JRC Scientific and Technical Reports

Is Public Private Partnership a suitable way to cope with security issues?

Alberto Stefanini, Marcelo Masera

EUR 23824 EN - 2009

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the IPSC is to provide research results and to support EU policy -makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information

Address: TP 210 I-21020 Ispra (VA)
E-mail: marcelo.masera@ec.europa.eu
Tel.: +39.0332.789238
Fax: +39.0332.789576

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC49803

EUR 23824 EN
ISBN 978-92-79-12416-7
ISSN 1018-5593
doi:10.2788/10855

Luxembourg: Office for Official Publications of the European Communities

Printed in Luxembourg

Is Public Private Partnership a suitable way to cope with security issues?

Alberto Stefanini* and Marcelo Masera, JRC
e-mail: marcelo.masera@ec.europa.eu

* Contract Agent (November 2005-November 2008)

Abstract

This report investigates whether Public Private Partnership (PPP) is a suitable approach to tackle global security issues, with special reference to sensitive information sharing in the context of critical infrastructures protection. To this aim, it outlines the PPP concept starting from its introduction in the early nineties, and provides a critical view on the questions that arise in many application areas of PPP. An overview of the current EU guidelines concerning PPP is provided. Concerning security information sharing, early and current attempts to apply PPP are summarised, and the open issues involved highlighted.

Table of contents

1 Introduction

The term *Public-private partnership* (PPP) has been associated in the last decades to ventures (mainly public services) funded and operated through a partnership of government and one or more private sector organisations. The concept of PPP has evolved and changed in the last decade, at times referring to different kinds of organisational arrangements, type of stakeholders and participation arrangements, financial provisions, and focus of the activities.

When first used as a concept, it was understood that typical PPP arrangements took place where the private sector supplied infrastructure assets and services traditionally provided by governments. However, many sorts of collaborations between public bodies, such as local authorities or central government, and private companies tends nowadays to be referred to as public-private partnership [Wikipedia, PPP: 2007-08] [Primer, 2008].

In some types of PPP, the government uses tax revenue to provide capital for investment, with operations run jointly with the private sector or under contract. In other types (Private Finance Initiative), capital investment is made by the private sector based on a contract with government to provide agreed services. Government contributions to a PPP are often in kind (notably the transfer of existing assets). Some authors consider the presence of external financing as a necessary condition; others focus specifically on design-build-finance-operate arrangements.

The spread of meanings attached to the term is quite significant, paving the way to imprecision and misunderstandings. Public private partnership is a relatively new concept (pressures that lead to its introduction date back to the economic dislocation of the late seventies and eighties) but its applications grew up extensively and stimulated a lively debate about the economic effectiveness of PPP together with several research strands in economics since then. Early in this decade, this also motivated the European Commission to try and provide a reference framework for PPP in its member states. (REF)

PPP has been extensively applied to public services implying large capital investments like public transports, for then being used in other service sectors, like health services and health care programs. Its application to security information sharing is recent a: it was pioneered in the US in 1996 with InfraGard, an FBI initiative to address physical and cyber threats to critical infrastructures, with the goal to promote dialogue and timely communication between private stakeholders and the FBI, so as to give InfraGard members timely access to information that enables them to protect their assets, and in turn give the government information useful to prevent terrorism and other crimes. In recent years InfraGard was questioned on ground of unconstitutionality, appearing as an attempt to turn private-sector corporations into surrogate eyes and ears for the federal services.

This report is mainly based on a literature compilation from the press and other open commonplace sources, so as to provide a broad picture of PPP and its security related applications and pinpoint elements to evaluate whether public private partnership is a suitable approach to tackle global security issues. In Chapter 2 the PPP concept is outlined starting from its introduction in the early nineties, early and current attempts to apply PPP are summarised, and a view of the questions that arise in many application areas of PPP is given. Chapter 3 shows as the EC tried to face the key questions by providing guidelines concerning risk assessment and negotiation of PPP agreements. In the final chapter, we focus on application of PPP in the security arena, and try to highlight the open issues involved.

2 The concept of PPP: history, main application areas, open issues

2.1 PPP history

Pressure to change the standard model of Public Procurement arose initially from concerns about the level of public debt, which grew rapidly during the macroeconomic dislocation of the 1970s and 1980s. Although the initial concept that private provision of infrastructure represented a way of providing infrastructure at no cost to the public has now been generally abandoned, the interest in alternatives to the standard model of public procurement persisted. In particular, it has been argued that models involving an enhanced role for the private sector, with a single private sector organisation taking responsibility for most aspects of service provisions for a given project, could yield an improved allocation of risk, while maintaining public accountability for essential aspects of service provision [Wikipedia PPP, 2007-08].

Initially, most public-private partnerships were negotiated individually, as one-off deals. In 1992, however, the Conservative government of John Major in the United Kingdom introduced the Private Finance Initiative (PFI), the first systematic program aimed at encouraging public-private partnerships. In the 1992 program, the main focus was on reducing the Public Sector Borrowing Requirement, although the effect on the public accounts was largely illusory. The Labour government of Tony Blair, elected in 1997, persisted with the PFI but sought to shift the emphasis to the achievement of 'value for money' mainly through an appropriate allocation of risk [ibidem].

The Private Finance Initiative (PFI) immediately proved controversial, as it was perceived by critics within the Labour party as a back-door form of privatisation [Wikipedia: PFI, 2007-08]. Nonetheless, the Treasury found the scheme advantageous and pushed Labour to adopt it after the 1997 General Election. Hence PFI has continued and, indeed, expanded under Labour. Under PFI, contractors pay for the construction costs and then rent the finished project back to the public sector [BBC News, 2003].

Critics against PFI have raised the following points:

- Taxpayers will in the end pay even more with privatisation. According to a survey conducted by the Labour Research Department, the 'rent' for PFI projects in the health service alone will top £13bn. There are also cases such as the Fazackerly prison in Liverpool, where the initial cost of the project has been paid back within two years, leaving 23 years of pure profit from the construction.
- The only way companies can turn a profit is by cutting employees' wages and benefits. Unions talk of jobs being 'privatised'. Their members are shifted into the private sector, where they have fewer employment rights and benefits.
- Some early PFI projects were not up to standards, and there are also cases where PPP proved a failure, like one of the most famous privatisations under the Conservative government, British Rail. Railtrack - responsible for track, signals and stations - had to be taken into administration by Labour amid huge debts, and the rail network may in future be run by a not-for-profit company [*ibidem*].

Controversy is also caused by the off-balance-sheet nature of PFI contracts. Under UK accounting, the PFI company does not enjoy the risks and rewards of the building - the government carries demand risk, for example - so the building is not shown on its balance sheet. Instead its main asset

is the finance debtor - the long term contractual obligation of the government to pay for the building. For the government accounting, the fact that it pays a single charge (the 'Unitary Charge') for both the building and its maintenance is sufficient for it to be classed as a revenue item, so neither the building or the long-term obligation to pay appear of the government's balance sheet. Were the total PFI liability shown on the UK balance sheet - as would be required under UK accounting standards - the government's finance would look somewhat different [Wikipedia: PFI, 2007-08].

Advocates of PPP say that many hospitals and schools would not be built at all if it were not for private finance, as public money was simply not available. They claim that PFI will lead to a dramatic increase in the quality of public services. Performance-related penalties that are now built into most PFI contracts will ensure a continuing improvement in standards, far in advance of anything that could be achieved in the public sector, they argue. The government has staked its reputation on delivering better public services but it is also aware that there is a limit on how far taxes can be raised. PFI is a fast, effective - and in the short term at least - cheap way of getting new facilities built. The biggest hospital-building programme in living memory is currently underway thanks to PFI Local authorities are increasingly being steered towards PPP [BBC News, 2003]. There are some areas where public-private schemes may ultimately prove unsuitable. Some PFI projects, such as Capita's managing of the housing benefit system in Lambeth and some IT projects, have already proved disastrous. But the government is hoping that the current hospital and school building programme will demonstrate to sceptics - and the unions - that it is the only way to revamp the country's ailing public services [*ibidem*].

2.2 PPP application sectors

A growing number of countries showed interest in following the most advanced administrations on the topic: Australia (Partnership Victoria) and the U.K. (Private Finance Initiative). Developing countries, in particular, try to develop PPPs to address economic infrastructure bottlenecks. However, the trend is universal: a recent study of PPPs in Europe found that between 1990 and 2005, more than a thousand partnerships had been signed in the European Union alone, representing an investment of almost 200 € billions [Primer, 2008].

In summary, the PPP concept has found wide application especially in infrastructural projects, typically roads, schools, prisons and hospitals, but it is not limited to such sectors. For instance, a recent study by Deloitte [2007] provides a view of the way public-private partnership is used to close the infrastructure gap worldwide. The study provides an overview of significant PPP projects worldwide, an analysis of major drawbacks on past PPP projects and recommendations about the way governments and public authorities should manage such projects. Application areas range from Transport to Water and wastewater, Education, Hospitals, Defense, Public Housing land and Development. Major applications in the EU are reported in chapter 4.

According to the Primer [2008], major applications of PPP in the US include Public infrastructures, like the State Route 125, San Diego, California, the Central Park, New York City, the Chicago Skyway Bridge and the redevelopment of downtown Chattanooga, Tennessee from the mid-1980s to present, but also Innovative Technologies, like the California Fuel Cell Partnership (CaFCP), Finance (the Federal Reserve) and Security (InfraGard - which is a main focus of Chapter 4 of this report).

Finally, the concept may also be applied to Public Social Private Partnerships (PSPP), defined as enterprises having social purpose, i.e. carrying out activities for the protection, support and improvement of opportunities for disadvantaged people, and implemented in partnership between public, purely commercial and social economic organizations and/or enterprises.

In fact, some large international health care programs may be considered public-private

partnerships, e.g.: The Global Alliance for Vaccines and Immunization is financed per 75% (750 Mio.US$) by the Bill and Melinda Gates Foundation.

As a UN agency, the World Health Organisation is financed through the UN system by contributions from member states. In recent years, the WHO's work has involved more collaboration with NGOs and the pharmaceutical industry [Wikipedia PPI 2007-08].

2.3 The debate on PPP

Because of the focus on avoiding increases in public debt, many private infrastructure projects in the early 1990s involved provision of services at substantially higher cost than could have been achieved under the standard model of public procurement. The central problem was that private investors demanded and received a rate of return that was higher than the government's bond rate, even though most or all of the income risk associated with the project was borne by the public sector [Wikipedia, PPP: 2007-08]. Although the general view that governments should seek "value for money" has been widely accepted, there have been continuing disputes over whether the guidelines designed to achieve these goals are appropriate, and whether they have been correctly applied in particular cases. Much of the discussion has been based on debates over the UK Private Finance Initiative.

In the main, experts still argue about [Primer, 2008]:

- the proper definition of PPP
- their microeconomic foundations
- their possible role as an antidote to the worldwide downturn in infrastructure investment

The research literature on PPPs follows various strands. One, following Schleifer [1998] in the comparison of the respective interests of private and public ownerships, underlines the roles of potential cost reduction leading to non-contractible deterioration of quality; innovation; competition and consumer choice; reputation mechanisms [1]; and government's credibility (non versatility). Its results are confirmed by another strand of literature, following a model pioneered by Hart [2002] and focusing on the advantage of contracts bundling construction and operation. Consensus currently crystallizes on a few singular points [Primer, 2008]:

PPPs to be limited to projects delivering greater Value for Money than other forms of procurement

- the contractibility of the quality of service
- the transfer of a significant share of risks to the private sector
- the presence of competition or incentive-based regulations
- a sound institutional and legal framework
- a sufficient level of technical expertise in the government
- the proper disclosure of PPP commitments, along with government guarantees, in government financial statements.

In conclusion, consequences of the generalization of PPPs are yet far from clear. The debate especially focuses on the fiscal aspects:

- accounting and off-budget spending

[1] potential loss of reputation because a partner reneges an agreement is a significant risk involved in PPPs. Partners often have different objectives when forming a partnership. If the common goal of the partnership is not defined clear enough, there is significant risk that one of the partners may renege the agreement when its expectations are no longer met.

- adequate control procedures
- best systems to negotiate and manage PPP contracts.

The following chapter overviews the state of affairs in the EU and focuses on the guidelines issued by the EC on these latter subjects.

3 PPP in the European Union: the EC guidelines 2003 and EC Communication C(2007) 6661

The quoted study by Deloitte [2007] analyses several application sectors for PPP worldwide and stresses among other the following major areas of application of PPP in the EU:

- **Transport.**
    - "Spain and Italy have considerable experience using PPPs for roads.
    - Most of the existing toll highways in Spain were put out to concession in the 1960s.43 Today, the government hopes to use PPPs to fund one-third ($113 billion) of the estimated investment needed in road and rail between 2006 and 2020.44.
    - Similarly, the transportation sector makes up the bulk of PPPs in Italy (with a value of $11.4 billion)".
- **Water and wastewater.**
    - "The largest European water PPP is in the Netherlands, where the Water Board of Delfland awarded a 30-year concession, with a total contract value of €1.58 billion. The project includes the design, construction, and operation of a new wastewater treatment plan and, to comply with more stringent discharge requirements, the refurbishment and operation of an existing wastewater treatment plant".
- **Education.**
    - "The United Kingdom is home to the world's largest and most sophisticated PPP schools program. Most new schools and tertiary education institutions are built under the PFI or some of its variants. All in all, nearly 100 education PFI deals valued at £3.5 billion have been signed. Over the next 10 –15 years, every school in Britain will be brought up to 21st century standards through a program called Building Schools for the Future. A$37 billion investment in new buildings and refurbishment will be delivered through a combination of joint venture models and more traditional design-and-build contracts, information technology and communication contracts, and facilities management contracts".
- **Hospitals.**
    - "Since 1997, 85 percent of funds for major UK National Health Service projects have come under the PFI scheme. The total number of PFI hospital projects, 130, dwarfs the 12 publicly funded hospital projects developed during that time.
    - In Portugal, 31 hospitals will be built using PPPs. The entire program, at an estimated cost of $37 billion, should be complete by 2014, with 10 new hospitals launched in 2006".
- **Public Housing land and Development.**
    - "The country with the deepest experience in this sector remains the Netherlands, which has been applying PPPs to social housing and regeneration projects for nearly two decades. Joint venture, the most commonly used PPP arrangement for these projects, suits the local governments' need to retain control over planning and development while utilizing the private partners' available resources and

expertise. PPP contracts typically last for 5 to 10 years, after which the land owner (the government or the private partner) takes ownership of the project. This model proved quite successful for more than 100 locally initiated projects in the Netherlands".

- **Defense.**
    - "The UK Ministry of Defense has employed various PPP models for more than 56 defense projects—everything from building military accommodations to training personnel to putting up satellites. Total value: £4.65 billion.60
    - The German defense ministry has likewise initiated a number of innovative defense PPPs. An Army maintenance joint venture with HIL GmbH involves the entire value chain for 10,000 combat systems (not including system purchase)".

This wealth of application sectors and areas – together with the many criticisms and concerns that wide adoption of PPP had caused, as seen in Chapter 2 – motivated the EC to formulate appropriate guidelines [2003] to ease analysis of the inherent risks related to this type of funding and provide guidance about how to perform negotiation between public authorities and potential private partners.

Later on in 2005, on the basis of a Green Paper (IP/04/593), the European Commission has launched a debate on the desirability of adapting the Community rules on public procurement and concessions to accommodate the development of public-private partnerships (PPPs). The main objective was to see whether it is necessary to improve the current rules in order to ensure that economic operators have access to PPPs under conditions of legal clarity and real competition. Further consultation among concerned parties has brought the EC to an interpretative Communication [C(2007) 6661] concerning Public Procurement and Concessions to Institutionalised Public-Private Partnerships (IPPP).

3.1 The EC Guidelines 2003

The Services of the European Commission have a particular interest in PPPs in view of the grants they provide within the context of Cohesion and Structural Funds and of the Structural Policies for PreAccession. In March 2003 the Directorate General Regional Policy of the European Commission - in consultation with the other concerned services of the EC - issued the *Guidelines for Successful Public-Private Partnerships*. Those guidelines identify four principal roles for the private sector in PPP schemes:

- to provide additional capital
- to provide alternative management and implementation skills
- to provide value added to the consumer and the public at large
- to provide better identification of needs and optimal use of resources

The Guidelines point out four **key issues** influencing the design of projects and their implementation. Although these are characteristic of grant financing in general, in view of cooperation with the European Commission their recognition and integration at an early stage facilitates project acceptance by the EC and more effective implementation:

1. *ensure open market access and competition.* A key requirement of Commission financing is that PPPs should neither impact on open market operation nor on the clear and transparent rules of these markets. This is particularly relevant to tendering and selection procedures, the grant purpose and provisions for contract renewal (especially about the length of concession agreements).

2. *protect public interest and maximise value added.* This requirement impacts in many forms over project design, scope and implementation. EC grants require that local public partners adopt European norms, quality and performance standards and effective monitoring and management. Public interest is to be taken into account concerning tender, evaluation and contracting (e.g. by re-negotiating a grant so as to sustain local capacity if required). The important role for the public must be recognised by encouraging the creation of independent consumer groups and associations acting as watchdogs.
3. *define the right level of grant financing.* The EC must ensure that its grants match real needs, so as to ensure financial efficiency and optimal use of limited funds. Grants must not constitute incompatible state aids. A further concern is to achieve balance between facilitating project realisation and limiting undue private sector's profits from grants.
4. *select the most suitable PPP type.* The degree of private involvement must match the objectives of the project and the needs of the public. A detailed cost/benefit assessment of private sector involvement vs. public alternatives must be undertaken to ensure that PPP enhance public benefit. Appropriateness, cost, ability of effectively implement and manage should be the paramount considerations in selecting a PPP structure.

The Guidelines present five thematic parts dealing with:

- *PPP structures, suitability and success factors*. Four broad categories of PPP structures are presented, each with increasing degrees of private sector involvement.
- *Legal and regulatory structures.* The legal environment for PPP projects is defined, in view of the existing legal provisions at the Community, national, regional and municipal level.
- *Financial and economic Implications of PPPs.* This part addresses the topic of risk management and its financial impact on a project. Several techniques and considerations are presented for determining and assessing value.
- *Integrating grant financing and PPP objectives.* The relative strengths and weaknesses of grant financing are assessed in view of the opportunities offered. The ability to use grants in a PPP depends on the ability to meet the constraints and provide sufficient safeguards to protect the grant providers' objectives.
- *Conception, planning and implementation of PPPs.* This part considers the PPP project cycle with the objective of providing a detailed discussion of the issues encountered and possible solutions, in view of the key issues presented above.

3.2 The Green Paper IP/04/593 and the EC Communication C(2007)6661 on Public Procurement

Following the broad adoption of PPP in many member states, it was considered necessary to explore how procurement law applies to the different forms of PPP, in order to assess whether there was a need to clarify, complement or improve the current legal framework at the European level.

To this end, on 30 April 2004, the Commission adopted a Green Paper on Public Private Partnerships and Community Law on Public Contracts and Concessions (IP/04/593). The Green Paper focused on the choice of a private partner by a public authority: this must be made in accordance with Community rules on the awarding of public contracts.

However, there was no specific system under Community law for PPPs and the Community rules on awarding public contracts were applied to PPPs with differing degrees of intensity. The Green Paper set out the scope of Community rules, with a view to identifying any uncertainties and assessing to what extent Community intervention might be necessary.

Respondents to the public consultation asked to clarify specifically two issues:

- **Institutionalised PPPs:** how EU rules should apply concerning the choice of private partners in "institutionalised PPPs" (IPPPs), i.e. public service undertakings held jointly by both a public and a private partner
- **Concessions:** what is meant by 'concessions' and the rules applicable to their award. Respondents expressed support to a legislative initiative of the EC in this regard.

A legislative initiative was deemed to be the preferable option to clarify the issues pointed out by the public consultation. Following further in-depth analysis, including an Impact Assessment, which was carried out in 2006, on 5 February 2008 the Commission adopted the Interpretative Communication C(2007)6661 [EC 2007] on the application of Community law on Public Procurement and Concessions to Institutionalised Public-Private Partnerships (IPPP). This Communication defines PPPs as *'arrangements which typically involve complex legal and financial arrangements involving private operators and public authorities developed in several areas of the public sector and widely used within the EU, in particular in transport, public health, public safety, waste management and water distribution'*.

The Communication explains the EC rules to comply with when private partners are chosen for IPPP. Depending on the nature of the task (public contract or concession) to be attributed to the IPPP, either the Public Procurement Directives or the general EC Treaty principles apply to the selection procedure of the private partner.

The Communication expresses the view of the Commission that under Community law, one tendering procedure suffices when IPPP are set up. The Communication also states that as a matter of principle IPPP must remain within the scope of their initial object and cannot obtain any further public contracts or concessions without a procedure respecting Community law on public contracts and concessions.

However, it is acknowledged that IPPP are usually set up to provide services over a fairly long period and must, thus, be able to adjust to certain changes in the economic, legal or technical environment. The Communication explains the conditions under which these developments could be taken into account.

4 PPP & Security

Since the late '90s, when cybersecurity threats were first recognised to be a major challenge against critical infrastructures [2], it was clear the need to find proper means for connecting the public dimension of the problem (related to the safety and security of society, but also to the deployment of needed infrastructural services), with the private one (both concerning the owners and operators of infrastructures, for the most part private, and the end users).

The first reaction across the globe was to establish links between companies and governments,. In the United States, a Partnership for Critical Infrastructure Security was launched by President Clinton on February 15, 2000 to maximize cooperation between government and private sector initiatives for cyber-security. Since the vast majority of the United States critical infrastructures are owned and operated by private industry, the main motivation for such Partnership was simple: *'recognizing that the Federal government could not protect these infrastructures alone nor assure the delivery of services over them'* [White House, 2000]. This strategy was later confirmed under the Bush presidency [White House, 2003], [White House, 2007].

The use of the term "partnership" in this context differs radically from those provided in the context of infrastructure privatisation [Wikipedia PPI 2007-08, Primer 2008]. From 2000 on, the PPP label begun to be attached to all types of interactions between public and private actions in the security field, and became the de facto standard. This label doesn't seem to convey any specific connotation, and it doesn't link with the legal and political use of the term until now:

> "*State, local, and tribal governments carry out their counterterrorism responsibilities within the broader context of their core mission to protect the public's health and safety and to provide emergency and non-emergency services… Success in these endeavours depends on a strong partnership with the public, built on a foundation of communication and trust between local officials and the members of their community*" [White House, 2007].

Uncertainty about what is meant by PPP in the security context results in potential misconceptions of the roles and responsibilities of the different actors: what is expected from them, which are the liabilities and obligations, which can be the legal effects of certain activities, etc. This situation asks for further reflection as a superficial use of the term might undermine the initiatives making use of the concept.

Nevertheless nowadays, the majority of developed countries declare to foster PPP as a way to cope with challenges against infrastructure security through dedicated programmes, like InfraGard [1996-2008] in the US and EPCIP [EC, 2004, 2006] in the European Union.

Historically, two main motivations were advocated for sustaining the adoption of public private partnership schemes in the security arena:

1. Public and private partners derive a common benefit from collaboration: typically, they achieve stronger security by sharing sensitive information and data concerning the assets/business under their responsibility. Partners involved may be working in (and across) different sectors, like:
    - process industries (power, gas, oil, utilities, etc.) making use of the same monitoring

[2] I.e. infrastructures providing key services upon which global security and economy depend, as well as the well-being of the citizens. According to the EC [2004] critical infrastructures *'consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States'.*

and control devices, and manufacturers of these same systems and devices;

- stakeholders (suppliers, end users, regulators, etc.) in a given business, e.g. power, gas and water distribution.

2. Public and private partners actually share the burden of taking joint decisions *(usually referred as governance)* because they have common responsibility upon an asset, like a critical infrastructure. They need to cope with security risks, jointly respond to incidents and manage crises by coordinating their actions. Collaboration may involve asset owners and operators, police forces and civil protection, and concern diverse activities like risk analysis, pre-emptive defense/surveillance measures, territorial control, counter terrorism operations, crisis management, control under emergency, restoration etc., and shall take place under a legal and regulatory framework where respective responsibilities are well defined by the government bodies in charge (e.g. the ministry of internal affairs and the regulating authorities in charge).

Nowadays, many such security-related collaborations already take place among partners at the national and international level; they may either be sporadic and due to specific events/initiatives, or be continuous and take place within a common framework and/or well defined international agreements.

The two different motivations above bear some continuity in between, because information sharing may actually lead to joint risk analysis, and this to pointing out and recognising the need for a stronger operational coordination. Thus, we may say that data and information sharing stands on the lower end of a spectrum, because it is a pre-condition to stronger collaboration: in fact, currently security related data is scarce, dramatically insufficient. Without data about vulnerabilities, incidents, etc., no effective assessment, no management, no assurance is possible.

On the other hand, gathering security-related data is hard: sources are diverse and scattered, crucial information may be missing, make analysis difficult and compromise objective comparison. Moreover, there may be several obstacles to distribution and joint analysis of security related information:

- stakeholders play different roles (e.g. regulators, owners and operators). They have jurisdictional limits. They may be competitors. All this inevitably leads to different attitudes and standpoints which reflect into different security concepts and languages;
- sharing security sensitive data raises legal concerns for two orders of reasons:
- disclosing vulnerabilities may compromise classified information and put at risk company assets and business; fair competition can be endangered.
- associating private companies to public authorities in any programme related with gathering security related information would bring the former to surrogate state responsibilities and may be deemed to violate civil rights on many grounds.

These difficulties may be enhanced when public and private partners have to agree upon liabilities and cost of security measures [Andersson and Malm, 2006].

Furthermore, although the concept of PPP remains rather fuzzy, it remains to be seen whether it can really be stretched so as to apply to partnerships of any kind between public authorities and private partners in the area of security.

It is clear, for instance, that simple agreements among public and private partners in order to share security relevant data do not easily fit with the commonly understood meaning of PPP as a *'government service or private business venture which is funded and operated through a partnership of government and one* or more private sector companies' [Wikipedia PPI 2007-08] and may hardly fit even the broader definition contained in the interpretative Communication C(2007) 6661: *"complex legal and financial arrangements involving private operators and public*

authorities in several areas of the public sector, in particular in transport, public health, public safety, waste management and water distribution".

4.1 Security Information Sharing and Analysis about Critical Infrastructures: the ISACs and the WARPs

4.1.1 ISACS in the USA

Information Sharing and Analysis Centers (ISACs) are US voluntary organisations which group together stakeholders in a given sector (e.g. Communication, Electricity, Emergency Management and Response, Financial Services, Highway and Information Technology) and federal administrations in order to facilitate voluntary collaboration and information sharing among its participants. The objective of the ISACs is to gather information on vulnerabilities, threats, intrusions, and anomalies from sector industries, government, and other sources, and promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist the sector participants take protective actions.

ISACs were established on the turn of the century when threats against US critical infrastructures became apparent. For instance, the NCC-ISAC, which was designated as the ISAC for telecommunications, commenced operations on March 1, 2000. The initial membership was based on National Communication Center (NCC) membership, which reflected a broader base of technologies comprising the telecommunications infrastructure.

The NCC is one of the services of the National Communications System (NCS), an office within the United States Department of Homeland Security charged with enabling national security and emergency preparedness communications. The genesis of the NCS dates back to the sixties, after the Cuban missile crisis when communications problems among the United States, the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state threatened to complicate the crisis further. After 40 years with the US Secretary of Defense, the NCS was transferred by President Bush to the Department of Homeland Security in March 2003.

The White House report [2007] confirms that information sharing with the private sector about Critical Infrastructures security remains a basic strategy of the US government – because the private sector is estimated to own and operate about 85% of the US critical infrastructures – and quotes terrorist attacks on transportation infrastructures in Madrid (2004) and London (2005) as a further proof of the need for strengthening collaboration with the private sector in this area. The report quotes the following as key factors to motivate governmental efforts to improve information sharing with the private sector:

- *'Current, reliable, accurate, and actionable information is critical to private sector decisions to protect their business;*
- *Private sector entities gather, process, analyze, and share information in order to protect their companies, assets, employees, infrastructure, and ability to operate, so as to maintain a competitive advantage;*
- *In many cases, private sector entities have spent years establishing strong working relationships with Federal, State, and local law enforcement and other entities; this Strategy respects and encourages those established relationships;*
- *The private sector operates within multiple information sharing frameworks: industry executives often prefer to separately share threat-related information with Federal and State as well as local government officials and other business executives as they assess the threat environment in which they operate, implement protective measures, and engage in*

emergency response planning activities;

- *As we incorporate the information sharing needs and capabilities of the private sector into our efforts to enable information sharing, we need to recognize that at times the environment in which homeland security, law enforcement, and terrorism-related information is shared mirrors the regulatory environment in which the sharing entity operates; and*
- *The private sector relies on multiple information sources including professional and local organizations, private information providers, news outlets, colleagues, open intelligence sources on the web, and company management in both domestic and foreign locations, in addition to the government at all levels (Federal, State, and local)'.*

The said report quotes a number of collaboration mechanisms to "facilitate the flow of information, mitigate obstacles to voluntary information sharing, and provide feedback and continuous improvement regarding structure and process". In addition to ISACs, these include Sector Coordination Councils, Government Coordination Councils, and a National Infrastructure Coordinating Center. ISACs are coordinated by the ISAC Council, whose mission is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government.

The public counterpart of the ISAC Council is the MS-ISAC (http://www.msisac.org/), a voluntary and collaborative organization with participation from all 50 US states and the District of Columbia. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and with local government.

Major objectives of the MS-ISAC include:

- disseminating early warnings of cyber system threats
- sharing security incident information
- providing trending and other analysis for security planning
- distributing current proven security practices and suggestions
- promoting awareness of the interdependencies between cyber and physical critical infrastructure, as well as between and among the different sectors.

The MS-ISAC was launched in 2004 compliant with the objectives of the National Strategy to Secure Cyberspace, established under Bush Presidency in January 2003 [White House 2003].

The effectiveness of the ISACs is rather controversial. For instance, the FS-ISAC (Financial Services Information Sharing and Analysis Center) proved its effectiveness in February of 2000, when it saved its membership from falling victim to the widespread denial of service attacks that affected much of the industry [SearchSecurity 2008]. The ES-ISAC, the Electricity Sector ISAC, is strongly related to a pre-existent organisation, the North American Reliability Council (NERC), which was quite effective in issuing appropriate guidelines for physical and cyber security to its members since 2002-2003 [NERC Security Guidelines 2002-2008].

However, a report of the National Infrastructure Advisory Council [NIAC 2004] found several inadequacies and drawbacks in the way ISACs were organised, and made recommendations about how to re-organise them, better integrate their membership and improve information dissemination. Although the report outlined a framework for action, it did not recommend government intervention into any sector – also due to the wide difference among the various sectors.

After the NIAC study, there is evidence that the ISAC effort was reorganised and took momentum

at least concerning the electricity sector, where the NERC became the reference organisation as the North American ERO (Electricity Reliability Council) in charge of ensuring compliance of the sector to its security guidelines.

4.1.2 Information exchanges and WARPs in the UK

UK launched two types of organisations for dealing with the sharing of information about critical infrastructure risks: information exchanges and WARPs. Though both initiatives rely upon the cooperation between public and private actors, their structure and functioning rules have no point in common with the definition of PPPs in the British or European context – as described beforehand. In any case, they are valid examples of beneficial activities in the security domain based on the partnership of public and private actors.

WARPs (Warning, Advice and Reporting Point) were launched in 2005 by the NISC, the n the UK government authority – now absorbed by CPNI (the UK's Centre for the Protection of National Infrastructure)- which offered protective security advice to businesses and organisations across the national infrastructure, in order to provide a community based service where members can receive and share up-to-date advice on information security threats, incidents and solutions [WARP 2005-08].

A WARP is a community based service where members can receive and share up-to-date advice on information security threats, incidents and solutions. Therefore it is dependent upon the active participation and organisation of the community members.

A WARP is to provide three core services:

- filtered warning: where members receive only the security information they need, selected via an on-line tick-list;
- advice brokering: where members can learn from other members' initiatives and experience, possibly through a members' bulletin board;
- trusted sharing: where reports are anonymised so that members can learn from each other's attacks & incidents, without fear of embarrassment or recrimination.

WARPs has the advantage of being able to customise its services (e.g. early warnings) to the needs and requirements of the participants. This is in any case facilitated by a toolbox and guidelines provided by the NISCC/CPNI.

Contrary to the ISACs, however, the WARPs are organised either on a territorial or on a corporative basis. They group:

- public services
- local government
- business
- voluntary organisations.

Penetration in business communities appears however in its early stages. Currently there exists 5 business WARPs only:

- ANSWARP: provides WARP services for local authority users of Anite Swift software.
- BTRWARP: groups British Telecom end-users
- LS1WARP: aimed at a small community within The Law Society's membership centred in London
- NECWARP: a WARP for the private SME Sector of the North East of England

- PENWARP: a WARP for journalists

In addition, the UK government has promoted the setting up of dedicated Information Exchanges (IE) in various CIP sectors. It is recognised that these mechanisms, although potentially very useful, are hard to build as they are based upon the personal mutual trust of the participants. For facilitating their development, the sharing information is carried out in confidential meeting, run under a version of the Chatham House Rule.

Up to the end of 2008, the following IE's have been set up:

- ADMIE
  - The Aerospace and Defence Manufacturer's Information Exchange was formed in December 2006, to share confidentially mutually beneficial information regarding electronic security threats in the aerospace and defence sector. The ADMIE comprises UK-based organisations involved in this sector.
- FSIE
  - The UK Financial Services Information Exchange was formed in February 2003, to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the UK financial sector. The FSIE includes members from UK-based financial organisations including banking, insurance, securities, service providers, exchanges and CPNI.
- MSPIE
  - The Managed Service Providers Information Exchange (MSPIE) consists of commercial organisations that supply IT services and security to UK CNI customers in the public and private sector. The main aim is to understand risks better and improve security to the benefit of customers, clients, stakeholder and UK national security through information sharing and cooperation. The MSPIE achieves this by facilitating the sharing of information in a confidential and trusted environment concerning threats, vulnerabilities and incidents of electronic attack between its membership.
- NSIE
  - The UK Network Security Information Exchange (UK-NSIE) was formed in April 2003 to share sensitive information in the information and communications technologies sector. It currently includes IP providers; core mobile operators; and traditional telecommunications providers, as well as CPNI. Participating companies now cover over 80% of the telecommunications market in the UK. It is linked to NSIE in USA, of which BT is a member. BT acts as the channel for information between the two Exchanges. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include: a guide to the procurement of resilient telecoms; best practice guidance on the secure implementation of BGP.
- PIIE
  - Pharmaceutical Industries Information Exchange was formed in September 2006 to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the pharmaceutical industry. All of the PIIE members are from global pharmaceutical corporations that have a significant UK interest.
- SCSIE
  - The SCADA and Control Systems Information Exchange is for those companies that

are dependent upon SCADA (Supervisory Control and Data Acquisition) or other process control or telemetry systems. Formed in October 2003, it shares confidential and mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the SCADA and process control environment. The SCSIE includes members from UK-based energy, transport and water companies. It has produced and is currently working on good practice guidance. Completed guidance includes: Implement secure architecture, understanding business risk, firewall deployment for SCADA and process control networks to name but a few.

- TSIE
  - The Transport Sector Information Exchange was formed in September 2006 and expanded coverage of the aviation sector Information Exchange to include other major transport methods.
- VSIE
  - The Vendor Security Information Exchange (VSIE) was formed in January 2005 to share confidentially mutually beneficial information regarding electronic security threats among the major companies involved in the ICT industry. The VSIE comprises members of major international companies in the ICT sector.
- SRIE
  - The Security Researchers Information Exchange (SRIE) was formed in November 2006 to share confidentially mutually beneficial information regarding electronic security threats in the penetration testing and security research sector. The SRIE comprises of members of UK penetration testing and security research companies.

4.2 The European SCADA and Control Systems Information Exchange

The European SCADA and Control Systems Information Exchange (E-SCSIE) is a Pan-European group designed to facilitate the exchange of information between its members, in a confidential and trusted environment, concerning threats, vulnerabilities and cyber incidents, or any other event negatively affecting process control networks and environments. The E-SCSIE also deals with solutions to risks associated with process control networks and environments [SCNI 2007-08].

The E-SCSIE includes:

- national Authorities;
- industrial users of SCADA systems which provide critical services (electricity, oil & gas, water, food, transports) or run potentially hazardous processes, e.g. chemical, radiological, biological, and nuclear;
- research institutes working on SCADA security technologies.

The E-SCSIE was started in 2004 by an initiative of the NISCC, the former UK National Information Security Co-ordination Centre [3], after they organised a successful SCADA Security Conference in London (May 2004),with the support of other European governmental agencies and the Joint Research Centre of the European Commission. It is currently chaired by the European Organisation for Nuclear Research (CERN) and the Swedish Energy Management Agency (SEMA).

The E-SCSIE has held ten meetings since June 2005, although its Membership Guidelines were initially set in June 2007 only, after long consultation among the partners. These set the terms of reference and the membership criteria of the group. Moreover strict rules for joining the E-SCSIE

[3] Today CPNI, Center for the Protection of the Critical Infrastructures

were established, which prescribe among other that unanimity is required to accept a new entry, and for information exchange among partners: in order to create a confidently high level of trust between the members, all members adhere to the Traffic Light Protocol [*ibidem*], [Freedictionary 2008], established in the last century for face-to-face meetings among British officers.

Information sharing includes

- discussions on the many good practice guides, standards and recommendations on Control System Cyber Security, and their application to existing and future control systems;
- the exchange of incidents and the discussion on possible mitigations;
- the provision of a forum to exchange information between governmental bodies and end-users on e.g. regulations, joint initiatives, etc.;
- the distribution of information being discussed in regional information exchange groups.

The long period between the earlier meetings and the acceptance of the membership guidelines is significant of how difficult is to gain trust among public authorities and private partners, especially in an international setting.

4.3 InfraGard and TIPS

According to its website InfraGard [1996-2008] is 'an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States'.

InfraGard is a Public-private partnership that began in the Cleveland, Ohio, FBI field Office in 1996, initially as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program then expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility to the former National Infrastructure Protection Center (NIPC). In 2003 responsibility passed to the FBI's Cyber Division. While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures, and InfraGard's mission expanded accordingly.

The authoritative White House report on the US National Strategy For Information Sharing [2007] confirms that InfraGard is a key US national security programme. The goal of InfraGard is *'to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes'* [InfraGard, 1996-2008]. Its objectives include:

- increasing the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs;
- increasing interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies;
- providing members with value-added threat advisories, alerts, and warnings;
- promoting effective liaison with local, state and federal agencies;
- providing members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential

crimes and attacks on the nation and US interests *[ibidem]*.

According to Wikipedia [2004-'08] since 2003, InfraGard Alliances and the FBI claimed 'to have developed a Trust-based PPP to ensure reliability and integrity of information exchanged about various terrorism, intelligence, criminal, and security matters. (InfraGard) supports FBI priorities in the areas of counterterrorism, foreign counterintelligence, and cybercrime'.

Early in 2008, the journal The Progressive started a campaign against InfraGard claiming that it would surrogate state powers in the event of martial law. Both the FBI and members of the InfraGard alliances have responded that this is untrue, and that InfraGard have no law enforcement powers of any kind. The Progressive echoed and revived the concerns expressed earlier in 2004 by the ACLU, the American Civil Liberties Union [ACLU 2004].

The main objective of the ACLU Report [2004] is to show that 'information-age technology, anaemic privacy laws and soaring profits have all combined to endanger privacy rights to a point never before seen in [the US] history'. The Report comments about the many public private surveillance endeavours created after 9/11, arguing that they might create a 'surveillance-industrial complex' endangering civil liberties in the US: 'there is a long and unfortunate history of cooperation between government security agencies and powerful corporations to deprive individuals of their privacy and other civil liberties'. The Report quotes and comments many such programmes in the US, orchestrated by different US administrations, e.g. Specifically about InfraGard, the ACLU report argues that it may 'turn private-sector corporations – some of which maybe in a position to observe the activities of millions of individual customers – into surrogate eyes and ears for the FBI'.

The Progressive and formerly the ACLU Report also somewhat connect InfraGard to Operation TIPS - Terrorism Information and Prevention System, an operation designed by President George W. Bush to have United States citizens report suspicious activity. Under Operation TIPS, transportation workers, utility crews and letter carriers could sign up to snoop on members of their communities [Wikipedia Operation TIPS 2002-08]. Operation TIPS came under intense scrutiny in July of 2002, when the Washington Post alleged in an editorial that the program was vaguely defined. Operation TIPS was accused of doing an 'end run' around the United States Constitution, and the original wording of the website was subsequently changed. President Bush's former Attorney General, John Ashcroft denied that private residences would be surveyed by private citizens operating as government spies. Mr. Ashcroft nonetheless defended the program, equivocating on whether the reports by citizens on fellow citizens would be maintained in government databases. While saying that the information would not be in a central database as part of Operation TIPS, he maintained that the information would still be kept in databases by various law enforcement agencies [ibidem].

The databases were an explicit concern of various civil liberties groups (on both the left and the right) who felt that such databases could include false information about citizens with no way for those citizens to know that such information was compiled about them, nor any way for them to correct the information, nor any way for them to confront their accusers [*ibidem*].

5 Conclusions

Without any supporting conceptual work, the term Public Private Partnership has been frequently advocated since the late nineties as a suitable way to cope with sensitive information sharing and other public-private interactions in the security area. PPP seems to be used as a label, attached to many different kinds of activities among public and private actors.

Many governments postulate partnerships as an appropriate arrangement to overcome the gap in control and information deriving from the privatisation of infrastructures. This appears as preferable to other incentives (e.g. economic), because it allows to retain a certain degree of control. Private stakeholders also deem partnerships preferable to direct regulation [Andersson and Malm, 2006]. It remains to be seen whether the partnerships proposed by governments and expected by private actors coincide, and whether these partnerships will be compatible with the current legal framework for PPPs.

Mostly based on a compilation of public sources, this report has presented an overview of some proposed partnerships and applications of the PPP term in the security area, and has tried to point out the key issues that characteristically such applications involve. In substance, they regard the considerable, long effort and the strong commitment needed to agree upon a common vocabulary and a set of commonly agreed rules among the interested community, and to gain the trust of individual participants so as to achieve critical mass. This effort is event stronger when partnerships are to be set up on an international scene. However, when such an initial effort was sustained – as it happened early in the US, under pressure of exceptional events, by force of the continued commitment of the government under two subsequent administrations and of its federal security agencies, a different type of concerns of a more fundamental nature was raised: whether involvement of private contractors in security matters may violate basic civil rights and in the end lead to an illiberal society.

Quite notably, all this debate is quite far away from the main issues that PPP applications raised in other areas. These are mostly of an economic nature and pertain to estimating the risks of setting up a Public Private Partnership, selecting appropriate arrangements, and negotiating contracts in such a way as to protect the public interest and preserve open market access and competition. When fundamental values are put at risk by PPP arrangements, they rather pertain to the sphere of market freedom and government credibility/reputation, than to the one of the basic civil rights.

In addition, we have noted that this substantial difference may reflect a more basic inconsistency between most public-private arrangements in the security area and the commonly agreed notion of PPP as a *'government service or private business v*enture which is funded and operated through a partnership of government and one or more private sector companies' or 'arrangements in which the private sector supplies infrastructure assets and services traditionally provided by governments' [Wikipedia PPI 2007-08, Primer 2008]. The PPPs we have examined in the security area may indeed be intended to provide a public service in a broad sense (i.e., strengthening infrastructure resilience to potential attacks), but this service is not rigorously specified as it happens with conventional PPPs.

6 References

[ACLU 2004] Jay Stanley, *The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society,* ACLU Report, August 2004, http://www.aclu.org/FilesPDFs/surveillance_report.pdf

[Andersson and Malm, 2006] Jan J. Andersson and Andreas Malm, *Public-Private Partnership and the Challenge of Critical Infrastructure Protection*, the International CIIP Handbook 2006, M. Dunn and V. Mauer (eds.), Center for Security Studies, ETH Zurich, 2006.

[BBC News, 2003] BBC News, *What are Public Private Partnerships?* 12 February, 2003. http://news.bbc.co.uk/1/hi/uk/1518523.stm

[Deloitte, 2007] William D. Eggers and Tom Startup, *Closing the Infrastructure Gap: the Role of Public-Private Partnerships,* Deloitte Development LLC (2007). http://www.deloitte.com/dtt/article/0,1002,cid%253D142684,00.html

[EC 2003] The European Commission, DG Regional Policy, *Guidelines For Successful Public – Private Partnerships,* Brussels, March 2003. http://ec.europa.eu/regional_policy/sources/docgener/guides/pppguide.htm

[EC 2004] The European Commission, *Critical Infrastructure Protection in the fight against terrorism*, Brussels, 20.10.2004, COM(2004) 702 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

[EC 2006] The European Commission, *Communication From the Commission on a European Programme for Critical Infrastructure Protection,* Brussels, 12.12.2006, COM(2006) 786 final http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

[EC 2008] *Commission Interpretative Communication* C(2007)6661 *on the application of Community law on Public Procurement and Concessions to Institutionalised Public-Private Partnerships (IPPP).* Brussels, 05.02.2008. http://ec.europa.eu/internal_market/publicprocurement/ppp_en.htm

[Freedictionary 2008] Farlex, *The Free Dictionary,* http://acronyms.thefreedictionary.com/Traffic+Light+Protocol+(information+sharing+security)

[Hart 2002] Oliver D. Hart, *Incomplete Contracts and Public Ownership: Remarks, and an Application to Public-Private Partnerships"* (July 2002). Available at SSRN: http://ssrn.com/abstract=388760 or DOI: 10.2139/ssrn.388760

[Infragard, 1996-2008] Federal Bureau of Investigation, *Infragard, a Collaboration for Infrastructure Protection,* Cleveland, 1996. http://www.infragard.net/

[NERC Security Guidelines 2003-2008]. The North American Reliability Council, *Library of CIP Documents,* 2003- 2008, http://www.esisac.com/library-guidelines.htm

[NIAC 2004] National Infrastructure Advisory Council, *Final Report and Recommendations of the NIAC study regarding Evaluation and Enhancement of Information Sharing and Analysis.* August

21, 2004, http://www.dhs.gov/xlibrary/assets/niac/NIAC_EEIS_Letter_0804.pdf

[Primer 2008] Francois Michel, *A primer on Public-Private Partnerships,* February 22, 2008. Posted on: \\cs.jrc.it\CS\My Documents\stefaal\critical infrastructures\PPP\PFM blog A primer on Public-Private Partnerships.mht

[The Progressive, 2008] Matthew Rothschild. *The FBI Deputizes Business.* The Progressive, March 2008 issue, http://www.progressive.org/mag_rothschild0308 ‘

[Schleifer 1998] Andrei Schleifer, *State Versus Private Ownership.* NBER Working Paper Series (1998). http://www.nber.org/papers/w6665.

[SCNI 2007-08] Security of Critical Networked Infrastructures, *European SCADA and Control Systems Information Exchange.* http://scni.jrc.it/03-projects/06-E-SCSIE/index

[SearchSecurity 2008] SearchSecurity.com, *What is IT-ISAC?* SearchSecurity is the on-line connection to the Information Security Magazine, http://searchsecurity.techtarget.com

[WARP 2005-08] WARP, *Warning, Advice and Reporting Points,* http://www.warp.gov.uk/index.htm

[White House, 2000] The White House, Office of the Press Secretary, *Strengthening Cyber Security through Public-Private Partnership,* February 15, 2000. clinton4.nara.gov/WH/New/html/20000215.html

[White House, 2003] The White House, *The National Strategy to Secure Cyberspace,* February 2003, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[White House, 2007] The White House, NATIONAL STRATEGY FOR INFORMATION SHARING - Successes and Challenges In Improving Terrorism-Related Information Sharing, October 2007, http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf

[Wikipedia InfraGard 2004-08] Wikipedia, the free encyclopedia, *InfraGard,* 2004-2008. http://en.wikipedia.org/wiki/InfraGard

[Wikipedia Operation TIPS 2002-08] Wikipedia, the free encyclopedia, *Operation TIPS,* 2002-2008, http://en.wikipedia.org/wiki/Operation_TIPS

[Wikipedia PFI 2007-08] Wikipedia, the free encyclopedia, *Private Finance Initiative,* 2007-’08, http://en.wikipedia.org/wiki/Private_Finance_Initiative

[Wikipedia PPP 2007-08] Wikipedia, the free encyclopedia, *Public-private partnership,* 2007-’08, http://en.wikipedia.org/wiki/Public-private_partnership

European Commission

EUR 23824 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Is Public Private Partnership a suitable way to cope with security issues?
Author(s): Alberto Stefanini, Marcelo Masera
Luxembourg: Office for Official Publications of the European Communities
2009 – 28 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-12416-7
doi:10.2788/10855

Abstract

This report tries to investigate whether Public Private Partnership (PPP) is a suitable approach to tackle global security issues, with special reference to sensitive data sharing in the context of critical infrastructures protection. To this aim, it outlines the PPP concept starting from its introduction in the early nineties, and provides a view of the questions that arise in many application areas of PPP. An overview of the current EU guidelines concerning PPP is provided. Concerning security, early and current attempts to apply PPP are summarised, and the open issues involved highlighted.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LB-NA-23824-EN-C

ISBN 978-92-79-12416-7