THE WAR ON CYBERTERROR: WHY AUSTRALIA SHOULD EXAMINE THE U.S. APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION

Elizabeth Tutmarc

Abstract: As the global community focuses on detecting and fighting terrorism, defense strategists have identified the vulnerability of certain cybersystems. Traditional methods of defense and warfare, however, often do not apply to new technologies. Thus the cybercommunity is developing new standards for protecting computer resources against terrorist attack.

From the perspective of national governments, much attention has been paid to the importance of secure "critical infrastructure." This category of computer-dependent resources includes sectors vital to the smooth and orderly operation of public society, such as transportation, communications, and food production. These sectors are becoming increasingly dependent on computers to function, and the majority of critical infrastructure is owned by the private sector. This relationship between the public's interest in critical infrastructure and the interests of the private sector raises questions about how to balance the public and private interests in a cyberterror protection plan.

While governments have an interest in ensuring the security of critical infrastructure, they are reluctant to directly regulate privately-owned businesses. Since the late 1990s, the United States has been developing methods to secure infrastructure through public-private information-sharing partnerships, and has successfully taken steps to respect corporate privacy in the process. Conversely, Australia is in the early stages of developing a national strategy for critical infrastructure protection, and the government has faced corporate resistance to developing an information-sharing security network.

In comparing the cybersecurity situation in Australia to that in the United States, the Australian government should follow many of the steps that have made the U.S. process such a success to date. In particular, it should adopt similar corporate privacy protection policies for information shared with the government for critical infrastructure protection purposes, and should emphasize the development of public-private co-regulation of critical infrastructure. While the United States has not yet reached complete cybersecurity, its extra years of experience should inform the development of Australian policymaking.

I. INTRODUCTION

As a consequence of the terrorist attacks on September 11, 2001, many countries have integrated terrorism legislation into their existing crime-prevention schemes. This new legislation has often provoked concern from members of the legal community. For instance, anti-terror measures in

† The author wishes to thank the editorial staff of the Pacific Rim Law & Policy Journal and Prof. Jane Winn for skilled assistance, her family for supportive encouragement, and Jason Sykes for love and insightful conversation.
Australia have been accompanied by complaints from privacy advocates, and the country's most recent anti-terror legislation is no exception. Australia's initial anti-terror legislation was drafted shortly after September 11, but the death of eighty-eight Australians in the October 12, 2002, terrorist bombing in Bali brought renewed vigor to Australia's attempts to address terrorist threats. Strong Labor Party opposition to proposed amendments to Australia's anti-terrorism legislation stalled passage until the end of the 2002 legislative session. After reintroduction of the amendments, they were eventually revised and enacted.

One of the reasons for the new legislation is that Australia is concerned with effects of terrorism on its business community. Cyberterrorists pose a threat to the networked computers used by most businesses and can exploit security vulnerabilities to cause serious harm. Information technology experts suggest that a way to minimize the effect of network vulnerabilities is to promote a dialogue within industries to discuss security risks and remedies and to develop cybersecurity standards.

Private corporations provide many of Australia's basic services, such as banking, utilities, and telecommunications. The Australian Privacy Commissioner has been vocal in its opposition to the new legislation, arguing that it infringes on privacy rights. The legislation is also criticized for giving law enforcement agencies too much power to monitor and intercept communications.

---


2 Privacy Commissioner Slams New Anti-Terror Laws, supra note 1.


6 ASIO Bill to be Reintroduced to Parliament, AAP NEWSFEED, March 20, 2003.


10 See generally id.

11 See generally id.
as public utilities, banking, and transportation; thus the federal government does not have direct access to these industries’ security information.\textsuperscript{12} Because of the government’s interest in national security, however, former Australian Attorney-General Daryl Williams created an information-sharing network to promote the exchange of security data within these critical industries.\textsuperscript{13} There is a tension between the corporate sector and the public interest inherent in information-sharing programs, as private businesses are concerned with protecting their reputations and the government seeks to collect sensitive information to encourage increased cybersecurity. While this scheme of public-private critical infrastructure protection is new in Australia, the United States has been working on a similar program since 1998.\textsuperscript{14}

This Comment argues that Australia should look to the critical infrastructure protection program in the United States and consider its balance between corporate privacy and cybersecurity. Part II of this Comment describes the history and current state of critical infrastructure protection in Australia. Part III addresses Australia’s privacy legislation, and how it interacts with security-related information-sharing as part of Australia’s critical infrastructure protection efforts. Part IV highlights the problems Australia faces in creating a federal plan for critical infrastructure protection. Part V focuses on the U.S. experience in protecting its critical infrastructure, arguing that it has, to date, been generally successful in doing so. Part VI applies experiences in the United States to analogous information-sharing situations in Australia and provides recommendations for a smooth implementation of Australia’s new scheme to ensure protection of its critical infrastructure.

II. UNDERSTANDING COMPUTER-DEPENDENT RESOURCES AND CRITICAL INFRASTRUCTURE

Both private business and the public sector increasingly rely on computers and networked systems to function effectively.\textsuperscript{15} The vulnerabilities of this dependency on computers, however, are increasingly

\textsuperscript{12} Id.
\textsuperscript{13} Id.
\textsuperscript{15} See generally COMPUTER SCIENCE & TECHNOLOGY BOARD, CYBERSECURITY TODAY & TOMORROW: PAY NOW OR PAY LATER 2 (2002) (giving examples in which nearly every business relies on computer systems) [hereinafter CYBERSECURITY TODAY].
being exposed. As the phenomenon of cybercrime becomes increasingly widespread in Australia, it is being addressed not only by the information technology sector, but also through legislation and law enforcement.

A. Securing Cyber Resources Against Crime and Terror Requires Critical Infrastructure Protection

Virtually all sections of society and industry have become increasingly dependent on computers and most businesses in any given field use computers for multiple functions. Because most corporate computers are connected in a network and also usually connected to the Internet, these linked computers are considered a type of foundational infrastructure supporting those industries that rely on computerized processes. A properly functioning "critical infrastructure" allows industries to consistently conduct operations necessary to provide products and vital services without unneeded delays, corruption of data, or unauthorized access to the network system.

The importance of understanding the ways in which a network can be vulnerable gained widespread public attention during compliance preparation leading up to the year 2000. Since then, both the public and governments across the globe have become aware of the negative effects of widespread network failures. The September 11th attacks have increased concern about vulnerabilities in the networks of vital-services providers and

---

16 See generally CYBERSECURITY TODAY, supra note 15, at 3.
18 CYBERSECURITY TODAY, supra note 15, at 2.
19 Id. at 3.
21 CYBERSECURITY TODAY, supra note 15, at 3.
23 COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, TRUST IN CYBERSPACE 1 (Fred B. Schneider ed., 1999) [hereinafter TRUST IN CYBERSPACE].
heightened the level of priority for securing critical infrastructure. One of the ways to secure critical infrastructure is through the sharing of security and vulnerability information across industries, in order to promote awareness of threats and to increase cooperation between government and the private sector.

Beyond being simply a tool for promoting awareness, information-sharing between the public and private sectors is supported by some in the information technology community as essential to protect against threats. Attacks by cybercriminals can interrupt a region’s communications, halt transportation methods, or leave financial institutions open to theft. Because a network depends upon the strength of each computer within the network, a single computer left open to a threat poses substantial risks to the rest of the system. Creating standards of network trustworthiness through information sharing provides one method by which various industries can seek to maintain the integrity of the entire system.

As part of a critical infrastructure protection strategy, businesses share information relating to system vulnerabilities (such as the number of incidents of attacks on the network) and remedies as a way to promote awareness within a particular industry sector. A large percentage of security breaches go unreported because the affected business does not realize that they have occurred. A dialogue regarding cybersecurity is intended to counter this effect. Another purpose of information sharing is to develop a warning system to alert other critical industries if a large-scale threat is encountered by one sector. Information sharing among computer network-reliant industries not only serves to assist the businesses themselves in combating crime, but also is a vital piece of a broad, national counter-terrorism policy.

---

24 CYBERSECURITY TODAY, supra note 15, at 6.
25 TRUST IN CYBERSPACE, supra note 23, at 253.
26 Id.
27 CYBERSECURITY TODAY, supra note 15, at 6.
28 See id. at 7.
29 See TRUST IN CYBERSPACE, supra note 23, at 251.
31 Id. at 11.
32 See generally id.
33 Id. at 21.
34 See generally id.
B. **Australia is in the Early Stages of Developing Critical Infrastructure Protections, but is Still Developing Implementation Plans**

As Australia encounters evidence of computer-network vulnerabilities and infrastructure dependence, the national government has passed laws in the hopes of preventing cybercrime.\(^ {35} \) An information-sharing network is being designed,\(^ {36} \) but the Australian government is almost entirely reliant on private businesses to create a system that can share information and strengthen critical infrastructure. Although the Australian government is reluctant to impose regulations on private businesses, it recognizes that the security of the country is dependent upon the private sector’s ability to detect and prevent cybercrime.\(^ {37} \)

1. **Australia’s Efforts to Combat Cybercrime**

Australia has already encountered incidents of cybercrime at the national level.\(^ {38} \) In 2001, an Internet financial network was attacked, revealing the private information of 1200 credit card customers.\(^ {39} \) In 2003, a hacker compromised another business network and gained access to the account information of 400,000 customers.\(^ {40} \) Australia’s public utilities system also fell victim to cybercrime in 2001, when 150 computer-controlled sewage-pumping systems were redirected to pump raw sewage into public waterways, causing thousands of dollars of damage to the area.\(^ {41} \) Australian businesses have expressed concern over their vulnerability to such security attacks,\(^ {42} \) especially in sectors dependent upon large computerized networks. Surveys reveal gaps in many Australian businesses’ cybersecurity systems, yet there is a lack of evidence that these businesses are taking steps to make their networks more secure.\(^ {43} \)

\(^ {35} \) See, e.g., Cybercrime Act, 2001 (Austl.).
\(^ {37} \) Sue Cant, Warning on Cyber Terror, AGE (Melbourne), Feb. 24, 2004, at 1.
\(^ {39} \) Lebihan, supra note 38.
\(^ {40} \) Hughes, supra note 38.
\(^ {41} \) Glenis Green, Sewage Overflow Linked to ‘Hacker,’ COURIER MAIL, June 16, 2000, at 14; Hughes, supra note 38; Lebihan, supra note 38.
Some steps to secure Australia’s critical infrastructure have been taken at the federal level. Australia’s National Office of Information Economy (“NOIE”) requested that the nation’s security experts advise the federal government on how to develop critical infrastructure security plans.\(^{44}\) To help do so, NOIE created the Critical Infrastructure Advisory Council (“CIAC”), which met for the first time in February 2004.\(^{45}\) The CIAC consists of security experts from around Australia who will collect security information from various critical industries and advise them on how to increase security.\(^{46}\) Government officials admit that Australia is behind some other countries in developing an infrastructure security strategy, but claim that the delay allows Australia to learn from others’ experiences.\(^{47}\)

Australia’s Labor Party has proposed the creation of a Department of Homeland Security, which would lead the effort to secure critical infrastructure.\(^{48}\) Prime Minister Howard’s Liberal Party, however, supports a “multi-layered” approach to national security, without the centralization of security under a federal department.\(^{49}\) The federal election expected to occur later this year, possibly in October, may determine which approach to national security Australia will be implemented in the future.\(^{50}\)

2. Questions Remain Regarding the Efficacy of Australia’s Trusted Information-Sharing Network

Following September 11, the Australian government created the Trusted Information-Sharing Network (“TISN”) by asking a variety of industries to voluntarily share information that it believed could help prevent

---


\(^{45}\) Lebihan, supra note 44.

\(^{46}\) Michael Gordon, *Be Alert for Terrorism, Bosses Told*, AGE (Melbourne), Feb. 26, 2004, at 3; Lebihan, supra note 44.

\(^{47}\) Lebihan, supra note 44. For information on Great Britain’s infrastructure protection efforts, see National Infrastructure Security Co-ordination Centre, at http://www.niscc.gov.uk/index.html (last visited May 21, 2004).


\(^{49}\) Anderson, supra note 48.

cyberterrorism. The TISN affects industries considered to be critical infrastructure and requests that these industries share information related to cybersecurity. Such information includes data on a business’ general systems attacks/failures, vulnerabilities yet to be exploited by criminals, and strategies to prevent network exploitation. The CIAC acts as an advisory link between the TISN and the Australian attorney-general, helping to coordinate communication between the sectors represented in the TISN and also with the federal government.

The government’s requests for an information-sharing process, however, have not been accompanied by a specific plan to protect customer and corporate confidentiality. Specifically, the banking industry has been resistant to the TISN without such privacy safeguards. The banking sector has indicated that, without statutory protection for customer privacy, government intervention will run counter to the public’s interest. More recently, the private sector has raised concerns about public access to confidential business information regarding system vulnerabilities. Australian businesses are not eager to allow disclosure of such information because of possible damage to their reputation and fear of government regulation.

The TISN is still in the process of being designed and organized, and the privacy concerns that have already been raised help to explain private-sector reluctance to the sharing of cybersecurity information. In order for Australia to effectively promote information-sharing as a method of infrastructure protection, uncertainty in the legal framework of corporate privacy must be eliminated. While there are many reasons why organizations, especially private-sector businesses, may be reluctant to enter

---

53 Information Sharing Arrangements, supra note 36.
55 Lebihan, supra note 1.
56 Peters, supra note 1.
58 Id.
into information-sharing agreements, little progress on information-sharing can be made until these concerns are addressed.

III. AUSTRALIA’S LEGISLATIVE FRAMEWORK FOR PROTECTING CORPORATE PRIVACY

In combating cybercrime and terrorism, Australia’s public and private sectors rely on federal legislation not only for definitions of applicable crimes, but also for the available protections. While critical infrastructure protection is focused on the prevention of cyberterrorism, the expansion of criminal definitions to specifically include acts of terrorism is also a crucial part of a broad counterterrorism policy. The Australian Security Intelligence Organization (Terrorism) Act 1979, the Freedom of Information Act 1982 and the Privacy Act 1988 create the legislative framework of Australia’s system of critical infrastructure protection.

A. Recent Australian Security Intelligence Organization Legislation Has Changed the Privacy Law/Infrastructure Security Regime by Defining Terrorism Offenses

Australia’s main piece of anti-terror legislation, the Australian Security Intelligence Organization (Terrorism) Act 2002 (“Terrorism Act”), expands the Australian government’s capacity to fight terrorism by granting extended warrant, search, and surveillance powers to the Australian Security Intelligence Organization (“ASIO”). Part 5.3 of the Terrorism Act, which includes the definitions section, also specifically expands the definition of

---

65 ASIO Amendment Explanatory Memo, supra note 61. The ASIO is Australia’s federal security organization, which advises the government on security matters and collects and investigates security intelligence. See ASIO Act, supra note 61, § 17, for further explanation of the functions of the ASIO.
terrorism to include cyberthreats. An action is considered an act of cyberterror if it:

- seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:
  1. an information system; or
  2. a telecommunications system; or
  3. a financial system; or
  4. a system used for the delivery of essential government services; or
  5. a system used for, or by, an essential public utility; or
  6. a system used for, or by, a transport system.

This anti-terror legislation recognizes the threat of cyberterrorism and is part of the government’s effort to secure Australia’s critical infrastructure.

The ASIO legislation builds on the criminal definitions and punishment scheme of the Cybercrime Act 2001 (“Cybercrime Act”). The Cybercrime Act defines electronic crimes and law enforcement powers relating to computers, and expands traditional criminal law and procedure to computers and networks. The Australian Attorney-General’s Department states that the Cybercrime Act and Australia’s anti-terror legislation demonstrate to the business community that cybercrime will be treated seriously. While the Cybercrime Act and the Terrorism Act provide investigation and punishment schemes for cyberterrorism, the Australian government has also demonstrated its willingness to prevent terrorism through critical infrastructure protection.

---

67 Id. pts. 5.3, 100.1(2)(e).
69 Id. scheds. 1 & 2.
B. The Freedom of Information Act of 1982 Interacts with ASIO Legislation to Provide a Check on Government Terrorist Investigations

While ASIO legislation provides the legal path by which the government can gather information about individuals of interest in terrorist investigations, Australia's Freedom of Information Act 1982 ("AusFOIA") allows individuals and organizations to gain access to certain government documents. AusFOIA creates a process by which the public can obtain copies of government documents, but access is limited if such a release is against the public interest.

AusFOIA defines certain limited exceptions to the general presumption that the public has a right to access government documents. The Privacy Commissioner has asserted that it is not the intent of the TISN to disclose sensitive personal data or corporate trade secrets. Yet because the federal government would gain access to information shared between businesses through the TISN, AusFOIA claims could potentially be used to obtain these documents. Documents shared with the government under the TISN program could fall under a number of exemption provisions in AusFOIA. AusFOIA's section 43 exempts confidential business documents from disclosure requests. Specifically, trade secrets and other information that would have less commercial value if they were disclosed are exempted from AusFOIA claims under this provision. This section may have limited applicability to the TISN, however, because it was not intended to be a forum for the sharing of trade secrets; cyber vulnerabilities are considered common to many infrastructure industries and more general in scope than

73 Id. pt. 1(3)(1)(c).
74 Information Sharing Arrangements, supra note 36.
75 Australia's Privacy Commissioner is in charge of regulating federal privacy, which involves responsibilities ranging from investigating complaints under the Privacy Act to issuing guidelines for compliance with privacy policies. See The Office of the Federal Privacy Commissioner, at http://www.privacy.gov.au/about/index.html (last visited May 21, 2004).
76 Rachel Lebihan, Eyes Wide Open on Trusted Data Sharing Network, AUSTRALIAN FIN. REV., June 19, 2003, at 18.
77 Information Sharing Arrangements, supra note 36.
78 AusFOIA's numerous exemptions have been criticized for their vague and confusing language, but the act has generally been viewed as a positive step toward open government in Australia. See Debra L. Silverman, Freedom of Information: Will Blair Be Able to Break Down the Walls of Secrecy in Britain?, 13 AM. U. INT'L L. REV. 471, 544-545 (1997).
79 Freedom of Information Act (Austl.) § 43.
80 Id. § 43(1) & (3).
the confidential business information typically considered a trade secret.\(^8\)

Section 43 also exempts information from disclosure that would have an adverse effect on the undertaking of an organization related to “its lawful business, commercial or financial affairs,”\(^2\) and information that, if disclosed, could “reasonably be expected to prejudice the future supply of information to the Commonwealth.”\(^3\) Information shared with the government regarding private sector system vulnerabilities meets both requirements of section 43, because such information relates to business undertaking, and disclosure of such information could make vulnerable industries less willing to share data with the TISN.

AusFOIA’s section 45 also guarantees the privacy of documents procured by the government in confidence if the source of the document could succeed with a claim for breach of confidence if the document was disclosed.\(^4\) Information procured by the government might fall under this category if the procurement resulted in a relationship of trust between the government and the private business.\(^5\)

Because AusFOIA claims are handled on a case-by-case basis, however, it is difficult to guarantee that a business’s vulnerabilities will not be disclosed by the government under any circumstances.\(^6\) Without a specific exemption for such documents, businesses will continue to use AusFOIA concerns as a rationale for avoiding information-sharing.\(^7\)

C. The Privacy Act 1988 Limits Both the Public’s and the Private Sector’s Ability to Disclose Personal Information, but it is Unclear if Critical Infrastructure Information is Included

In addition to the right of access granted by AusFOIA, the Privacy Act 1988 (“Privacy Act”) assures Australians that their government will comply with certain minimum standards to protect the privacy of their personal information.\(^8\) The Privacy Act also creates an independent federal

---

\(^{81}\) *Information Sharing Arrangements*, supra note 36.

\(^{82}\) Freedom of Information Act (Austl.) § 43(1)(c)(i).

\(^{83}\) *Id.* § 43(1)(c)(ii).

\(^{84}\) *Id.* § 45.

\(^{85}\) A relationship of trust would exist if, for instance, the government’s procurement had been accompanied by a confidentiality agreement, stating that the government would not disclose the information it received from the private business.

\(^{86}\) *Information Sharing Arrangements*, supra note 36.


entity, the Office of the Federal Privacy Commissioner, to oversee all privacy-related complaints and conduct investigations into breaches of privacy.\(^\text{89}\)

The Privacy Act outlines eleven information privacy principles ("Privacy Principles") that explain how the federal government must handle personal information.\(^\text{90}\) In accordance with these principles, the government can collect personal information for lawful purposes with minimal intrusion on an individual's privacy, but the individual must be able to access such information and make corrections if necessary.\(^\text{91}\) These principles applied only to the public sector under the original 1988 law, but the Privacy Act was amended in 2000 to include the private sector as well.\(^\text{92}\) As part of the amendment's strategy\(^\text{93}\) for the private sector, businesses are allowed to create industry-wide privacy codes for themselves, which are then to be approved by Australia's Privacy Commissioner.\(^\text{94}\) The Privacy Principles generally protect information that consumers provide to businesses, with limitations on how the information may be used and when it may be disclosed.\(^\text{95}\) This approach, requiring minimal legislative involvement in corporate privacy practices, has been criticized by privacy advocates and scholars for not going further to protect citizens' privacy.\(^\text{96}\)

As the Privacy Act and its 2000 amendment stand now, there is one private sector Privacy Principle that is particularly relevant to an

\(^{89}\) For information regarding the legislative history of the Privacy Act and the structure of the Office of the Privacy Commissioner, see Paul Kelly, *Recent Developments in Private-Sector Personal Data Protection in Australia: Will There Be An Upside Down Under?* 19 J. MARSHALL COMP. & INFO. L. 71 (2000).

\(^{90}\) Privacy Act § 14.

\(^{91}\) *Id.* For further explanation of the principles, see *Privacy Laws for the Private Sector Now a Reality*, 3 No. 9 E-COMMERCE L. REP. 21 (2001).


\(^{96}\) See, e.g., Kohel, supra note 92; John Bentivoglio et al., *Global Privacy Law Update*, 20 COMPUTER & INTERNET L. 1 (2003).
information-sharing network. In general, personal information collected by a business may not be disclosed for a reason unrelated to the primary purpose of a business, but an exception is granted for law-enforcement purposes. According to Principle 2.1(f), an organization may disclose personal information if it has:

reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

Businesses may also disclose information for the purposes of law enforcement for “the prevention, detection, investigation or remedying of seriously improper conduct or proscribed conduct.”

A note to this section of the Privacy Principles states that “[i]t is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.” While it is not a purpose of the TISN to include the sharing of personal information, if it were disclosed in an investigation, it would be subject to these sections of the Privacy Act.

With the expansion of ASIO legislation to specifically cover cyberterrorism and the creation of a TISN, the Australian government has shown that it is committed to protecting its computer-networked resources. The lack of clarity in the FOIA and Privacy Act exemptions, as applied to critical infrastructure information, however, leaves private industries without a clear plan for progress toward effective cooperation with the government.

IV. THE CURRENT STATE OF AUSTRALIAN CYBERSECURITY

Although Australia’s federal government has demonstrated an intention to protect its critical infrastructure through public-private
cooperation, efforts are moving ahead slowly.\textsuperscript{103} The slow pace reflects uncertainty about how to balance security and corporate privacy, and arguments have been made for both increased government involvement and more private independence.\textsuperscript{104} While that tension should be addressed, delay on critical infrastructure protection only increases the risk that vulnerabilities will be exploited.

Cybersecurity experts cite many reasons for Australia’s slow progress in protecting its critical infrastructure.\textsuperscript{105} Trade groups have blamed the government for a lack of implementation and regulation of information-sharing mechanisms.\textsuperscript{106} Although the CIAC was created in 2002,\textsuperscript{107} the government has not used the CIAC to adopt private sector recommendations.\textsuperscript{108} Critics argue that a strained and undefined relationship between the government and the private sector is at the root of the delay.\textsuperscript{109} Australia’s Computer Emergency Response Team (“AusCERT”), appointed by the Australian government to advise the public and businesses on cyberthreats as part of the TISN,\textsuperscript{110} is concerned that other Pacific Rim countries—including Malaysia, South Korea and Japan—are significantly outspending Australia’s investment in infrastructure security, and that Australia cannot afford to lag behind.\textsuperscript{111} Moreover, global infrastructure analysts point to Australia’s lack of funding of infrastructure protection as evidence that the government is pursuing a limited role in this form of cybersecurity.\textsuperscript{112}

A government official in the Attorney-General’s Department defends the government’s slow approach, arguing that it is in Australia’s interest to
make sure the TISN is effective. Along the same lines, Australia’s delayed development of a critical infrastructure security scheme similar to the United States’ has been called an advantage, as it might afford Australia the opportunity to learn from the failures and successes of the U.S. example.

At least one member of Parliament has called for more government regulation of infrastructure security and for the private sector to make cybersecurity a top priority. She also argues that the private sector will not share system vulnerabilities merely because of voluntary requests from the government, but only if it is required to do so under law. She also points to infrastructure security legislation in both the United States and Great Britain as examples of minimal, but effective standards required for the private sector. The Attorney-General’s Department has responded by stating that, because legal regulation of private-sector security would require the government to inquire into countless industries’ security systems, requiring the private sector to share security information would only be a last resort should voluntary sharing fail.

In a time of heightened sensitivity to the threat of terrorism, the publicity surrounding potential cybervulnerabilities legitimately worries both critical infrastructure industries and the public. When the Australian government published a 1998 report on terrorist vulnerabilities in communications and utilities industries on its website in July 2003, with information on how terrorists could infiltrate those industries, some media outlets called the publication a “breach of security.” The Attorney-General’s Department replied that national security was not threatened because the report was already public information, was outdated, and because the vulnerabilities had already been fixed. Even though this report allegedly had limited security value, the fact that reports of system vulnerabilities alarm the public gives credence to corporate insistence that cybersecurity information supplied to the government must be kept private

113 Lebihan, supra note 103 (quoting Mike Rothery, the Attorney-General’s Senior Adviser on national information infrastructure).
114 Id.
115 Cochrane & Cant, supra note 110. See also SEN. KATE LUNDY’S WEB PAGE, http://www.katelundy.com.au (for statements and press releases, suggesting that Australia needs to take cybersecurity more seriously and ensure that the TISN makes progress) (last visited May 21, 2004).
116 See Cochrane & Cant, supra note 110.
117 Id.
118 Id.
120 Govt Denies Terror Blue-Print Threatens National Security, AAP NEWSFEED (Canberra), July 29, 2003.
121 Id.
to protect market competitiveness. The public is becoming more aware of the risks of vulnerabilities in public and private networks, and the Australian government needs to take decisive steps to ensure the protection of critical infrastructure.

V. CRITICAL INFRASTRUCTURE PROTECTION IN THE UNITED STATES

In many ways, the cybersecurity situation in the United States parallels Australian attempts to increase its protection of critical infrastructure. The United States began to recognize the need for national critical infrastructure protection in the late 1990s, and these extra years of experience gave it a head start over Australia. As such, Australia should look to the U.S. experience in developing its own cybersecurity measures.

A. New Threats and Changing Law Enforcement Priorities Caused the Evolution of U.S. Critical Infrastructure Protection Strategies

In 1998, the United States Department of Justice and the Federal Bureau of Investigation created the National Infrastructure Protection Center ("NIPC") as a clearinghouse for the sharing of information relating to the security of critical infrastructure. As defined by the Critical Infrastructure Information Security Act of 2001, critical infrastructure includes:

physical and cyber-based systems and services essential to the national defense, government, or economy of the United States, including systems essential for telecommunications (including voice and data transmission and the Internet), electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services (including medical, fire, and police services), and the continuity of government operations.

At the time of NIPC's creation in 1998, the goals of the U.S. government were to create a critical infrastructure that would be invulnerable to intentional attacks by 2000, and to be running at "enhanced

122 Dick, supra note 14, at 3.
123 This definition comes from the unenacted Critical Infrastructure Information Security Act, S. 1456, 107th Cong. § 4(2) (2001) [hereinafter CIISA]. For other definitions of "critical infrastructure" found in legislation and private documents, see Joseph Summerill, Is it Safe For Your Client to Provide the Government With Homeland Security Data?, 50-JAN FED. LAW. 24, n.7 (2003).
capability" by 2003. As the United States developed early models of infrastructure protection, the government's role in cybersecurity received attention. When it became apparent that the private sector was the main provider of critical infrastructure services, however, the government's strategy shifted to focus more on the security of private businesses.

Following the events of September 11, 2001, NIPC was absorbed into the Department of Homeland Security's ("DHS") Information Analysis Infrastructure Protection Division. Other federal agencies dealing with infrastructure security, including the Department of Defense's National Communication System and the Commerce Department's Critical Infrastructure Assurance Office and Computer Security Division, were also reorganized under the umbrella of DHS. Through the consolidation of federal departments and agencies working on infrastructure security, the government intended to facilitate more efficient information sharing between groups and avoid redundancies among staff resources across separate offices.

NIPC requests information related to security threats and measures taken to remedy the threats from public and private sector infrastructure industries. While the government is still asking the private sector to volunteer information related to infrastructure security, recent U.S. legislation, particularly a recent addition to Freedom of Information Act ("U.S. FOIA") exemptions, has made privacy concerns related to information-sharing less burdensome on private industries.

---

124 "Enhanced capability" is defined in contrast to "initial operating capability," but the term is not specifically defined. This lack of clarity in definitions is noted as problematic later in the document. SIGNIFICANT CHALLENGES, supra note 30, at 5.

125 Id.


127 SIGNIFICANT CHALLENGES, supra note 30, at 25.


129 SIGNIFICANT CHALLENGES, supra note 30, at 13-14.

130 See id. at 14.

131 Summerill, supra note 123, at 25.


133 Id. at 26.
B. Corporate Privacy Concerns Exist About Information Shared with the U.S. Government for Infrastructure Protection Because Corporate Information Could Make its Way into the Public Domain

One of the concerns of private U.S. industries has been the application of the U.S. FOIA to any information they voluntarily submit to DHS. Because U.S. FOIA is primarily applicable to government agencies, a private sector business is not the typical target of a U.S. FOIA disclosure request. Because DHS receives information from the private sector in connection with system vulnerabilities, however, such information could conceivably be subjected to a U.S. FOIA claim, thus rendering sensitive private business material available to the public.

The Critical Infrastructure Information Security Act ("CIISA"), proposed in 2001 but never enacted, would have eliminated this possibility by adding a new disclosure exemption for infrastructure security documents voluntarily submitted to the government. While U.S. FOIA already includes an exemption for confidential business information and documents related to national security and law enforcement, CIISA would have made it clear to private critical infrastructure-related companies that their corporate privacy would remain protected from disclosure. CIISA explicitly protected voluntarily submitted information, not only from U.S. FOIA claims, but also from use by other government agencies for any purpose other than the protection of critical infrastructure.

When DHS was created in 2002, many of the goals of CIISA were realized. Section 214 of the Homeland Security Act of 2002 ("HSA"), is entitled "Protection of Voluntarily Shared Critical Infrastructure Information" and includes an exemption from U.S. FOIA for such documents. The HSA also prohibits government agencies and other third parties from using such information in a civil action against the provider if the information was submitted in good-faith compliance with security standards. The HSA also makes clear that voluntary submission of

---

134 Summerill, supra note 123, at 25. This same concern was raised during the preparation for Y2K, and information shared with the government under the Year 2000 Information and Readiness Disclosure Act, Pub. L. No. 105-271, § 4(f)(3)(A) (1998).
136 Id.
137 CIISA, supra note 123, § 5(a)(1)(A).
138 Id. § 5.
139 Id.
142 Id. § (a)(1)(C).
infrastructure information does not constitute a waiver of trade secret protection. 143

Civil liberties groups and scholars decry the new U.S. FOIA exemption in the HSA as eliminating a vital check on government abuse. 144 Especially considering that U.S. FOIA already includes an exemption for documents relating to national security and law enforcement, and also exempts confidential business information, these groups argue that another exemption is unnecessary. 145 These groups assert that there is no evidence that such a U.S. FOIA exception would succeed in encouraging private industries to turn over infrastructure-related information to the government, and that it is more likely that industries are not concerned about U.S. FOIA disclosures. 146 If the proposed exemption merely serves to protect the government from embarrassing public revelations of infrastructure weaknesses, these groups are concerned that U.S. FOIA’s purpose of promoting open government would be undermined. 147 Furthermore, these groups have argued that public citizens have a right to know about infrastructure vulnerabilities. 148 If industries are exempt from both disclosure of and liability for their cyberweaknesses, they argue, the sharing of information will not enhance protection of U.S. national security. 149

Prior to passage of the HSA, the Senate Committee on Governmental Affairs heard testimony noting that U.S. FOIA’s fourth exemption already covers confidential commercial information obtained by the government. 150 The government defended the HSA exemption as necessary to encourage the sharing of information. 151 Unlike in Australia, where privacy legislation has recently been extended to include the private sector, the United States has

143 Id. § (a)(1)(F).
145 See ACLU Letter, supra note 144. For more information about FOIA exemptions, see Summerill, supra note 123, at 26.
146 See ACLU Letter, supra note 144.
147 Id.
148 See EPIC Statement, supra note 144 (because if a private business can hide its vulnerabilities, it does not have an incentive to increase security).
149 Id.
150 Id.
151 Summerill, supra note 123, at 27.
not regulated the privacy practices of private U.S. business. While the private sector might be ignorant of the privacy safeguards in existing U.S. FOIA exemptions, the government nonetheless argued that adding an exemption would indicate its commitment to the privacy of private industries and consumers. According to the government, the broad protections outlined in the case law surrounding U.S. FOIA's fourth exemption do not satisfy industry concerns that their specific information will be not be disclosed. Thus, a clear exemption for infrastructure security information is needed.

U.S. government officials have noted this tension between public and private interests as the need for critical infrastructure protection has gained publicity, especially after the August 2003 massive blackout on the East Coast of the United States. One legislator succinctly described the inherent tension between the public interest and concerns of the business community:

So we are sitting there trying to struggle as a Congress and as an administrative agency that the Department of Homeland Security is, and ask how do we get industry to step up to the plate and protect these critical assets to the point where we need it to be, while at the same time we understand that the important thing for business is the bottom line.

C. Public-Private Partnerships Are Helping the United States Take Additional Steps to Protect Its Critical Infrastructure in All Sectors

DHS has divided the U.S. critical infrastructure into various

---

154 Found at 5 U.S.C. § 552(b)(4), this provision exempts documents that are "trade secrets and commercial or financial information obtained from a person and privileged or confidential" from U.S. FOIA disclosure.
155 See Malcolm Statement, supra note 153. This viewpoint was supported by industry groups such as the Information Technology Association of America. See Critical Information Protection, at http://www.itaa.org/es/cne/cipover.htm (last visited May 21, 2004).
157 Id. at 12 (quoting Rep. Loretta Sanchez (D-CA)).
Information Sharing and Analysis Centers ("ISACs"), such as telecommunications and public utilities, with the assumption that communication will be most effective between groups within the same industry. DHS has appointed applicable federal agencies or industry leaders to sponsor each ISAC. For example, the U.S. Treasury is the lead for the financial services ISAC, and the non-profit Food Marketing Institute oversees the food and agriculture ISAC. Businesses within each sector have the opportunity to join their corresponding ISAC, usually for a fee.

Once a particular business joins an ISAC, it then has access to alerts and warnings of cyberattacks for that industry and can share information on building more secure networks. Upon request from the U.S. government, an ISAC can provide a sanitized compilation of a sector's threats and security efforts. The threat information may then be analyzed by government security experts, who can recommend remedies. The ISAC system has facilitated progress on critical infrastructure protection through increased organization.

The ISAC system, however, is not without flaws. A recent symposium of all the ISACs revealed that most industries do not have the

158 For a list of all ISACs and links to information on them, see Department of Homeland Security, Threats and Protection: Information Sharing & Analysis Centers, at http://www.dhs.gov/dhspublic/display?theme=73&content=1375 (last visited May 21, 2004) [hereinafter DHS ISAC].


160 See DHS ISAC, supra note 158.


163 See, e.g., Financial Services ISAC, Next Generation FS/ISAC Frequently Asked Questions, at http://www.fsisac.com/faq.cfm (last visited May 21, 2004) (explaining membership fees for the financial services sector) [hereinafter FSISAC FAQ]. Basic membership is free, but basic members receive only urgent and crisis alerts and can participate in sector surveys. Core membership, available for US$ 10,000, provides the full range of alert options and web site access, participation in conference calls and meetings, and use of the resources of a staffed security center. Id.


165 This means that the document has no without any identifying marks to an individual business or trade secret.

166 FSISAC FAQ, supra note 163.

167 Id.

168 See INFORMATION SHARING RESPONSIBILITIES, supra note 128, at 22.

169 Hosted by George Mason University School of Law, which runs a Critical Infrastructure Protection Project ("CIP Project"), in conjunction with James Madison University. See Preliminary Findings of the CIP Project's ISAC Symposium, supra note 159. According to Appendix A of the findings report, the following industries were represented at this symposium: banking and finance, chemicals,
necessary funding or staffing to fully engage in effective infrastructure protection.\textsuperscript{170} Additionally, the symposium found that roles of the government and of the private sector are not clearly delineated, which can lead to duplication of efforts and confusion of responsibilities.\textsuperscript{171} This confusion has led to increased debate about the proper structures and allocations of authority among ISACs without implementation of any solutions.\textsuperscript{172}

One way to alleviate such confusion could be for the U.S. government to make critical infrastructure protection mandatory for businesses in those industries, but it could prove difficult to implement because of potential private sector opposition. DHS has not completely eliminated this possibility, although businesses are generally opposed to increased government involvement in the corporate realm.\textsuperscript{173}

Some scholars have noted that the true problems of infrastructure protection have not even been addressed because of the preliminary problems associated with information-sharing.\textsuperscript{174} These problems include both the threat of disclosure of private corporate information under U.S. FOIA, and direct federal entanglement with private-sector cybersecurity.\textsuperscript{175} In order to make communication possible between public and private sectors, these two legal issues surrounding critical infrastructure protection must be addressed.\textsuperscript{176}

\begin{itemize}
\item electric power, emergency management and response, emergency law enforcement, food, information technology, interstate, oil and gas, railroad, surface transportation, telecommunications, water supply, and healthcare. \textit{Id.}
\item \textit{Id.} at 2.
\item \textit{Id.} at 4.
\end{itemize}
The first issue has already been officially addressed through the enactment of the DHS exemption from U.S. FOIA, and as this is tested and supported by private industries, critical infrastructure protection strategies can be further developed and implemented. Corporate resistance to government regulation, the second threat to private infrastructure protection, cannot be overcome simply by legislation, but recent efforts by the electric power industry suggest a possible model of cooperation in lieu of unilateral government regulation.

1. NERC Regulations Can Serve as a Model for Public-Private Cooperation on Information-Sharing

The North American Electric Reliability Council ("NERC") was named ISAC for the electricity sector, and complied with the U.S. government's request for a draft of minimum standards for computer network security for the nation's electricity grids. Because a breach in security within the electricity sector can result in such drastic consequences, NERC recognized that implementing security standards is an issue that warrants the attention of the electricity industry.

The Federal Energy Regulatory Commission included these standards in its regulations and opened the drafts for a period of public comment. The public comment period is still open, but NERC is already at work on developing methods for implementing the standards. Once member companies adopt the standards as NERC requirements, energy organizations will self-certify that they are complying with the standards. This

---

177 For further description of how DHS currently maintains the privacy of critical infrastructure information, see Procedures for Handling Critical Infrastructure Information, 69 Fed. Reg. 8074 (Feb. 20, 2004).
178 See Gorman, supra note 173, at 18.
181 See Lewis, supra note 179, at 19.
184 See Lewis, supra note 179, at 19.
AUSTRALIA'S WAR ON CYBER TERROR

The certification process will require electricity entities to claim compliance or explain their degree of non-compliance. NERC will not conduct investigations to verify these self-certifications. Such certifications will be confidential, and not disclosed by NERC. The standards implemented by NERC will be in effect for 2004 only, and then will be re-assessed for 2005 and beyond. While the NERC situation is unique because most of the bulk electric grid operators are members of NERC and therefore already subject to its standards, this model of industry-created self-certifying standards enforced by the government is one way of achieving infrastructure protection while maintaining corporate input.

By creating a specific U.S. FOIA exemption for information shared with the government for critical infrastructure protection, and finding a successful model for public-private partnership in the electricity sector, the United States is making progress toward security. The roles of government and the private sector in critical infrastructure protection are being examined and delineated, and this clarity will make future protection efforts more effective. Public-private partnerships still need to expand into other sectors, but the recent years of progress suggest that cooperation between the private sector and the government will continue to increase.

VI. U.S. LESSONS IN INFRASTRUCTURE SECURITY THAT AUSTRALIA SHOULD CONSIDER ADOPTING

While Australia and the United States agree that critical infrastructure protection is a government priority and a necessary part of an effective counterterrorism campaign, Australia is still in comparatively early stages of developing a national plan for cybersecurity. The debate surrounding the need for balance between corporate security and public awareness exists in both countries, yet the United States has taken specific action to encourage further steps toward complete protection of its critical infrastructure. Australia should consider these steps in designing and

\[186\] See Implementation Plan, supra note 184.
\[187\] Id.
\[188\] Id.
\[189\] Id.
\[190\] Id.
\[191\] Not all agree that the United States has appropriately and/or effectively balanced privacy and security in its efforts to protect critical infrastructure, but this Comment argues that the continuing U.S. debate over these issues should be considered in the Australian decisionmaking process. See, e.g., Mark Ellison, America’s Response to 9/11 (2004) (unpublished manuscript, on file with author).
\[192\] See CHALLENGES AND EFFORTS, supra note 171, at 21. The U.S. General Accounting Office has requested that DHS create a comprehensive plan for national infrastructure by December 2004. Id. at 8.
adopting its own program of cybersecurity.

Like their U.S. counterparts, Australian businesses are legitimately concerned about sharing information regarding system vulnerabilities with the government because of a fear that the government might disclose their cyberweaknesses. They would rather maintain a good reputation among consumers and investors with respect to their cyberstrength and address threats on their own, rather than risk exposing their vulnerability to the public. Australian businesses should not have to choose between their reputations and their cybersecurity. Legislative bodies should provide corporate privacy safeguards such as an additional AusFOIA exemption for this specific type of security-related information. While it is true that existing AusFOIA exemptions, like their U.S. FOIA counterparts, may apply to business information voluntarily shared with the government, the inertia of business reticence to share information could be more effectively overcome if the exemptions were clarified. If corporate information shared with the government as part of a security effort is given a specific AusFOIA exemption, corporate concerns regarding misuse of such information would no longer serve as a justification that businesses could use to resist security-related information-sharing plans. This approach was used in the United States, with a specific U.S. FOIA exemption given in the DHS Act to private-sector infrastructure information shared with the government.

The second preliminary concern facing Australian businesses is the level of government involvement in private-sector information-sharing. While government regulation is generally considered a hindrance to corporate success, a system of purely voluntary information sharing has been lethargic at best in the United States and would likely have a similar effect in Australia. Nevertheless, the U.S. approach to identifying specific infrastructure sectors and creating an ISAC hierarchy among them has promoted at least some semblance of organization to the U.S. cyber-protection effort, especially with the creation of DHS. DHS has brought together the previously fragmented infrastructure-protection groups and organized them into a single, yet multi-layered, web of cybersecurity offices.

---

193 See INFORMATION SHARING RESPONSIBILITIES, supra note 128, at 18 (arguing that government-led organization of critical infrastructure industries has supported better communication and actual information sharing, but further efforts are still needed to meet all the challenges).

194 The efficiency promoted by centralization of resources, as seen in the DHS example, has also led some to suggest that the United States, like Australia and other countries, should create a federal privacy agency. William S. Challis & Ann Cavoukian, The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective, 19 J. MARSHALL J. COMPUTER & INFO L. 1, 36 (2000). This argument is
At this time, Australia does not have a federal department devoted to security issues. While the creation of a department like DHS could result in more effective communication and clearer delineation of roles in Australia’s infrastructure protection efforts, the mere creation of such a department has not produced complete compliance with critical infrastructure protection plans in the United States. With or without a federal security department, Australia should recognize that an element more crucial to successful information sharing in the United States has been the balancing of corporate self-regulation and government-enforced compliance.

Although increased cyberstrength could be an incentive for businesses to share information on network vulnerabilities, U.S. businesses have been reluctant to invest in critical infrastructure protection. Using the U.S. energy sector as a working model of infrastructure protection, however, demonstrates that cooperative regulation between the public and private sectors is possible. This is especially true when the private sector is actively involved in the creation of its own standards that can be implemented and enforced by the government.

The Australian government should mirror this cooperation in its own critical infrastructure sectors as a preliminary step toward complete security. Australia itself has used such a model of cooperative regulation in its private sector privacy legislation. While the cooperative regulation method has its critics, it does serve as a first step toward effective critical infrastructure protection, and the level of federal regulation could be increased if early efforts prove ineffective. The self-certification process for corporate cybersecurity allows for corporate autonomy, but also meets the government’s interest in furthering the awareness and implementation of critical infrastructure protection. Self-regulation is a step toward greater awareness of the problems inherent in networked critical infrastructure computer networks. Because Australia has used self-regulation systems in other areas of cyberspace and privacy, it should apply the same regime to

---

195 See CHALLENGES & EFFORTS, supra note 171, at 19 (suggesting that businesses do not focus on cybersecurity because they believe cyberattacks are rare, and thus possibly expensive protection plans are not economically justifiable).

196 Australia has also used a self-regulation system in its laws on restricted adult content on the Internet. See Ulrich Sieber, Responsibility of Internet Providers: Comparative Analysis of a Basic Question of Information Law, in LAW, INFORMATION & INFORMATION TECHNOLOGY 231-92 (Eli Lederman & Ron Shapiro eds., 2001).

197 See, e.g., Sieber, supra note 196, at 265; KLAUS GREWLICH, GOVERNANCE IN 'CYBERSPACE': ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS 292-297 (1999).

198 See Kohel, supra note 92.
critical infrastructure protection in order to provide greater security.

As soon as possible, Australia should take initial steps to identify lead organizations in each sector (like NERC in the U.S. electricity sector) and then direct members of each sector to meet and draft standards among themselves. Dividing the sectors into industry specific ISAC-like units is crucial to the fostering of open communication within industries; the information-sharing should be mostly between businesses of the same sector to promote not only effective conversation but also to limit the amount of information that eventually is shared with the government.

VII. CONCLUSION

While not all of the U.S. sectors have reached full compliance with their respective critical infrastructure protection program at this point, the progress the United States has made in at least two areas should be mirrored in Australia. An AusFOIA exemption for corporate information shared with the government for cybersecurity purposes could, like the exemption added to the U.S. FOIA, reassure the private sector that the government respects corporate privacy. AusFOIA already contains a list of exemptions, so an additional exemption could be added without disrupting the statutory scheme.

The United States has also made some progress in developing public-private partnerships, which provide mechanisms for setting standards and enforcement. Although the private sector is loath to be subjected to increased government regulation, the U.S. system of ISACs has produced a minimally intrusive method of encouraging cybersecurity efforts. Australia should work to create a similar system to allow its various sectors to create their own standards for compliance and methods of enforcement before resorting to stricter government regulation.

In the arena of critical infrastructure protection, a federal government must balance private sector privacy and competitive strategy against the public interest in preventing cyberterrorism. Although this balance has been debated in the United States for years, the U.S. model has not yet been perfected. Even without success in all areas of critical infrastructure protection, however, the United States has been working in this arena for years already, and Australia can learn from this experience of both success and challenge in developing its own infrastructure protection strategy.