THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 6 NUMBER 12

JUNE 2008
INTERNATIONAL CIP

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This month, *The CIP Report* once again provides its annual International CIP issue. It is important to not only understand critical infrastructure within the United States, but to also recognize international ideas and methods for ensuring the protection of infrastructure, as well as the population and economy. This year, five different countries and the European Union are featured, and each respective article highlights their current work on critical infrastructure protection.

The first article discusses Israeli policy on critical information infrastructure protection (CIIP) and how the policy was created. A second article describes Australia's resilience planning and the development of emergency plans; importantly, its planning gives strong attention to natural disasters. Another article comes from Sweden and introduces the Swedish Civil Contingencies Agency (MSB), a new agency designed to enhance preparedness and response in its society. An article is presented from Estonia on the new Cooperative Cyber Defence (CCD) Centre of Excellence (COE), established in cooperation with six other nations. A contribution from the United Kingdom provides a summary on its updated system developed to identify and categorize critical infrastructure. Moreover, an article from the European Union offers information on how Member States approach critical infrastructure protection and how the European Council has worked to establish a directive on the identification, designation, and protection of European Critical Infrastructure (ECI).

In addition to the articles from international contributors, an update on the Committee on Foreign Investment in the United States (CFIUS) law and proposed regulations is provided. This month, *Legal Insights* looks at the Visa Waiver Program (VWP) and the establishment of the Electronic System for Travel Authorization (ESTA). Lastly, a press release and update on the July issue of *The CIP Report* are provided.

We hope you enjoy this issue and, as always, appreciate your continued support.

Critical Information Infrastructure Protection Policy in Israel

by Dan Assaf *

Israel's policy towards critical information infrastructure protection ("CIIP") is a very interesting subject matter. Israel is very similar to the United States in some issues that relate to CIIP but at the same time very different in other matters. On the one hand, both countries share a perceived higher threat and risk resulting in increased focus on national security and homeland security. In addition, both are technologically-advanced, and hence heavily rely on information systems for every aspect of their society. The perceived high threat, together with the heavy reliance on information infrastructures, resulted in CIIP being an important component in both countries' national security policies. Nevertheless, these two countries are quite opposite in their choice of regulatory arrangements as part of their CIIP policies. While the United States focuses mainly on the market, or market-based arrangements, to provide an adequate level of CIIP, Israel has adopted a state-centric, interventionist approach, relying on its security apparatuses to reach this objective, and leaving almost no role to the private sector. In the following pages I delineate the main concepts of the Israeli policy, namely the origins of the policy, its legislative/regulatory frameworks and the manner in which privatization of critical infrastructures is dealt with.

Policy Origins and Main Institutions

Circa 2000, the Israeli security community[1] began to work closely on drafting a policy that would address CIIP. The security community has come to understand the threat information operations may pose on critical infrastructures' information and communication systems, and the importance of creating a strategic plan of action to address this threat. The main debate related to the question of responsibility: which organization should have an overall responsibility for CIIP.

The outcome of this cooperative activity, a CIIP plan, was approved by the Israeli Government in December 2002, through the adoption of a special Government Resolution. This Resolution mandated the creation of a Stirring Committee, headed by the head of the National Security Council (NSC) and staffed by representatives from the security apparatuses, as well as from various government ministries. Further, the Resolution assigned the responsibility for CIIP to the General Security Service (GSS), Israel's internal security apparatus, through a designated authority — the National Information Security Authority (NISA).

The Stirring Committee has been created with the goal of consolidating inclusive steps to protect the Israeli critical information infrastructures. The Committee's mandate has been to steer the activity of the various actors involved in CIIP, and especially that of NISA. This Committee meets on a regular basis to discuss the threat to critical information infrastructures, and the principles of security that must be implemented in order to address that threat. One of the main powers accorded to the Committee is its authority to determine, together with NISA, that a company or a sector, whether public or private, is critical, and hence to subject it to the executive power of NISA.

NISA has been in place long before the Resolution, within the Protective Security Division in the GSS. It held the responsibility for information security within the Israeli Government, embassies and government-owned companies. Its new executive powers came with a substantial supplement in professional manpower and a budgetary increase. It should be noted that this responsibility has its limits: The Israeli Defense Force (IDF) and the Mossad are responsible for protecting their own information infrastructures, and Malmab is responsible for protecting the information infrastructures of the Ministry of Defense and the defense industrial base.

(Continued on Page 3)

[1] Consisting of the General Security Service (GSS), the Institute for Intelligence and Special Operations (known as the "Mossad"), the Israeli Defense Force (IDF), the Chief of Security in the Ministry of Defense ("Malmab") and the National Security Council (NSC).

Israel *(Cont. from 2)*

Legislative Framework

Following the Government Resolution and the establishment of both the Stirring Committee and NISA as the institutions governing CIIP, the two bodies engaged in a process to define the critical infrastructures and establish the underpinning legal framework that would allow them to assume their authority.

For this purpose, the Regulation of Security in Public Bodies Law of 1988,[2] which sets out the security requirements for public bodies and institutions, has been amended to reflect the new theme of CIIP, as well as to establish the authority given to NISA.

While the name of the law suggests that the regulated entities are public bodies only, by law various critical infrastructures, both public and private, are subjected to it. This law is characterized by hierarchy and control. It provides NISA with very broad regulatory authority, including the power to determine whether an infrastructure is critical; the power to approve the appointment of an officer in charge of securing the vital information systems within a critical infrastructure; the power to give directions and instructions to that officer regarding required security actions, including control and reporting; and the power to inspect and audit the state of CIIP within that regulated entity. Put simply, this law represents a very centralist and hierarchical approach towards CIIP, one that provides almost no discretion at all to the privately held critical infrastructures.

Privatization and CIIP

One would assume that the difference in conception between Israel and the United States regarding the role of the public and private sectors in CIIP is because the majority of Israeli critical infrastructures are owned and operated by the government. One would hence conclude that the shift Israel is undergoing since the late 1980s from a socialist, centralist economy to liberalization, deregulation and privatization,[3] that includes the privatization of critical infrastructures such as the national electricity corporation, telecommunication service providers and oil refineries, would narrow the gap between the Israeli and American policies.

And yet, realizing the importance of maintaining the government's vital interests in such companies, as well as the challenges private control may have on the ability of NISA to regulate, monitor and enforce CIIP, the Israeli Government endorsed in 2005 an amendment to the Government Companies Law of 1975 (governing the process of privatization in Israel) to include a framework authorizing the government to declare, through ministerial decrees and orders, that the state has vital interests in a privatized company. As in the case of the Regulation of Security in Public Bodies Law, these decrees vest very broad authorities and discretion as to CIIP.

The intensity and centrality of this regulatory authority is quite fascinating. The Government Companies Order (Declaration of Vital Interests of the State of Israel with Respect to the Company "The Oil Refinery – Ashdod Ltd.") of 5765-2005[4] provides an excellent example: It places restrictions on the ability of foreign entities to hold parts of this critical infrastructure; it requires numerous key personnel in the company[5] to be Israeli citizens and to undergo security screening; and it directs the company, the director of computer security and the director of security to "carry out the directives of the Competent Officer"[6] regarding CIIP, "including directives concerning control and reporting."[7] It further requires the company to fulfill a list of requirements designed to monitor access to all vital computerized systems; to supervise and control the operating and maintenance activities; to prevent unauthorized access to the

(Continued on Page 13)

[2] Regulation of Security in Public Bodies Law, 5758-1998, Statute Book of 5758-1998, p. 348, Statute Book of 5765-2005, p. 204.
[3] Jonathan Nitzan and Shimshon Bichler, The Global Political Economy of Israel, (Sterling, VA: Pluto Press, 2002), at 2.
[4] Online at http://www.gca.gov.il/bazan/hebrew/files/InterestsH.pdf [in Hebrew].
[5] Including the majority of directors (including the chairman of the board), general managers and their deputies in the engineering, operations and information systems units, legal counsels, internal auditors, the director of security and the director of computer security.
[6] Defined as the representative of the General Security Service.
[7] Section 12(a).

Resilience Planning for CIP in Australia: Legal Implications

by Dr. Adrian McCullagh *

On May 7, 2008, the Australian Strategic Policy Institute (ASPI) released its risk report on Australia's critical infrastructure, "Taking a Punch: Building a more resilient Australia." The underlying theme of the report is that even though the threat of a terrorist attack on Australia's critical infrastructure must not be underestimated the real threat will most likely come from Mother Nature. This valuable report directs its readers to past major events that have occurred in Australia such as cyclone Tracy which destroyed the city of Darwin, the capital of the Northern Territory, on Christmas Eve in 1974. The authors of the report also discuss the effects of cyclone Larry which devastated North Queensland in the Ingham area in 2006. As noted in the report, if cyclone Larry had, instead of destroying much of Ingham, a fairly small town in North Queensland, hit the city of Cairns then the devastation could have been Australia's version of Hurricane Katrina.

The devastating effect of Hurricane Katrina is a lesson that all can learn from. The hardening of critical infrastructure is obviously one aspect that government can attempt to undertake but this may not necessarily work or be possible for all types of critical infrastructure. For example, it is possible and highly desirable for redundant paths to be deployed for telecommunications infrastructure but the deployment of redundant paths may be cost prohibitive in the transmission or distribution of electricity. It may arise that the best possible ability any government has in better protecting its citizens and its critical infrastructure against the ravages of Mother Nature is to establish an effective early warning system. Obviously such a system does not prevent the event occurring but it can assist in making more resilient the critical infrastructure. Further, an early warning system can better safeguard the residents who could be affected by the potential impending disaster from some of the devastating effects arising from such catastrophes. That is, residents if aware of the impending disaster can take appropriate evasive action to better protect their own assets and themselves from the forthcoming event.

This then results in the ability of governments to provide proper communications of imminent dangers. Clearly, these communications do not prevent the event occurring but they do assist in mitigating the damage that may occur especially to human life. The recipients of such information can implement evasive action to better protect themselves and possibly better protect their property and belongings.

Recently, the Queensland State Government in association with the Brisbane City Council (the Capital of Queensland) jointly developed the "Brisbane CBD Emergency Plan." Similar plans have been or are in the process of being developed by other major centers located within Australia. An early warning system for impending dangers is a substantial aspect of the plan as well as post disaster action. Coordination of post event actions is of primacy with the plan.

It is generally accepted that an early warning system could have greatly reduced the loss of life that resulted from the 2004 tsunami that hit South East Asia. An early warning system if properly implemented could have warned many of the residents located across the affected coast line of the impending danger and given them sufficient time to reach high land and thus avoid the disaster. But early warning systems are just one aspect of the arsenal that a government should employ. Post event mechanisms must also be developed and maintained. These mechanisms must, it is suggested, involve resilience hardening of the infrastructure and the services that support the community.

In order to develop a resilient environment, governments need to also develop appropriate recovery disaster plans which come into effect if a disaster occurs. As stated above, the Queensland State Government in conjunction with the Brisbane City Council recently released its Brisbane CBD Emergency Plan.

(Continued on Page 13)

A New Leader of Societal Security Efforts in Sweden

by Jesper Gronvall *

On January 1, 2009, Sweden will have a new agency, the Swedish Civil Contingencies Agency (MSB). The agency will work to protect basic values such as democracy, the rule of law and individual freedoms and the lives and health of citizens, and to strengthen critical societal functions. The new agency is the result of a merger between the Swedish Emergency Management Agency, the Swedish Rescue Services Agency and the National Board of Psychological Defence.

MSB will be responsible for leading and coordinating all actors in society, working horizontally and vertically to enhance preparedness, bolster response capacity and learn from crises. This responsibility spans from everyday accidents to severe crises that can affect the population's health and property, and as well disrupt critical societal functions. If everyday accidents are not managed well they can escalate into costly crises, affecting the ability for legitimate and effective democratic governance. Critical functions in society can be divided into two groups. The first concerns those functions where a disturbance could cause a severe strain on society. The second group includes functions that must be resilient to be able to manage a severe strain on society. It should be understood that functions are not only technical infrastructure; having trained and prepared leaders and a resilient population are key factors in societal security.

Another organizational development is the creation of a Crisis Management Secretariat in the Prime Minister's Office. In preparation for crises, the Secretariat will lead education and training efforts for the various ministries and provide advice on potential threats and risks to society for top governmental leadership. During crises, its crisis coordination center can be used by the highest levels of government. MSB and the Secretariat are expected to work together, especially during crises to rapidly ensure national situational awareness and understanding.

The organizational reform was largely driven by the lessons learned from the tsunami catastrophe in South-East Asia in 2004, where thousands of Swedes were on vacation. There were 550 citizens of Sweden who lost their lives in the horrific waves. The commission created to probe the management of the crisis called for stronger national level capabilities. The purpose of creating MSB is to solidify a comprehensive approach to societal security.

The Emergence of a Societal Security System

Societal security is the preferred term in Sweden, and increasingly in the European Union, to homeland security in the United States. It better reflects the reality of fluid risks and threats that may easily cross geographic borders. The challenges of the 21st century are less about the integrity of the territory than safeguarding critical functions in society. In essence there is a merger of the domestic and international (security) arenas. The strategic environment is complex and interdependent, as effects and consequences in one country can have their origin far from its territorial border.

The purpose of creating MSB is to solidify a comprehensive approach to societal security.

A fundamental notion is that an all-hazards approach is necessary; it is not possible to know what the crisis of tomorrow may look like. Societies should be as prepared as possible to deal with emerging challenges in whatever shape or form. Although it may be a stretch for the MSB to take on a motto such as "Ad omnia paratus" — Prepared for all things — which for example the European Union's Nordic Battle Group has,

(Continued on Page 6)

Sweden *(Cont. from 5)*

it does have the ambition to create a flexible and resilient system that is prepared to also deal with the unexpected.

During the Cold War the threats to Sweden were clear; they came from the East in the form of the Soviet Union. The key objective of national security was to ensure the survival of the nation by preserving territorial integrity and national sovereignty. Vast resources were allocated to create and sustain a military capacity that could ensure non-alignment in peace and neutrality in a war situation.

The threat of territorial invasion and occupation has faded. There is discussion in Sweden on what threat, if any, that an invigorated Russia poses. One could ask what a perilous operation to send military forces would accomplish, rather than buying a piece of land instead. However, there are ways other than using military tools that a nation can use to impose its will on others. The power of controlling energy valves is one of them. Although the nationalistic territorial domination strategies of the 20th century can return to Europe, governments have an obligation to manage existing challenges. These threats and risks are different in character and demand new strategies for prevention, preparedness, response and recovery than the challenges of the past.

A key characteristic of threats and risks is the ability for direct and indirect consequences to spill-over sectors and governmental levels in a nation, between nations and across continents. A driver of this development is globalization. Rising connectivity between nations and continents brings many positive effects, such as economic growth that is lifting millions of people out of poverty. Most nations are now connected to the global economy where transactions are immediate and transnational. However, challenges also come with globalization. Increased economic activity leads to environmental failures, and the rapid movement of people may enhance the speed and spread of infectious diseases. Cross-border infrastructures and processes may cause unanticipated ripple effects within and between continents. Increased connectivity also enables networks, organized crime cartels or terrorism movements to cause havoc.

Building a Transatlantic Partnership for Shared Preparedness

To be successful in building preparedness it is necessary to create and sustain partnerships, across sectors, across nations and between continents. This is of course an important task for governments, but the responsibility is shared between the public and the private sectors, and the citizens. All actors in society need to understand and accept that it is a joint mission to prepare for the known and the unknown risks and threats of the 21st century.

One critical partnership in the societal security domain is that between Sweden (and the European Union) and the United States. There are profound historical and human ties that bond the United States and the nations of Europe together.

Director General Helena Lindberg of the Swedish Emergency Management Agency will become the first Director General of the Swedish Civil Contingencies Agency (MSB) on the 1st of January 2009.

The transatlantic community shares core values, such as liberty, democracy, respect for human rights and fundamental freedoms and the rule of law. It is also exposed to the same risks and threats, which means that for the future, more joint efforts are needed to continue to provide an open, prosperous, safe and secure environment.

Sweden is one of six countries (the others are Canada, Mexico, the United Kingdom, Australia and Singapore) that currently have a bilateral science and technology agreement with the U.S. Depart-

(Continued on Page 14)

Cooperative Cyber Defence Centre Established by Seven Nations

by Eneken Tikk, Legal Advisor, Cooperative Cyber Defence Centre of Excellence

On May 14, 2008, Estonia and six more nations (Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain) signed the memorandum of understanding (MOU) concerning the establishment, administration and operation of the Cooperative Cyber Defence (CCD) Centre of Excellence (COE).

The overall concept for North Atlantic Treaty Organisation (NATO) COE-s dates back to 2003 when the world's leading military organisation decided to engage nations in enhancing its already existing as well as new capabilities. Centres of excellence are there to support the Alliance in the fields of their founders' best knowledge and expertise.

The Estonian decision to offer NATO the cyber defence centre of excellence was made already in 2004. It took another four years to provide infrastructure, select and hire the core project team, engage nations in the project and finally sign the MOU-s. Today, CCD COE is making preparations for accreditation as a NATO COE.

The background of this decision is related to the fact that Estonia, with its 1.4 million inhabitants, is a profoundly IT-friendly country where development of the information society is one of the main political priorities. As a small country, Estonia has saved lots of resources introducing information systems and electronic services that significantly raise the quality of life of its population. In the past three years, more than 80% of all taxpayers have moved their declaring activities on-line, every fourth new company is founded electronically and a specific data exchange layer is created that makes the information and services of more hundreds of public institutions accessible from one single point of entry.

About 75% of Estonians carry in their pocket a national ID-card which works both as an ID as well as a measure for providing electronic signatures and secure on-line authentication. This has allowed both public and private sectors to take several secure e-services to the market. Early in 2007, Estonia was the first country to try out on-line parliament elections and these days people are trying out the mobile ID solution, making it possible to engage in transactions with the help of a cell phone.

It goes without saying that remarkable information and communication technology (ICT) solutions come with significant threat of vulnerability. The "society of cyber addicts" needs a strong cyber defence doctrine and the Estonian offer to NATO was to work together to share best practices and experience in the field.

The cyber attacks against Estonia in April and May 2007 turned out to be significant supportive events on the way to establishing the Centre. Successful *ad hoc* public-private as well as international cooperation made it possible to cope with extensive distributed denial of service (DDoS) attacks against government and critical infrastructure servers and made cyber threat more clear to the world than ever before.

CCD COE is there to further develop concepts and doctrines in the field of cyber defence, to elaborate methodologies and capabilities to eliminate cyber threats as well as analyse and simulate different threats.

The events speeded up both national and international processes related to cyber defence — early this year NATO adopted two significant documents in the field (Cyber Defence Policy and Cyber Defence Concept), Estonia elaborated a new

(Continued on Page 15)

Defining the "Critical" in UK Critical National Infrastructure

by the Centre for the Protection of National Infrastructure

In 2007, the United Kingdom (UK) Minister for Security and Counter Terrorism conducted a review of the protection of the UK critical national infrastructure (CNI). The review recommended that the system for identifying and categorising critical infrastructure be updated. Work to develop the new "criticality scale" and to map critical infrastructure has involved the Centre for the Protection of National Infrastructure (CPNI) as well as other UK Government departments and infrastructure owners. The approach takes full account of logical assets and information systems as well as physical assets and installations.

CPNI protective security advice is impact driven, vulnerability focused and threat informed

The categorisation of assets within the UK national infrastructure (NI) is taking place across nine sectors: communications, energy, emergency services, finance, food, government, health, transport and water. The results of this work will help determine the programme for reducing the vulnerability of the CNI from national security threats. A clearly defined CNI is important for CPNI advice delivery as this helps to ensure that resources are targeted at the most critical assets. However, it is still important that CPNI provides protective security advice to the whole of the NI as well as other businesses in the UK. Much of this advice can be found at www.cpni.gov.uk.

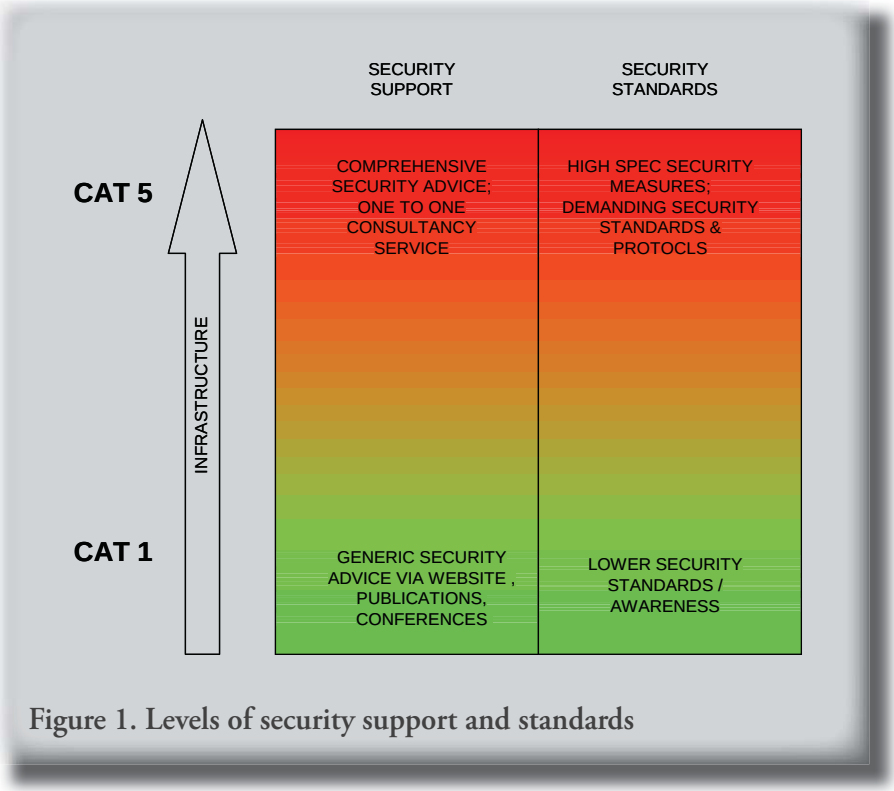

Figure 1. Levels of security support and standards

CPNI advice is integrated across the physical, personnel and information security disciplines

Infrastructure is categorised against levels 0-5 on the criticality scale. The criticality of an infrastructure asset will help determine the appropriate degree of security support it should receive from government and the standard of security that should be in place. The vulnerability of the asset and the degree of threat should also be taken into account.

When categorising an asset, the key factor that is considered is the impact its loss would have on the availability or integrity of our essential services, as well as the potential impact on life or the economy.

When considering the severity of the impact on essential services, three factors have a bearing:

(Continued on Page 17)

Protecting European Critical Infrastructure

by Andrea Rigoni *

Member States of the European Union (EU) are more and more conscious of the importance of protecting the National Infrastructure. Many of them have already a national legislation for the identification and protection of those infrastructures that provide critical services to the nation and its citizens.

At the same time, the European Council is working on a Directive "on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection."[1]

"The Directive raises the level of security for all EU citizens, provides legal clarity to operators and increases competitiveness," declared European Commission Vice-President Jacques Barrot.

The Directive establishes the procedure for the identification and designation of European Critical Infrastructure (ECI) and a common approach to assessment of the need to improve the protection of such infrastructure in order to contribute to the protection of people.

ECI means critical infrastructure located in the EU Member States the disruption or destruction of which would have a significant impact on at least two Member States of the EU. The Directive concentrates on the ***energy and transport sector*** *and will be reviewed after three years, to assess its impact and the need to include other sectors within its scope - inter alia the* ***Information and Communication Technology (ICT) sector****.*

Each designated European Critical Infrastructure is to have an ***Operator Security Plan (OSP)*** *covering inter alia identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures.*

A ***Security Liaison officer*** *will function as the point of contact for security issues between the European Critical Infrastructure owner/operator and the relevant Member State authority.*

Every two years, each Member State will forward to the Commission information on threats and risks encountered in each European Critical Infrastructure sector. On the basis of

(Continued on Page 10)

The identification process for ECI has four main steps:

Step 1: Each Member State shall apply sectoral criteria according to the characteristics of individual energy and transport infrastructure in order to make a first selection of potential "Critical Infrastructure;"

Step 2: Checking if the infrastructure matches the criteria established in the Critical Infrastructure;

Step 3: Establishment of trans-boundary effect of the infrastructure (i.e., affecting two or more Member States); and

Step 4: Application of the following cross-cutting criteria to the infrastructure:

- casualties criterion (assessed in terms of potential number of fatalities or injuries);
- economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services, including potential environmental effects); and
- public effects criterion (assessed in terms of the impact of public confidence, public health and disruption of daily life, including the loss of essential services). Infrastructure that satisfy all the above criteria, will be designated as "European Critical Infrastructure."

[1] Reference 2006/0276, Council of the European Union, April 11, 2008. The latest version of the Directive is available at http://register.consilium.europa.eu/pdf/en/08/st05/st05051-re04.en08.pdf.

EU CIP *(Cont. from 9)*

those reports, the Commission and the Member States will examine whether further protection measures at the EU level should be considered.[2]

On the 5th of June 2008, the European Council reached a political agreement on the Directive, that is expected to enter into force before the end of 2008.

Together with the Directive, the European Commission defined a European Program for Critical Infrastructure Protection (EPCIP), described in last year's international issue of *The CIP Report* (page 6).

While the Directive focuses on ECI, the Program aims to support the leverage of national initiatives at an International level. One area that is of particular interest is *Information Sharing*. Information Sharing is a key concept of modern protection and is the main pillar of Intelligence. There are many initiatives and projects in Europe on Information Sharing, most of them at a National level. Some exceptions are those systems that interconnect operators in a specific sector (i.e., Banks, Air Controls, adjacent Power Transmission Operators, etc.), but are used for daily operations and not for Critical Infrastructure Protection.

Information Sharing has gained popularity after 9/11 and today it is at the centre of many National Security Intelligence Strategies. Many EU Member States have already implemented Information Sharing and Alert Systems, but most of them are targeting end users and citizens, mainly to share alerts on ICT vulnerabilities and threats. According to a European Network and Information Security Agency (ENISA) study, "EISAS - European Information Sharing and Alert System," 13 Member States do not have any known Information Sharing activity, 5 Member States have a dedicated organization and the other 9 have some initiatives managed by non-dedicated organizations. In the study, only two Member States are reported to have organizations in charge of Information Sharing that have Critical Infrastructures in their constituency,[3] but this number does not reflect the reality: many other Member States are running information exchanges facilitated by government organizations, where Critical Infrastructures meet regularly; these initiatives are all very successful and the major key success factor is the importance given to the creation of trust among all participants, including the government.

EU Member States share the need to exchange information on an International level, in particular for the protection of Critical Infrastructures, where many of them are interconnected or interdependent, or the impact of one could affect one in another Member State. This is why the European Commission included the creation of Information Sharing Systems in this year's Critical Infrastructure Program.

An important aspect that should be always considered when talking about International Information Sharing Systems is that most of the times these services are used by governments and National Infrastructures to exchange notifications and communications about new vulnerabilities, threats, incidents and good practices and in most cases this exchange assumes a relevance in respect to National Security.

This is one of the main reasons why most Member States are promoting a federated approach, both at a National and European level. The most successful projects in Europe, such as the UK WARP (Warning, Advice and Reporting Point), owe their success to this approach that, among the other things, can address the specific requirements of certain sectors.

The Energy Sector, for example, is considered among the most critical ones in Europe: in particular, Transmission System Operators (TSOs) run the European Power Grid that provides electricity to all European citizens. TSOs form a strong and well-connected community. Information Sharing is vital to these companies: a problem, fault, incident or attack to one operator could have disastrous impacts on the other operators; that is why building a "Shared Situational Awareness" improves the overall resilience of the

(Continued on Page 15)

[2] "Critical Infrastructure Protection," European Commission, Press Release IP/08/899, June 6, 2008, emphasis added to original.
[3] See, *EISAS – European Information Sharing and Alert System: A Feasibility Study 2006-2007*, European Network and Information Security Agency, January 1, 2008, available at http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf.

Foreign Direct Investment in Critical Infrastructure: An Update on the New CFIUS Law & Proposed Regulations

by Maeve Dion, JD, Legal Research Associate

The *Foreign Investment and National Security Act of 2007* ("FINSA") came into effect on October 24, 2007. As required by FINSA, in April of this year the Department of the Treasury issued new proposed regulations regarding the processes and authorities of the Committee on Foreign Investment in the United States ("CFIUS").

Foreign Investment and National Security Act of 2007 ("FINSA"), Pub. L. No. 110-49, 121 Stat. 246.

Proposed Regulations and Public Comments (closed June 9, 2008).

For those unfamiliar with the history and role of CFIUS, a background article can be found in the January issue of *The CIP Report*, and other CFIUS articles are on our website. In short, CFIUS is an interagency committee that reviews and investigates foreign mergers, acquisitions, and takeovers that may pose a threat to national security.

The term "national security" has never been defined in this context, allowing CFIUS the flexibility to adapt its analyses to the changing threat environment. While the term is still undefined by CFIUS, Congress used FINSA to clarify that "national security" must include issues of homeland security and related critical infrastructure concerns.

FINSA adopted the standard federal definition of "critical infrastructure" (first defined in the USA PATRIOT Act), and the proposed regulations do not further refine this definition. Thus, determining if a transaction involves "critical infrastructure" necessitates (1) assessing the systems and assets (physical and virtual) involved in the transaction, and (2) deciding if the incapacity or destruction of those assets would have a debilitating impact on national security.

Given that both "national security" and "critical infrastructure" are necessarily broad in definition, Congress wanted to provide more detailed guidance that could be helpful to companies whose transactions might fall under CFIUS authority. FINSA therefore required that not only new regulations be promulgated by the end of April 2008, but that there also be issued specific guidance on the kinds of transactions that implicate national security risks and involve critical infrastructure.

Unfortunately, as of the writing of this article, that guidance has not yet been released. Upon issuance of the new guidance, we will provide a timely update in a subsequent issue of *The CIP Report*. Also, the CIP Program is currently developing an in-depth article on the history and impact of CFIUS, and we will notify our readership when it is published. ❖

Legal Insights

Effective Electronic System for Travel Authorization Key to New Visa Waiver Security Rules

by Timothy P. Clancy, JD, Principal Research Associate for Law

The Visa Waiver Program (VWP) allows nationals from participating countries[1] to travel temporarily to the United States without a visa. The VWP was established in the 1980s to promote tourism and commerce and improve relations between the United States and participating nations. Nathan Sales, Professor of Law at the George Mason School of Law and a former top policy official at DHS, observed recently that the VWP's security standards are not up to the job post-9/11, as the Program originally sought to prevent unauthorized economic migration, not thwart transnational terrorism.[2] This has left the Program in a precarious position politically, particularly with the prospect of radicals entering the United States from VWP countries such as the United Kingdom.[3]

However, the Bush Administration has seen the VWP as an important tool to enhance security while at the same time improving economic and diplomatic ties abroad. It has sought to strengthen and modernize the VWP security requirements and concurrently expand VWP participation to reward countries such as the Czech Republic, Estonia, Lithuania and South Korea for their active cooperation in combating transnational terrorism. According to Professor Sales, the rules had treated these nations as "second-class citizens" under the VWP since the percentage of a country's immigration overstays in the United States must be very low (3%) to allow participation, even if a country has strong security standards and shares information with the United States on terrorism threats.

On June 2, 2008, Homeland Security Secretary Michael Chertoff announced the establishment of the Electronic System for Travel Authorization (ESTA) for the VWP, as directed by Congress last year.[4] The ESTA was one of the requirements set by Congress to tighten VWP security procedures and to expand VWP participation.[5] This new system will alter significantly the entry procedure for just over half of all foreign visitors to the United States.[6] The new system will be available on a voluntary basis starting on August 1, 2008 with a goal of being mandatory by January 2009.

Currently visitors under the VWP fill out a paper form (known as an I-94W) en-route with personal information — travel plans, basic

(Continued on Page 14)

---

[1] Countries currently participating in the VWP: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, The Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland and the United Kingdom. See, "Overview of the Visa Waiver Program (VWP)," Customs and Border Protection, DHS, December 4, 2007, http://www.customs.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/vwp.xml.

[2] "Members Only: We must waive securely," Nathan A. Sales, *National Review*, February 27, 2008, http://article.nationalreview.com/?q=YjU1ZTUwZWZlM2UwMDMwODNhYTRhZjc0NjM3Y2FkMDE.

[3] "U.S. Seeks Closing of Visa Loophole for Britons," Jane Perlez, *The New York Times*, May 2, 2007, http://www.nytimes.com/2007/05/02/world/europe/02britain.html.

[4] See, Secure Travel and Counterterrorism Partnership Act of 2007, passed as part of the Implementing Recommendations of the 9/11 Commission Act of 2007, Section 711 of P.L. 110-53, August 3, 2007.

[5] The Act gives the Secretary of DHS, in consultation with the Secretary of State, the authority to waive the nonimmigrant refusal rate requirement for admission to the VWP, if the Secretary certifies to Congress that the ESTA is operational prior to being able to waive the nonimmigrant refusal rate requirement. The Act also requires the Secretary of DHS to certify to Congress that an air exit system is in place that can verify the departure of not less than 97% of foreign nationals that exit through U.S. airports. For a summary of the VWP see, *Visa Waiver Program*, CRS Report for Congress, RL32221, Updated January 31, 2008, http://italy.usembassy.gov/pdf/other/RL32221.pdf.

[6] In FY 2006, 15.3 million visitors entered the United States under the VWP, constituting 51% of all overseas visitors, according to the Congressional Research Service. See, CRS, RL3221, January 31, 2008.

Israel *(Cont. from 3)*

systems; and to identify attempts at unauthorized access.[8] All these measures and their procedures are pursuant to the directives of NISA, and the company is required to provide NISA access, at any time, to any system or site of the company.[9]

This example shows how authoritative and interventionist is the regulatory policy in Israel and one can say that the privatization process in critical infrastructures excludes the element of information security, and leaves it, *de facto*, nationalized.

Conclusion

To sum up, Israel has taken a state-centric, interventionist approach towards CIIP. Its policy emphasizes law and hierarchical control as its cornerstones. Thus far, the privatization of certain critical infrastructures has not resulted in a move towards a more liberal policy that would see the private sector as a collaborator rather than a subordinated entity. Rather, it stressed how the state regards its role in CIIP — proactive and dominant rather than as a facilitator and enabler. Notwithstanding this, it is still unclear how successful NISA is in enforcing its authority over Israel's critical infrastructures and whether the costs affiliated with such policy are justified. ❖

* Dan Assaf is a doctoral candidate at the Faculty of Law, University of Toronto. Dan Assaf's research focuses on the regulatory and governance mechanisms used to address the problem of critical information infrastructure protection. His research interests lie in the intersection of law, economics and security, with emphasis on homeland security and information security. He received his LL.B. and B.A. (economics) in 2003, both from Tel Aviv University. He can be reached at dan.assaf@utoronto.ca.

[8] Section 12(b).
[9] Section 12(c).

Australia *(Cont. from 4)*

As noted in the ASPI report, "Sustaining a prosperous nation rests on ensuring that Australia can withstand the impact from a range of hazards, both deliberate and natural." Resilience involves how an individual, organisation or society can adapt to a changed environment. For example, it involves organisation operations both independently as well as interdependently in times of disaster. It must be understood that no organisation operates in isolation. Commercial entities are dependent upon supply chains and as such when a disaster occurs organisations need to assist each other in ensuring that as a combined whole within the commercial environment they can continue to operate as a complete commercial structure.

The fundamental aspect of the recovery disaster plan is the establishment of a chain of command so that there is but one line of communications and especially important one line of command control. The Brisbane CBD Emergency Plan is under the control of the Queensland police department, with the Commissioner of Police undertaking the head of the communication and action control. It really does not matter who is in control, but as is very much identified in the Brisbane CBD Emergency Plan someone with authority must take control and supervise the post disaster actions.

The effect of a state of emergency is that certain laws may need to be suspended or curtailed so that rapid recovery can be achieved. The Brisbane CBD Emergency Plan does not at present deal with how and in what circumstances laws should be suspended pending recovery. From a research perspective, very little has been undertaken in investigating what laws should be suspended other than providing some form of marshal law to prevent looting or other reprehensible activities. This is really the next stage in building a resilient environment as it should be possible to predetermine under what circumstances laws need to be suspended and when they should be reinstated. ❖

* Dr. Adrian McCullagh is an Adjunct Professor at the Information Security Institute, Queensland University of Technology, Australia.

Sweden *(Cont. from 6)*

ment of Homeland Security (DHS). This is considered to be a highly important agreement that solidifies a strong partnership in the homeland security area. Several bilateral and multilateral activities in the areas of first responder protection technologies, biological/chemical networks and maritime domain awareness with mutually rewarding results have already taken place and additional activities are planned for in the future.

In 2009, the Swedish Government (coordinated by MSB) and the Directorate for Science and Technology at DHS will jointly host a transatlantic Stakeholders Conference in Stockholm, Sweden. The conference will be held on the 1st-2nd of October 2009. The conference is organized back-to-back with the European Union's Security Research Conference on the 29-30th of September 2009 in Stockholm. As DHS has created a solid homeland security research framework, parallel efforts in the European Union have set up a robust security research program (about €1.5 billion) in the multi-billion euro European Union Seventh Framework Program. In addition, several member states, including Sweden, have created national security research programs. This conference will provide a first opportunity for these programs to form strong transatlantic partnerships. ❖

* Jesper Gronvall
Senior Analyst, Homeland Security Project
Swedish Institute of International Affairs
(Based in Washington, D.C.)
1111 19th Street, NW
Washington, D.C. 20036
jesper.gronvall@ui.se
Office: 202-223-5956

Legal Insights *(Cont. from 12)*

biographical information. These forms are presented to U.S. Customs officials at the port of entry. The major difference with the new system is this same information must be submitted in advance using ESTA and VWP visitors must obtain authorization before departing — no later than 72 hours prior to travel and valid up to 2 years. An authorization under ESTA will not mean automatic entry — Customs officials will continue to make that determination at the airport. Having ESTA information in advance will help serve as a triage for Customs officials and hopefully lead to smoother entry for travelers.

According to Secretary Chertoff, this advance authorization should greatly improve security: "Getting this information in advance enables our frontline personnel to determine whether a visa-free traveler presents a threat, before boarding an aircraft or arriving on our shores."[7] Chertoff also stated that the new technology should greatly improve efficiency at the ports of entry and help officials to assess risk based on individuals as opposed to countries or groups.

All of this is logical — and necessary. The security standards of the Visa Waiver Program must be strengthened to meet 21st century threats. New countries cannot be admitted to the VWP without a trusted ESTA. Establishing such a system sounds simple but history says otherwise. Implementing security technology of any kind — even a relatively simple web-based registration system — is bound to be rough, as DHS officials know well from other initiatives. Personal data security and privacy are concerns with the new system, including possible conflict with European Union data privacy laws.[8] Too many false negatives from the system and the United States will suffer economically and diplomatically. Too many false positives will create unacceptable vulnerabilities. So, the stakes are high for full ESTA implementation in 2009. ❖

[7] "DHS Announces Pre-Travel Authorization Program for U.S.-Bound Travelers from Visa Waiver Countries," DHS, Press Release, June 3, 2008, http://www.dhs.gov/xnews/releases/pr_1212498186436.shtm.
[8] See, *The United States and Europe: Current Issues*, CRS Report for Congress, RS22163, January 24, 2008, http://ftp.fas.org/sgp/crs/row/RS22163.pdf.

Estonia *(Cont. from 7)*

cyber defence strategy in less than a year and many other nations started to update their national cyber-approaches.

Already more than a year before its establishment, the Centre's project team had been working with different cyber defence projects as risk assessments, policy and concept development and legal research and training in the field. CCD COE does not provide immediate cyber emergency assistance — according to current cyber defence doctrines it is vital that every nation secures proper proactive defence measures and tasks national CERT-s with response obligations. It is the responsibility of each nation to make sure that its critical information infrastructure is protected.

CCD COE is there to further develop concepts and doctrines in the field of cyber defence, to elaborate methodologies and capabilities to eliminate cyber threats as well as analyse and simulate different threats. One of the most challenging projects of the Centre is to provide for a cyber defence legal framework for NATO.

In a way this seems a mission impossible — NATO was never created to develop a legal regime of its own and existing international instruments do not contain efficient cyber defence mechanisms. On the other hand, the Estonian legal case study as many others before suggests that there will be no legal solution without international cooperation. As there is no reason and no point to duplicate the efforts of other international organisations, especially the Council of Europe and European Union in the field, the approach of the legal projects is to gather best legal practices of countries who have learned lessons similar to the one of Estonia. Based on these case studies, the CCD COE legal team will compile a checklist of legal problems that may occur in the course of applying different cyber defence measures like blocking, white-listing, tracking, logging, etc. This may be used as basis for national legal risk assessment and legal doctrine building.

Another task in front of the Centre is to create a community of interest comprising of NATO and nations' lawyers acting in the field in order to unify views and exchange information on actual problems and solutions. Law based on the principle of territoriality cannot be used as a primary tool for defence against cyber attacks. It can, however, be supporting the measures that are readily available in technological terms. To make law a solution, not a burden, takes common effort of the legal community. ❖

EU CIP *(Cont. from 10)*

system. These companies are already exchanging a lot of information both at an operative and a strategic level. The exchange is based on "peer to peer" relations, mainly due to the fact that there is not a single authority or organization that is in charge of regulation or coordination of the operators.[4]

Another challenge is the adoption of an integrated approach, combining information, personnel and physical security. It is still an area that did not reach its maturity and where many governments are investing. In particular, governments are more aware that a logical attack could impact physical infrastructures or vice versa and that personnel are not only important assets to protect, but can also represent an insidious threat or a vulnerable link that could be exploited to attack critical services. ❖

* Andrea Rigoni
Director of Critical Infrastructure Protection
Europe, Middle East and Africa (EMEA) Strategic Team – Symantec

Mr. Rigoni also runs a blog on CIP, containing daily news and articles on CIP with a particular focus on Europe and select key topics that are discussed in the United States. The blog can be accessed at: http://criticalinfrastructure.blogspot.com.

[4] In Europe there are various associations that group together Transmission System Operators or Large Power Companies: Union for the Coordination of Transmission of Energy (UCTE), TSOs in Ireland (TSOI), UKTSOA (the United Kingdom TSO Association), NORDEL (the Nordic TSOs) and the International Council for Large Power Operators (CIGRE). There is also the European Transmission System Operators Association that groups together UCTE, TSOI, UKTSOA and NORDEL. Despite the large number of entities, none of them have a complete coverage of formal authority to coordinate the sector.

The CIP Program and *The CIP Report* Recently Referenced by Congressman Wolf

Below is a copy of the George Mason University School of Law press release "Congressman Wolf Cites CIP Program in Press Release," dated June 12, 2008. Congressman Wolf makes specific mention of The CIP Report, noting that it is "required reading" in numerous homeland security agencies at the federal, state, and local levels.

The Critical Infrastructure Protection (CIP) Program at George Mason and James Madison Universities was cited in a press release issued by Congressman Frank Wolf (R-10th) in which he announced his intention to introduce a privileged resolution on the House floor calling for increased protection of congressional computer and information systems.

Wolf revealed in his press release that four computers in his personal office, as well as those of several other House members and of the House Foreign Affairs Committee, were compromised by outside sources believed to have probed the computers to evaluate the systems' defenses and to view and copy sensitive information. Wolf believes there is a strong likelihood that these cyber attacks issued from within the People's Republic of China.

"Computer systems control all critical infrastructures, and nearly all of these systems are linked together through the Internet. This means that nearly all infrastructures in the United States are vulnerable to being attacked, hijacked or destroyed by cyber means," Wolf stated.

Wolf Reveals House Computers Compromised by Outside Sources, Press Release from the Office of Rep. Frank Wolf (R-10th), June 11, 2008.

Excerpt:

> "Not long ago, few people within the U.S. government or in universities were systematically studying how a massive failure of our infrastructure could seriously disrupt our economy and way of life.
>
> "Few understood that we could be vulnerable to damaging attacks launched from overseas using only computers via cyberspace.
>
> "The Critical Infrastructure Protection (CIP) Program at George Mason University and James Madison University, which is now six years old, was formed in response to this gap in our knowledge about cyber threats.
>
> "At my request, the CIP Program began producing a monthly topical publication on homeland security issues that is required reading in the Pentagon, Homeland Security, DOE and state and local homeland security agencies.
>
> "Despite everything we read in the press, our intelligence, law enforcement, national security and diplomatic corps remain hesitant to speak out about this problem. Perhaps they are afraid that talking about this problem will reveal our vulnerability. In fact, I have been urged not to speak out about this threat.
>
> "But our adversaries already know we are vulnerable. Pretending that we are not vulnerable is a mistake.
>
> "As a nation, we must decide when we are going to start considering this type of activity a threat to our national security, a threat that we must confront and from which we must protect ourselves."

Read the Press Release Read Wolf's Resolution

Insight into Next Month's Issue

The July 2008 issue of *The CIP Report* will focus on public-private partnerships and highlights of recent conferences, including the 2nd National Conference on Security Analysis and Risk Management and the 2008 Homeland Security Symposium. The former was co-hosted by the CIP Program and held on George Mason University's Arlington, Virginia campus from May 13-15, 2008. The latter was co-hosted by the Institute for Infrastructure & Information Assurance at James Madison University, a CIP Program partner, and the Federal Facilities Council of the National Academies and held in Washington, DC on May 22, 2008. To maintain the timing of our annual International CIP issue, these conferences will be addressed in detail next month.

UK *(Cont. from 8)*

- the degree of disruption to an essential service;
- the extent of the disruption, in terms of population impacted or geographical spread; and
- the length of time the disruption persists.

Once the criticality of a site or system (and thus the impact of its loss) has been established it is then possible to calculate the risk to it by examining the:

- vulnerability; and
- threat.

The re-categorisation exercise has enabled the production of an up-to-date catalogue of more than 500 critical UK assets. These assets will be included in a centralised database and geographically mapped.

CPNI is the lead UK government authority responsible for providing protective security advice on terrorism and other threats to the UK national infrastructure

Ongoing analysis of the criticality scale and catalogue will be undertaken by working groups within the UK Government's counter terrorism machinery (of which CPNI is part). ❖

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1