PROTECTION OF 'CRITICAL INFRASTRUCTURE' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY

May 2008

This report is published under the OECD Secretariat's responsibility and was prepared by Kathryn Gordon (Senior Economist, OECD) and Maeve Dion (George Mason University Law School) in support of discussions at the OECD freedom of investment roundtables.

Investment Division, Directorate for Financial and Enterprise Affairs
Organisation for Economic Co-operation and Development
2 rue André-Pascal, Paris 75116, France
www.oecd.org/daf/investment/statistics

Executive summary

Critical infrastructure has received special attention in recent changes to national investment policies in some countries. This paper reviews the role of investment policies in broader national strategies for protecting critical infrastructure. The key findings are:

- Many countries have national plans or strategies for protecting critical infrastructure. These strategies generally define 'critical infrastructure" as physical or intangible assets whose destruction or disruption would seriously undermine public safety, social order and the fulfilment of key government responsibilities. Such damage would generally be catastrophic and far-reaching. Sources of critical infrastructure risk could be natural (e.g. earthquakes or floods) or man-made (e.g. terrorism, sabotage).

- The national strategies studied generally adopt a risk management approach to critical infrastructure protection. This approach helps governments to identify key security assets, assess risks and establish strategies and priorities for mitigating these risks. Generally, the risk management strategy involves measures to be taken in the following areas: prevention, preparedness, response and recovery. The plans seek to improve coordination among relevant agencies and with private sector operators of critical infrastructure facilities in order to manage risks associated with critical infrastructure.

- Information provided by notifications made under the OECD National Treatment Instrument shows that all adhering countries have one or more investment measures that address infrastructure. These are of three types: 1) blanket restrictions; 2) sectoral licensing or contracting; 3) trans-sectoral measures such as investment review procedures. For some countries, these discriminatory investment policies are extremely limited in scope (e.g. they concern *cabotage* or investments in vessels flying the national flag), whereas for others the sectoral coverage of restrictive policies is broad.

- The critical infrastructure policies reviewed here attempt to coordinate the role of private operators of such infrastructure - be they domestic or foreign - in broader national efforts to protect critical infrastructure. However, the role assigned to investment policies in critical infrastructure protection varies. Many countries perceive the value added by investment policy measures, relative to other policies (e.g. defense, law enforcement, sectoral), as negligible and accordingly assign little or no role to investment policy. Others note that, while their critical infrastructure protection policy adopts a broad approach to risk, investment policy is used to address only a narrow range of these risks - those related to national security - and only as a measure of last resort, i.e. only if other, less restrictive and non-discriminatory, measures cannot adequately mitigate the identified risks.

I. Introduction

Since early 2006, the Freedom of Investment (FOI) project has provided a forum for discussing how governments can reconcile their duty to safeguard the essential security interests of their people with the need to protect and expand an open international investment system. The project includes in-depth policy discussions of selected national security topics. Recent policy changes in OECD and non-member countries show that critical infrastructure has gained prominence as a concern for essential security interests. Drawing on notifications made under OECD investment instruments and on other publicly available information, this note presents a factual survey of governments' general strategies for protecting critical infrastructure and of the role that investment policy plays in these strategies.

This note contains the following sections:

- Section II. Definitions of Critical Infrastructure
- Section III. General policy frameworks for the protection of critical infrastructure
- Section IV. Review of foreign investment policies in infrastructure sectors
- Section V. The contribution of investment policy to critical infrastructure protection

II. Definitions of Critical Infrastructure

This section reviews definitions used by governments in the context of national or regional infrastructure protection programmes. Table 1 shows the definitions of critical infrastructure used in 6 published critical infrastructure protection plans or strategies. This review of definitions considers separately the two words - "critical" and "infrastructure" - and then looks at the sectoral coverage of critical infrastructure protection programmes:

- *Critical*: In most countries' definitions, the word "critical" refers to infrastructure that provides an essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities. For example, Canada's definition of criticality involves "serious impact on the health, safety, security, or economic well-being of Canadians or the effective functioning of governments in Canada." Germany refers to "significant disruptions to public order or other dramatic consequences." The Netherlands' critical infrastructure policy refers to infrastructure whose disruption would cause "major social disturbance", "tremendous loss of life" and "economic damage". Thus, the word "critical" refers to infrastructure which, if disabled or destroyed, would result in catastrophic and far-reaching damage.
- *Infrastructure:* The definitions of "infrastructure" used in official descriptions of critical infrastructure tend to be broad. All 6 governments in Table 1 refer to physical infrastructure. Most also include intangible assets and/or to production or communications networks. Australia, for example, refers to "physical facilities, supply chains, information technologies, and communications networks." Canada refers to "physical and information technology facilities, networks, services and assets". The United Kingdom refers to "assets, services and systems".
- *Sectoral coverage:* Table 2 shows a sample of the sectoral lists identified as being of concern for critical infrastructure protection in six national programmes and by the European Commission. These lists show that most governments adopt a broad sectoral perspective on critical infrastructure – they include sectors that account for substantial portions of national income and

employment[1]. Their lists cover what might be considered "traditional" infrastructure sectors, such as transport and telecommunications, but also sectors that would not normally be considered as infrastructure sectors (food, health, government and finance).

Table 1. National Definitions of Critical Infrastructure

Australia	"Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."
Canada	"Canada's critical infrastructure consists 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 Canadians or the effective functioning of governments in Canada."
Germany	"Critical infrastructures are organisations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences."
Netherlands	"Critical infrastructure refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage… "
United Kingdom	"The [Critical National Infrastructure] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: 1) cause large-scale loss of life; 2) have a serious impact on the national economy; 3) have other grave social consequences for the community; or 3) be of immediate concern to the national government."
United States	The general definition of critical infrastructure in the overall US critical infrastructure plan is: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." For investment policy purposes, this definition is narrower: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security."

Sources:
Australia: "What is critical infrastructure?" Australian National Security accessed May 2007. (www.ag.gov.au/agd).

Canada: About Critical Infrastructure, Public Safety Canada accessed January 2008 (www.ps-sp.gc.ca).
Germany: Critical Infrastructure Protection in Germany. Federal Office for Information Security (www.bsi.de/english/topics/kritis/KRITIS_in_Germany.pdf).

Netherlands Report on Critical Infrastructure protection; Ministry of the Interior September 2005.
United Kingdom Home Office Security. Counter Terrorism Strategy: Protecting the Critical National Infrastructure (www.security.homeoffice.gov.uk).
United States: Department of Homeland "National Infrastructure Protection Plan" (2006) (www.dhs.gov).

[1] Edward Graham and David Marchick estimate that the sectors covered under the US definition of critical infrastructure employ almost 25 per cent of the US non-agricultural workforce.

Table 2: Sectoral Coverage of Critical Infrastructure Plans

Sector	Australia	Canada	Netherlands	UK	US	EU
Energy (including nuclear)	x	x	x	x	x	x
ICT	x	x	x	x	x	x
Finance	x	x	x	x	x	x
Health care	x	x	x	x	x	x
Food	x	x	x	x	x	x
Water	x	x	x	x	x	x
Transport	x	x	x	x	x	x
Safety	Emergency services	x	x	Emergency services	Emergency services	x
Government		x	x	x	x	x
Chemicals		x	x		x	x
Defence industrial base	x	x	x		x	
Other sectors or activities	Public gatherings, national icons		Legal/ judicial		Dams, commercial facilities, national monuments	Space and research facilities

Sources: Australia: "What is critical infrastructure?" Australian National Security (www.ag.gov.au/agd). Canada: About Critical Infrastructure, Public Safety Canada (www.ps-sp.gc.ca); Netherlands: Report on Critical Infrastructure protection; Ministry of the Interior 16/9/05; UK: Counter-terrorism strategy (www.security.homeoffice.gov.uk); United States: Department of Homeland "Security Sector Specific Plans" (www.dhs.gov); Commission of the European Communities Green paper on a European Programmes for Critical Infrastructure Protection COM(2005)576.

In summary, this section shows that, in the context of national strategies for critical infrastructure protection, definitions of critical infrastructure tend to be broad. The definitions of "critical" refer to infrastructure whose disruption or destruction would cause catastrophic and far-reaching damage. "Infrastructure" refers to physical and intangible assets and to production systems and networks. The sectoral coverage of the programmes tends to be very wide.

III. General policy frameworks for the protection of critical infrastructure

All of the government programmes studied adopt a risk management approach to critical infrastructure protection. Risk management helps governments to identify key security assets, assess risks and establishes strategies and priorities for mitigating these risks. Generally, the risk management strategy involves measures to be taken in the following areas: prevention, preparedness, response and recovery arrangements. Private operators of critical infrastructure facilities will generally play an important role in all of these activities. The governments whose critical infrastructure strategies were studied tend to take an "all hazards approach": that is, they consider threats to critical infrastructure that originate from natural disasters, from accidents or deliberate attacks. However, while governments have plans, it will be shown below that the role of discriminatory investment policy is always relatively narrow – that is, it is either non-existent or addressed to a much narrower range of risks than those covered by the overall infrastructure protection strategy.

Inter-dependence is a major challenge for risk management in critical infrastructure. This is because economies and societies rely on interdependent and inter-connected infrastructure systems. This gives rise *inter alia* to a phenomenon known as "cascading events" – that is, once one disruption occurs, others are

likely to follow within systems and processes that are connected to the infrastructure affected by the initial disruption. The Canadian government describes one such episode:

> *... during the 1998 Ice Storm, large segments of rural and urban communities were in the dark and without heat. Traffic and street lights were out. Banking and government services were interrupted. The disruption in one sector – electricity affected a score of others, interrupting the delivery of important services upon which Canadians depend* [2]

Because of the "all hazards" approach to risk management and the inter-dependence of infrastructure systems, critical infrastructure protection necessarily involves diverse actors. These include many different government agencies from different levels of government, as well as international organisations. Private operators of critical infrastructure facilities are also important participants in all phases of critical infrastructure protection. It also requires a range of expertise. The Australian critical infrastructure website notes that its process for CI protection brings together specialists from diverse fields of expertise[3]:

- law enforcement and crime prevention
- counter terrorism
- national security and defense
- emergency management, including the dissemination of information
- business continuity planning
- protective security (physical, personnel and procedural)
- e-security
- natural disaster planning and preparedness
- professional networking, and
- market regulation, planning and infrastructure development.

In summary, this section shows that general policy frameworks for critical infrastructure protection tend to:

1. take a comprehensive approach to risk - that is, the programmes cover major threats to infrastructure regardless of source (natural disasters or attacks, sabotage, vandalism, etc.);

2. involve coordination among a diverse range of actors (public and private, different levels of government and different sectoral responsibilities, diverse expertise).

After reviewing discriminatory investment measures that apply to infrastructure (Section IV), Section V looks at possible contributions of investment policy to this more general policy framework.

---

2 Quoted from Public Safety Canada website; section entitled "About critical infrastructure". February 2008.

3 See also the US National Infrastructure Protection Plan (www.dhs.gov/nipp) for another comprehensive list of public and private actors whose actions are to be coordinated under the national plan.

IV. Review of foreign investment policies in infrastructure sectors

This section describes discriminatory investment policies that are applied to infrastructure. It also provides background information relevant for consideration of the "value added" that such policies might have in broader strategies for protecting critical infrastructure.

As a first observation, based on notifications made by countries adhering to the OECD National Treatment Instrument, infrastructure appears to be the focus of an extensive array of discriminatory investment policies. The Annex Table shows that all 39 countries covered in published compilations of discriminatory investment measures report that they discriminate against foreign investors in one or more critical infrastructure sectors. Transport is the most targeted sector - all 39 countries report having discriminatory measures in this sector. In many cases, these discriminatory investment policies are minor (e.g. limited to *cabotage* and investments in vessels flying the national flag). Twenty-nine have discriminatory policies in Post and Telecommunications; 28 in energy; 25 in Radio and Television; 22 in agriculture/food and in defence; 18 in drinking water and treatment systems; and 17 in banking and finance.

These infrastructure-related discriminatory investment policies take several forms:

- *Blanket restrictions*. Many blanket restrictions affect infrastructure. In some cases, this takes the form of an absolute ban. For example, nearly all countries have bans on cabotage. In Switzerland, air transport of people and goods is reserved for Swiss companies. In other cases, the ban only applies to entities that exceed an ownership or control threshold. For example, in Korea, radio and television broadcasting is wholly closed to foreign investors, although cable and satellite broadcasting is allowed when the foreign investor's control ratio is 33 per cent or less.

- *Sector-specific licensing provisions*. Twenty-five measures[4] involve licensing or contractual procedures - usually under the authority of sector-specific government agencies - that discriminate against foreign nationals. For example, the US Federal Communications Commission may require mitigation of national security threats when a foreign entity applies for a license.

- *Trans-sectoral measures including investment approval procedures*. A number of countries operate trans-sectoral measures that can apply to infrastructure investments. According to an earlier report [DAF/INV/WD(2006)13/REV1], 11 countries operate trans-sectoral investment approval procedures that could be used to block infrastructure investments that are deemed to pose threats to essential security interests.

This section has shown that infrastructure is an important focus for discriminatory investment policies and that countries use a variety of discriminatory measures (blanket restrictions, sector specific licensing or contracting, trans-sectoral measures) to influence foreign investors' access to these sectors. For some countries, these discriminatory investment policies are minor (e.g. limited to *cabotage* and investments in vessels flying the national flag), whereas for others the sectoral coverage of these policies is broad.

[4] Measures reported under the National Treatment Instrument.

V. The contribution of investment policy to critical infrastructure protection

This section explores the "value added" of investment policy relative to the more general policies for protecting critical infrastructure. As shown in the preceding section all governments have, to varying degrees, discriminatory investment policies that focus on critical infrastructure. However, in the survey conducted for this paper, no policy evaluations were found that shed light on investment policy's net contribution to protecting critical infrastructure, relative to the broader policy framework described in Section III. The detailed national and regional policy papers on critical infrastructure discuss at length the roles of various government agencies, but they assign varying roles to investment policy. The Netherland's plan does not mention discriminatory investment policy at all.[5] The United States' plan mentions its investment review body (CFIUS) as part of a broader policy involving dozens of federal and state government bodies.[6] Thus, the Netherlands strategy indicates that it cannot be taken for granted that discriminatory investment policy has a role to play in critical infrastructure protection. Furthermore, if investment policy does have a role (as in the United States), it assumes this role as part of a coordinated government effort involving many different agencies.

Two broad sources of "value added" for investment policy in enhancing protection of critical infrastructure may be identified. First, investment policy can serve as a policy of last resort – if all other mechanisms fail, investment policy can be used to prevent investments by foreign entities that are deemed to pose risks. For example, both Israel and the United Sates may directly prohibit a specific foreign acquisition only if other laws are not sufficient to mitigate perceived security risks.

Second, investment policy can be used to address or to assist other agencies in identifying and dealing with security threats that might be posed by international investors. The following is an adaptation of a list of security threats[7] that might be mitigated through discriminatory investment policy (although some countries, report that their list of threats would also be used to analyse the suitability of national investors as operators of critical infrastructure[8]):

- Shutting down or sabotaging a critical facility;
- Impeding law enforcement (e.g. carrying risk of facilitating law-breaking by organised crime or by terrorist organisations) or national security investigations.
- Accessing sensitive data or becoming aware of investigations by national intelligence or law enforcement agencies, including moving data or records offshore;
- Limiting government access to information;

---

5 See the Netherlands Ministry of Interior and Kingdom Relations' *Report on Critical Infrastructure Protection* 16 September 2005.

6 See the US Department of Homeland Security's *National Infrastructure Protection Plan* (2006) see: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

7 Part of the list is adapted from Edward Graham and David Marchick. (2006) *US National Security and Foreign Direct Investment*, May. Institute for International Economics. Page 54. Other items come from written contributions by individual countries to the 'Freedom of Investment" discussions.

8 See, for example, Italy's description of the circumstances that allow the special powers established in the "golden share" clause of its legislation of privatisation of state-owned enterprises. It notes that the arrangements apply to "both national and foreign investors."

- Denying critical technology or key products that are important for essential security instruments to the government or moving them offshore;

- Unlawfully transferring technology abroad that is subject to export control laws;

- Undermining technological leadership in sectors important for safeguarding essential security interests;

- Compromising the security of public or private networks with grave risks to public safety and public order;

- Facilitating espionage or aiding the military or intelligence capabilities of a foreign country.

What is clear from looking at this list of potential threats is that the evaluation of the threats posed by a proposed investment is case-specific. It depends on a number of factors. First, the exact nature of the investment may affect perceived threats and vulnerabilities – an investment in nuclear power is not the same as an investment in solar power. Second, the nature and the nationality of the foreign investor may influence the risk assessment. For example, different home countries have different political relations with potential host countries; government-controlled investors, may, by their very nature, pose different risks than private investors. Third, in some cases, it might be quite easy to mitigate risks through contractual arrangements, while in others this might not be easy. It may be possible to determine simple rules for government policies in some cases (e.g. some countries impose blanket bans on foreign investments in nuclear power). Generally, though, risks posed by particular investments are very much linked to the specifics circumstances of those investments (home country, host country, business activity, physical location, etc.). Fourth, not all countries may have the national security and intelligence capabilities to be able to carry out in-depth evaluations of potential national security threats specifically posed by foreign investors. Moreover, some countries may not wish to spend the money needed to develop such capabilities.

In summary, this section notes that it cannot be taken for granted that investment policy can make major contributions to critical infrastructure protection. It can serve as a barrier of last resort or it may enhance the ability to mitigate risks related to the specifically international dimension of perceived threats. The evaluation of risks is often case-specific and it may not be easy to establish simple rules for the evaluation of those risks. However, not all countries have the national security and foreign intelligence capabilities that are needed to make case-by-case evaluations of foreign investments in infrastructure.

Annex Table. National Treatment Exceptions and Transparency Measures

	Trans-sectoral	Banking & Finance	Energy	Defence	Transport	Drinking Water, Treatment Systems	Agriculture & Food	Post & Telecom	Radio & Tele-vision	Health	Chemicals Petroleum
Argentina			T	T	NTI	T			NTI		
Australia	NTI			T	NTI	T	NTI	NTI	NTI		
Austria	NTI		T	T	NTI		NTI	T	T		
Belgium		NTI	T		NTI			T			
Brazil		NTI			NTI		NTI	NTI	NTI	NTI	
Canada	NTI	NTI	NTI		NTI		NTI	NTI	NTI	T	
Chile	NTI		T	T	NTI		NTI		NTI		T
Czech Republic					NTI						
Denmark			T	T	NTI			T	T		
Estonia		NTI	T		NTI	T		T			
Finland	T			T	NTI						
France	NTI		T	T	NTI	T		T	NTI		
Germany				T	NTI		NTI	T			
Greece		T	T		NTI		NTI		NTI		
Hungary			T		NTI	T		T			
Iceland	NTI	NTI	NTI		NTI		NTI	NTI			
Ireland			T		NTI	T	NTI	T			
Israel	T		NTI	T	NTI	T		NTI	NTI		
Italy			T		NTI	T	NTI	T	T		
Japan			NTI	T	NTI		NTI	NTI	T	T	
Korea	NTI	NTI	NTI		NTI		NTI	NTI	NTI		
Latvia	NTI	NTI	T	T	NTI		NTI	T			
Lithuania					NTI		NTI		NTI	NTI	
Luxembourg			T		NTI	T		T	T		
Mexico	NTI	NTI	NTI	T	NTI	T	NTI	NTI	NTI		T
Netherlands		NTI	T		NTI	T		T	T		
New Zealand	NTI				NTI		NTI	NTI	NTI		
Norway			T	T	NTI	T	NTI	T		T	
Poland					NTI				NTI		
Portugal		NTI		T	NTI	T		T			T

Romania				T	NTI	T					T
Slovak Republic					NTI						
Slovenia			T	T	NTI	T		T			
Spain	NTI	NTI	T	T	NTI			T	NTI		T
Sweden		NTI	T	T	NTI		NTI	T	T	T	
Switzerland	NTI	NTI	NTI	T	NTI		T	T	NTI		T
Turkey		NTI	T	T	NTI	T	NTI	T	NTI		T
United Kingdom	T	NTI	T	T	NTI	T	NTI		NTI		
United States	T	NTI	T	T	NTI	T	NTI	NTI	NTI		

NOTES

(1) NTI indicates data taken from “Adhering Country Exceptions To National Treatment For Foreign-Controlled Enterprises” (May 2007).

(2) T indicates data taken from “National Treatment for Foreign-Controlled Enterprises, List of Measures Reported for Transparency” (February 2007).

(3) Many Concessions comments did not include enough information to determine the details of restrictions to foreign bidders. If the country specifically indicated that the concession/permit/license is open to foreign bidders, then it is not included in chart; otherwise, concessions not overtly indicated as open to foreign bidders are included in the chart.

(4) The chart includes territorial divisions (below federal level) even if only one city / territory has the restriction / requirement.

(5) In the two referenced OECD documents, the “Health” category refers to health professions and distribution of pharmaceuticals. No other health sector information (e.g., hospitals) was available.