects, but also consider the consequences of events when risk sources are not recorded. In the case of complex partnership agreements with more contracting parties, stakeholders and assets, the parties should consider multiple causes and scenarios, and pay special attention to potential correlations between sources of risks and interdependencies.

Recommendations

The concept of cooperation between the public and private sectors for strengthening the critical infrastructure resilience and protection

After it is clearly defined what we understand under CI protection and resilience, and what it needs to achieve, it will be necessary to devise a strategy for its implementation and to provide the political will to implement its objectives. The following step is to raise awareness among all stakeholders, especially between the CI owners and operators of. Provided the preceding steps have been completed, it will be necessary to establish the foundation of cooperation between the public and private sectors which includes the following:

1. The development of standards and exchange of best practice

2. Promotion of education and training

3. Promotion of research and development

4. Exchange of information

During the project, the Faculty of Security Studies, as the Project beneficiary in the Republic of Serbia, will ensure the participation of representatives from relevant ministries, agencies, sectors and other state bodies, as well as representatives of the most important economic entities (potentially identified as CI facilities), professional and academic community, Serbian Association of Corporate Security Managers, the Association of Private Security Managers within the Chamber of Commerce of Serbia, the Commission for Public-Private Partnerships and numerous other stakeholders to discuss and propose the optimal concept of cooperation.

Public-private partnership projects aimed at strengthening the critical infrastructure protection and resilience

Although PPP is not the ideal model for all infrastructure projects, it is necessary to consider a joint action wherever possible and mutually justified. Construction of missing CI capacities, maintaining and improving the resilience of the existing ones, and the CIP, is easier to achieve through public-private partnerships in relation to the options of the public sector.

The public sector should aim at a larger, more innovative and long-term financing of infrastructure projects by the private sector, but also carefully consider the private sector interest, in order to avoid the impression of unidirectional partnerships.

PPP projects facilitate transfer of risk from the public to the private sector. This approach brings benefits such as the development, modernization and maintenance of large infrastructure facilities through private funding. To this purpose we propose the following: conclusion of long-term projects by public sector; joint public and private funding; involvement of the private sector in the responsibilities of the public sector (procurement, construction, management, maintenance, etc.); creation of risk and responsibilities sharing models during the course of the partnership.[6]

In Serbia, currently there is an initiative to include private security companies in the TETRA protected communication network, set within the 112 Service, which is also being implemented.[7]

During the course of the Project, FB will organize meetings and discussions on potential models of cooperation between the most important stakeholders in this field, and it will also collect and analyse the best available practice and models for their implementation.

Establishment and improvement of normative framework with the view to strengthening of CI protection and resilience

The establishment of normative framework is an extremely demanding work that will facilitate the regulation of a certain field, and in addition open ground for further action, new ideas and

[6] John Forrer, James Edwin Kee, Kathryn E. Newcomer and Eric Boyer "Public Private Partnerships and the Public Accountability Question" u: Boyer E. et al. (2014:4).

[7] In all EU countries, 112 is the contact number of emergency services (ambulance, firefighters and police). The calls are free of charge and the number is accessible 24/7.

models of implementation of legal regulations. In addition, normative framework should provide a stimulative approach for new investments and creation of new values.

First of all, we refer to the adoption of Law on Critical Infrastructure that will regulate this field, as well as to bylaws pertaining to this law. Furthermore, we refer to amendments in other laws (Law on Public-Private Partnership, Law on Defence, Data Security Law, Law on Information Security, Law on Private Security etc) and strategic documents (National Security Strategy, Cyber Security Strategy, Strategy for Terrorism Prevention, Strategy of Socially Responsible Business...) directly or indirectly related with CI protection and resilience, and also regulate PPP in this field.

In the process of establishing the normative framework for a new framework, the lawmaker most frequently takes over the *acquis communitaire* (in the EU context) and opens a public discussion with all stakeholders. As the preparation and adoption of Law on Critical Infrastructure (an obligation of the Republic of Serbia in the process of accession to the EU) is announced for 2016, an important part will be dedicated to the regulation of PPP in CIP. FB will broaden the public discussion with the aim of obtaining high quality proposals for the improvement of the normative framework, in order to make it clear, flexible and open for new investments, as well as for the bigger and better cooperation between public and private sector.

Identification and prioritization of CI using the mechanism of PPP

After the CI related law and bylaws are adopted and the CI sectors and facilities identified, the following step will be the prioritization, as not all CI sectors and facilities are equally critical from the aspect of the disruption of their operations or interruption of supplies of goods and services.

Taking into account the large number of CI sectors and facilities and the experience of countries that have already adopted this paradigm, it is concluded that it would be impracticable to equally protect and build resilience of all CI facilities. Private actors, primarily the owners and operators of the privately owned CIs can provide a valuable contribution to this process.

Project partners will collect and share the best international practice with all stakeholders and ensure the platform for establishment of PPP in the field of CIP.

Development of programs and tools for building and improvement of CI protection and resilience using PPP

First and the foremost, CIP includes prevention and risk assessment of CIs. On the other hand, resilience signifies the ability of a system to reduce efficiently both the magnitude and duration of the deviation from targeted system-performance levels.[8] As it is a complex concept that requires holistic approach, PPP is a very convenient tool for strengthening its resilience.

[8] Biringer B, Vugrin E and Drake Warren, *Critical Infrastructure System Security and Resiliency*, CRC Press, Boca Raton, 2013, p.107

During the course of the project, national partners will perform the necessary research in order to connect knowledge and experience, and consequently recommend programs and tools for building and improvement of critical infrastructure protection and resilience using PPP.

Conclusion

FB will continuously work on updating and reviewing of this document in coordination with all stakeholders.

This chapter intends to create national standpoints on PPP in CI protection and resilience and to exchange the best practice regarding: the concept of cooperation; projects; security; improvement of normative framework; prioritization of vital CI; development of programs and tools for building and improvement of CI protection and resilience.

Literature

Strategies and Laws

Narodna Skupština Republike Srbije (2009) *Strategija nacionalne bezbednosti Republike Srbije*, dostupno na: http://www.kombeg.org.rs/Slike/CeBezbednost/statika/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf , (accessed July 2, 2015.).

Narodna Skupština Republike Srbije (2011) *Zakon o javno-privatnom partnerstvu i koncesijama*, dostupno na: http://www.paragraf.rs/propisi/zakon_o_javno_privatnom_partnerstvu_i_koncesijama.html , (accessed July 2, 2015.).

Standards

ISO 31000 Risk management – Principles and guidelines on implementation

ISO/IEC 31010 Risk management – Risk assessment techniques

ISO/CD 3 22397 Societal security — Guidelines for establishing partnering arrangements

ISO/TC 223 N 337 Societal security - Public private partnership — Guidelines for establishing partnership agreements among organizations

SRPS A.L2.002:2008, Društvena bezbednost – Usluge privatnog obezbeđenja – Zahtevi i uputstvo za ocenjivanje usaglašenosti, Službeni glasnik RS, br.07/2009.

SRPS A.L2.003:2010, Društvena bezbednost – Procena rizika u zaštiti lica,imovine i poslovanja. Službeni glasnik RS, br. 92/2010.

EU Documents

Critical Infrastructure, *Security and protection, The Public - Private opportunity*, CoESS, B-1780 Wemmel, Belgija, May 2012

Risk Management Capability Assessment Guidelines (ECommisison notice, 2014)

European Commission (2009) Mobilising private and public investment for recovery and long term structural change: developing Public Private Partnerships.

Research papers

Auzzir Z.A. et al. (2014) *Public-private partnerships (PPP) in disaster management in developing countries: a conceptual framework,* http://www.sciencedirect.com/science/article/pii/S2212567114010065, (pristupljeno 24. jula 2015.).

Biringer B, Vugrin E and Drake Warren (2013), *Critical Infrastructure System Security and Resiliency*, CRC Press, Boca Raton.

Boyer E. et al. (2014) *Public-Private Partnerships and Infrastructure Resilience, How PPPs Can Influence More Durable Approaches to U.S. Infrastructure,* http://www.uschamberfoundation.org/sites/default/files/article/foundation/PPPs%20and%20Infrastructure%20-%20NCF.pdf, (pristupljeno 24. jula 2015.).

Heammerli, B. i Renda, A. (2010) *Protecting Critical Infrastructure in the EU*, Brussels: Centre for European Policy Studies, http://www.ceps.eu/ceps/dld/4061/pdf (pristupljeno 5. februara 2014.).

Keković, Z., Savić, S., Komazec, N., Milošević, M., Jovanović, D. (2010) *Procena rizika u zaštiti lica, imovine i poslovanja,* Centar za analizu rizika i upravljanje krizama, Beograd

6. CLASSIFIED SHARING IN THE CRITICAL INFRASTRURCTURE PROTECTION SYSTEM

Thanks to the first security incidents in cyber space it was noticed that computer systems and networks represent a huge source of risk to information and, indirectly, to individual, corporate, national, regional and global security. Due to the continuous process of informatization of the population and progressive automatization of the critical infrastructure and services, the significance of information security has increased. This concept has become a central element of the national security policies of all technologically developed countries, and also of regional and global security policies. Many experts have concluded that "security, economy, standard of living and, quite possibly, the very existence of industrialized countries depend on" electricity, telecommunications and computers ... which are, in addition to traditional physical threats, exposed to new cyber threats."

Therefore, the information is the main entity exposed to the security threats from the arsenal of information warfare. Three aspects of information can be compromised: privacy, integrity and availability. In addition, the total infrastructure in charge of transmission of data and information and their storage is exposed to threats and risks.

Disruption of normal operation of information systems in the modern society can have severe consequences in all spheres of social life. The consequences can be even fatal, if critical information infrastructure, such as systems for control of land and air transport, hydro-dams, nuclear power plants, security and health services, or even systems for electricity distribution, is compromised. After the 9/11 terrorist attacks, the issue of security of cyber space and the protection of critical information infrastructures has come in the focus in developed countries. The focus on these issues, according to some analysts, was the result of fear of the US administration of possible "boomerang effect", i.e. as an understanding that the Internet for terrorists constituted the tool for planning and implementing attacks. Heightened perception of the possibility of transferring terrorism threat to the cyber space, but also of other forms of information warfare that may cause material damage to the state and its citizens, jeopardize defence systems, negatively impact human rights, health and life, put the possibility of creating a safe information space high on the agenda of regional and international organizations.

In the growing number of discussions on CIP, the information infrastructure receives special attention. Over the years various measures for prevention and response to possible incidents, caused by technical failures, natural disasters or intentional destructive acts were developed. The growing dependence of systems on information infrastructure represents an additional risk, given that it permeates all other systems and imposes them its own vulnerabilities. A typical example of the permeation can be shown in the example of control systems - specialized computers and technologies

that are used in many industries and infrastructure services for the monitoring and control of the most sensitive processes. In the electricity industry, for example, control systems manage and control the generation, transmission and distribution of electricity. In the gas distribution the monitoring of the flow of gas in the pipelines is performed from remote locations. In water distribution such systems control the water level in wells and reservoirs, the pumps, the level of water quality and the presence of chemical additives.

Nowadays the information base, control systems and means of communication are interconnected at the global level. This situation has its "Achilles heel" as the most advanced technological party may, at the same time, be the most vulnerable one, or if adequately protected, the most dangerous one. The rapid entry of "information conflicts" into the civil and corporate sphere is a serious problem for managers responsible for the safety and security of the information infrastructure. Management structure at the corporate-economic level should be aware of the broad scope of potential attacks, including espionage, organized crime, perceptual battle, as well as attacks by hackers and groups sponsored by a state or business competitors. The concept of managing security risks in the information space in terms of national security, however, requires harmonization of national legislation with the existing international standards.

The Republic of Serbia is lagging behind many EU countries, as well as behind another participant in this project, the Republic of Croatia, which passed the Law on Critical Infrastructure in 2013 (Official Gazette No. 56/13), and the Data Protection Law, which clearly defined the problem of sensitive information. The problems that our country face are reflected in the following shortcomings: the lack of horizontal and vertical connection of participants responsible for the protection of sensitive information, insufficient recognition of the importance of categorization of classified data and sensitive information, diverse procedures in the protection of personal and business data, lack of capacity for protection of sensitive information, an unclear role of the Ministry for Construction, Transport and Infrastructure, lack of skilled personnel in the Ministry to deal with the CI issues, the lack of permanent education of managers in the field of CI and in the field of information protection, the lack of awareness of people in charge of the CI of their own role in data and information protection, lack of knowledge of procedures for information and data sharing with other stakeholders, insufficient harmonization of data protection practices with international standards etc.

The recognition of importance of secret data, sensitive information and their protection is reflected in the Data Secrecy Law ("Off. Gazette of RS", no. 104/2009). This Law regulates the single system of determination and protection of secret data of interest for national security and public safety, defence, internal and foreign affairs of the Republic of Serbia; protection of foreign classified data; access to classified data and their declassification; competence of authorities and oversight of the implementation of this Law, as well as accountability for non-implementation of obligations arising from this Law, and other issues of importance for data secrecy protection. The Law provides definitions of various concepts: data of interest for the

Republic of Serbia, classified data, foreign classified data, document, classification of data, determining the level of secrecy 'top secret', 'secret', 'confidential' or 'restricted, security clearance, damage, classified data controller, data user, security risk and protection measures. According to the Law Data that can be classified as secret shall be any data of interest for the Republic of Serbia, whose disclosure to an unauthorised person would result in damage, if the need to protect the interest of the Republic of Serbia prevails over the interest to have free access to information of public importance. The data from paragraph 1 of the Article 8 are particularly relevant to: 1. national security of the Republic of Serbia, public safety, or defence, foreign, security and intelligence affairs of public authorities; 2. relations between the Republic of Serbia and other countries, international organisations and other international entities; 3 systems, equipment, projects, plans and structures in connection with the data from items 1) and 2) of this paragraph; 4. scientific, research, technological, economic and financial affairs in connection with the data from items 1) and 2) of this paragraph.

Data classification is performed by authorized persons under the conditions and in the manner prescribed by the Law. The Article 9 mentions the following authorized persons: 1. the President of the National Assembly; 2. the President of the Republic; 3. the Prime Minister; 4. the head of a public authority; 5. elected, appointed or nominated public authority officials, authorised to classify data by law or regulation adopted under law, or authorised in writing by the head of a public authority; 6.persons employed by a public authority, who have been authorised in writing for data classification by the head of the public authority. The authorised persons from paragraph 2 items 5) and 6) of this Article may not delegate their authority to other persons. The authorised persons classify data during their creation, i.e. when the public authority begins to perform an activity resulting in the creation of classified data. As an exception to paragraph 1 of this Article, an authorised person may also classify data subsequently, upon fulfilling the criteria established by this Law.

In classifying data, an authorised person assesses possible damage to the interest of the Republic of Serbia. A person employed by or performing certain tasks for a public authority is obliged, within his/her tasks or powers, to inform an authorised person of any data that can be classified as secret. A document containing classified data is marked with: 1. a classification level; 2. the manner in which it is to be declassified; 3. details on the authorised person; 4 details on the public authority. The Government prescribes the manner and procedure of marking the level of classification, i.e. the document. The data from Article 8 of the Law are assigned one of the following levels of classification: 1. "TOP SECRET", which is assigned with a view to preventing irreparable grave damage to the interests of the Republic of Serbia; 2. "SECRET", which is assigned with a view to preventing grave damage to the interests of the Republic of Serbia; 3. "CONFIDENTIAL", which is assigned with a view to preventing damage to the interests of the Republic of Serbia; 4 "RESTRICTED", which is assigned with a view to preventing damage to the operation or performance of tasks and activities of the public authority which defined them. In determining the level of data classification, only the levels of

classification from paragraph 1 of this Article may be applied. The Government defines more detailed criteria for determining the "TOP SECRET" and "SECRET" levels of classification, upon obtaining an opinion of the National Security Council. The Government defines more detailed criteria for determining the "CONFIDENTIAL"and "RESTRICTED"levels of classification, at the proposal of the competent minister or the head of a public authority.

According to the Law, a public authority establishes a system of procedures and measures to protect classified data according to the following criteria: 1. the level of classification; 2. the nature of the document containing classified data; 3. classified data security threat assessment. A public authority applies general and special protection measures under law and regulations adopted under law, with a view to protecting classified data in its possession. General measures for the protection of classified data include: 1. determining the classification level; 2. assessing classified data security threat ; 3. establishing the manner of using and handling classified data; 4. designating a person responsible for keeping, using, exchanging and other forms of classified data processing; 5 designating a classified data controller, including his security clearance depending on the classification level; 6. determining special zones, buildings and premises intended for classified data and foreign classified data protection; 7. classified data handling control; 8. measures for the physical and technical protection of classified data, including the installation and set-up of technical means of protection, determination of a security zone and protection outside that zone; 9. protection measures for information and telecommunication systems; 10. crypto protection measures; 11. protection regime for jobs and formation posts, under any internal acts on job classification and systematisation; 12. establishing special educational and training programmes required for the protection of classified data and foreign classified data; 13. other general measures prescribed by law. With a view to efficiently implementing general measures for classified data protection from Article 32 of the Law, special measures for classified data protection can be brought under a Government act.

Classified data are kept in such a manner that only authorised users are allowed access to these data. Classified data may be transmitted and delivered outside the premises of a public authority only in compliance with the prescribed security measures and procedures ensuring that classified data could be received only by a person who has a certificate for access to classified data and is entitled to receive them.

In transmitting and delivering classified data outside the premises of a public authority, security procedures and measures are determined according to the classification level assigned to such data, under law and in compliance with any regulation adopted under law. The application of the prescribed measures of crypto protection is mandatory in transmitting and delivering classified data over telecommunication and information systems. In transmitting and delivering classified data from paragraphs 3 and 4 of this Article, crypto protection measures are implemented under law. When an official, employee or a person performing specific tasks in a public authority, learns of any loss, theft, damage, destruction or unauthorised disclosure of classified data or

foreign classified data, he/she shall inform the authorised person of a public authority thereof without delay.

In addition, the Law regulates the access to classified data, procedure for issuing certificate or permission to natural, legal and foreign persons, control and oversight (the role of the National Security Council in particular), punitive, transitional and final provisions.

Bearing in mind that data and information are among the most important resources with which societies dispose, and that without them the elementary areas of everyday life would be impossible to maintain, it is necessary to adopt a holistic and multidimensional approach to the problem of storing and protection of classified data in public and private sector. The first assumption in their protection is timely prevention of their exposure and abuse.

Suggestions and Conclusions

1. With a view to establish the efficient exchange of classified and sensitive documents and data between the participants in the field of critical infrastructure risk management, as well as harmonizing the exchange procedures of with owners/operators of critical infrastructures it is necessary to create „Standard operative procedure (SOP) for classified and sensitive data and documents“.
2. For this purpose we suggest the establishment of intersectorial working group of stakeholder representatives from the system of critical infrastructure protection and risk management.
3. Accelerate the process of inclusion of private security sector in the TETRA communication system and in the “112 Service”.

7. PRECONDITIONS FOR DEVELOPMENT OF THE NATIONAL CI CENTRE

One of the main institutional preconditions for the establishment of an efficient CIP system is the development of a National CI Centre (NCIC) that would, among other tasks, coordinate the CIP activities taking into account important issues discussed above: PPP and classified data exchange.

As the Republic of Croatia has an established CIP system, the model and proposal for the establishment of the NCIC developed by our project partners from Croatia deserves to be mentioned. According to this proposal the establishment of NCIC will be the task for the Government of the Republic of Croatia, DUZS and other stakeholders. The NCIC should have clearly defined tasks, competencies and responsibilities for implementation of the regulations in the field of CI, as well as for the coordination and improvement of cooperation of all participants. DUZS and VVG propose two models for its establishment. According to the first model, the NCIC may be established either within the DUZS as an independent sector, as a service within the Civil Protection Sector, or as a department within the Service for Prevention, Planning and Analytics of the Civil Protection Sector. The second model proposes the intersectoral establishment of the NCIC as a separate agency of the Croatian Government.

Regarding its functionalities, NCIC would be in charge of: 1. creation of the holistic concept of the CIP, 2. review, harmonization and improvement of the relevant legal framework, 3. oversight of the implementation of the legal framework.

Some of the important short-term NCIC activities shall be: 1. creation of sectoral and intersectoral measures for identification of criticality levels, 3. definition of protection measures to be implemented depending on the identified criticality level, 3. implementation of the procedures for identification of a criticality level.

Regardless of its future structure, NCIC will perform its duties through the CIP Committee (intersectoral working group). The Committee members will have the role of security coordinators for CI. The main task of the committee would be the verification of documentation and procedures created by the NCIC. Such approach implies that NCIC has the mandate for the engagement of relevant professional institutions and experts with the purpose of creation of CIP related documents and procedures. The work of the committee would not require significant additional funds. On the other hand, for creation of the mentioned documents and procedures NCIC should obtain necessary financial means from the state budget.

RECIPE project partners agree that functionalities of NCIC both in Serbia and in Croatia should be clearly defined as the first step, as afterwards it would be easier to decide whether it should be established within an existing institution or as an independent body. The partners agree that NCIC must have both consulting and research aspect. Instead of simple information collection and distribution, the Centre needs to have capacities for their analysis, as well as capacities for oversight over the implementation of the Law on CI at the national level. As a good example and

potential model for the future NCICs in the region, the partners recommend the UK Centre for Protection of National Infrastructure http://www.cpni.gov.uk/ .

8. CONCLUSION

In the Republic of Serbia, the process of identification, prioritization, protection, resilience and legal regulation of the field of CI is at the very beginning. RECIPE project intends to provide assistance to the lawmakers and relevant state bodies to regulate this field in an easier and more efficient manner, through consultations and exchange of experience and good practice with the partners from the EU member states.

The creation and adoption of the Law on Critical Infrastructure is announced for 2016, and the results of the RECIPE project will be taken into account during the writing of its draft. Certainly, the existing problems and challenges will not be resolved with passing of this law. The CI sectors and facilities identification and prioritization, adoption of methodologies for the CI risk assessment, PPP in the field of CIP, exchange of classified data, as well as prospective establishment of the National Critical Infrastructure Centre are the main, but not the only challenges that lawmakers, CI owners and operators and other stakeholders in Serbia will face in the coming period. These challenges may be overcome by passing of the bylaws, adoption of amendments and harmonization of other relevant laws (e.g. Data Secrecy Law, Law on Public-Private Partnership, Law on Defence etc.), by education and raising awareness of CI owners and operators, by adoption and implementation of national and international standards and improved cooperation with academic institutions.

The project partners argue that CI sectors should be identified as 'narrowly' as possible, as the national capacities and state budgets are limited. For instance, the Republic of Croatia has identified eleven CI sectors, which is, in opinion of Croatian experts, too many for efficient protection. Consequently, the process of prioritization has caused much disagreement between CI owners and operators on one side, and lawmakers on another. On the other hand, the Directive 114/2008/EC identifies only two European CI sectors – energy and transport, which is arguably a too narrow classification to be applied for the national CI sectors. Therefore, a balanced solution between these two approaches should be found.

The establishment of PPP mechanism in the CI protection and resilience arena is of particular importance, as during the process of liberalization more CI facilities will pass into private ownership, whilst private security sector plays an increasingly important role. Long-term arrangements of private security companies in the contracts related to CIP and legal regulations on mandatory protection of facilities that private CI owners and operators must comply with are the key points of this issue.

The question of classified data sharing in the CIP system is a complex one and will need to be considered carefully by all stakeholders. An efficient and secure system of sensitive and classified data exchange needs to be established, with the accent on the 'horizontal' approach (exchange of data between sectors and CI systems), in comparison with the 'vertical' one, which is still prevalent, but is not quick and efficient enough. Furthermore, the provisions on the exchange of classified/sensitive data need to be incorporated in the future Law on Information Security, Regulation on Encryption Protection, and in the Cyber Security Strategy.

For purpose of the efficient implementation of the future Law on CI, as well as for collection, processing and analyses of the CIP related data, the partners propose establishment of National Critical Infrastructure Centre, modelled after the UK Centre for Protection of National Infrastructure. In Serbia, this centre could function either within the Sector for Emergency Management, as an independent organizational unit of the Ministry of Interior, or even as an independent Government agency.

This National Standpoints draft document on CI protection and resilience in the Republic of Serbia was submitted for review to all relevant stakeholders for comments and possible amendments. The final version in English language is submitted to the donor, i.e. European Commission, and will be used as the material for joint workshops at which the participants will exchange experience and good practice, which should consequently result with Guidelines/Instructions for better and more efficient CI management.