TOWARDS A CENTRE

FOR

CRITICAL INFRASTRUCTURE

PROTECTION

11 JUNE 2001

TOWARDS A CENTRE FOR CRITICAL INFRASTRUCTURE PROTECTION

EXECUTIVE SUMMARY

This report follows from the previous NIIP report on protection of critical infrastructure from cyber-threats, written in December 2000. As recommended in that report, officials have investigated setting up a centre for critical infrastructure protection in New Zealand. This report is the result.

This report recommends that Government set up a Centre for Critical Infrastructure Protection (CCIP) because:

- People and businesses in New Zealand are highly dependent on various infrastructure services
- These services are themselves operated or managed by IT systems, which are vulnerable to a rapidly changing array of threats over the Internet and through dial-up access.
- There is an increasing risk to businesses of damage through the activities of virus writers and "hackers", many of whom are not in New Zealand and may not be traceable.
- The risk is increasing and this trend is likely to continue.
- A CCIP will ensure that infrastructure operators and government agencies are kept up to date on vulnerability and threat information and are given the best advice and tools to manage the associated risks.

The US, Canada, UK and Australia (among other countries) have set up, or are setting up, equivalent centres because they perceive a risk to their citizens, businesses and international reputations.

The New Zealand CCIP would provide a free service to infrastructure owners, government agencies, and to some extent to the New Zealand public. It would provide timely and relevant information about viruses, denial of service attacks, newly found flaws in software, and IT security issues in general. It would build strong relationships with overseas counterparts, with law enforcement and with infrastructure owners.

The CCIP's functions would be divided into three groups: a 24 hour watch and warn function; an investigation and analysis function; and an outreach and training broking function.

Its location is constrained by the need to give private sector companies the confidence that their sensitive commercial and security information will be adequately safeguarded, and by the need to provide a secure environment to adequately protect intelligence information to which the CCIP must have access. Various government departmental homes have been considered. The recommended location is within the GCSB, which already has significant IT security skills and a culture of security.

The total cost of the CCIP would be approximately $1million / pa plus $300,000 capital. It is recommended that this be centrally funded, as are all overseas counterparts since restricting membership by means of a subscription would not meet the objective of gaining as wide an uptake among infrastructure owners as possible.

The timeframe for implementation, if approved, is 1 October 2001 for starting the establishment phase, with operations starting in January 2002, and being fully operational by 1 March 2002.

INTRODUCTION

Purpose of this Report

The National Information Infrastructure Protection (NIIP) project was initiated in October 2000 as part of the then newly-formed E-government Unit in the State Services Commission. The aim of the project is to improve the protection of New Zealand's critical infrastructure from information–borne threats ("cyber-threats").

The project team presented a report in December 2000 entitled *Protecting New Zealand's Infrastructure from Cyber-Threats*[1]. This report described the threats to the critical infrastructure (defined below) and provided recommendations to protect against them, including:

> The E-government Unit should investigate the establishment of a New Zealand-based security monitoring and incident handling organisation.

This report fulfils that recommendation.

Critical Infrastructure

By *critical infrastructure* this report means infrastructure necessary to provide critical services. Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement.

From an analysis of overseas studies[2] and the New Zealand situation, the December 2000 report identified New Zealand's critical infrastructure as those assets and systems required for the maintenance of: governance including law and order and national and economic security; telecommunications and the Internet; energy including electricity generation and distribution and the distribution of oil and gas; finance and banking; transport; and emergency services.

Some of the infrastructure required to deliver critical services is directly concerned with the transmission and manipulation of information (e.g. the telecommunications network). Other infrastructure areas make extensive use of networked information technology (IT) in their management and control systems. In principle, such areas of infrastructure are subject to IT-borne threats. Infrastructure operators are aware of this and, to varying degrees, have taken steps to mitigate the risk of infrastructure failure due to these threats.

Process Undertaken

Since its previous report, the NIIP project team has researched overseas models for critical infrastructure protection, discussed the issues with public sector and private sector infrastructure owners, and consulted various government agencies about possible structures. The proposals presented in this paper reflect the consensus from the Team's research and consultation, and fit well with international initiatives to combat the ever-growing incidence of cyber-attack.

---

[1] Available on the Internet at *http://e.govt.nz/projects/niip/index.php3*

[2] E.g. President's Commission on Critical Infrastructure Protection – Critical Foundations: Thinking Differently, Oct 1997

PROTECTING NEW ZEALAND'S CRITICAL INFRASTRUCTURE

New Zealand's critical infrastructure, and the information-borne threats to it, is described in the December 2000 NIIP report. Research undertaken since that report has highlighted various risks, in particular:

- the lack of management-level understanding of the need for audited IT security;
- the impact of ongoing denial of service attacks;
- a sharply increasing number and types of attacks being perpetrated over the Internet; and
- the near-impossible task facing IT systems administrators who need to maintain security as vulnerabilities continually emerge in widely-used software.

Responsibility for Infrastructure Protection

Owners of infrastructure are responsible for its security and protection. In particular this covers ensuring that adequate safeguards are in place to mitigate the threat loss of service due to cyber-attacks. Owners have commercial and other incentives to ensure its continuance. However, shareholders (or their board) might decide, for example, to pursue commercial advantage through attempting a hostile acquisition of a rival and become distracted from the engineering necessary for risk management. This is possibly more likely in instances where the customer has no real choice, which is often the case for critical infrastructure providers. Therefore commercial incentives may lead to a lesser level of infrastructure protection than is appropriate, particularly where a de facto monopoly exists. Government departments are effectively monopoly providers of various services also.

Government, as a proxy for New Zealand's people and businesses, has a strong interest in ensuring that critical infrastructure is adequately protected. Furthermore, our critical infrastructure exists in a technical environment which is increasingly interconnected and harbours changing threats. It is reasonable therefore for Government to seek answers from infrastructure owners about the extent of their efforts to protect infrastructure, and to provide such support as it is best positioned to.

The Case for a Centre for Critical Infrastructure Protection

The CCIP is proposed as an insurance measure in that it mitigates, for a low cost, a risk of a large loss.

Telecommunications and the Internet open business to a range of evolving threats, many of which are poorly understood. For example, in the last two years:

- Many businesses, including some New Zealand Government departments, were infected by the Melissa and ILOVEYOU viruses. This caused business and government disruption worldwide. Cost estimates range from hundreds of millions upwards.
- Denial of Service attacks crippled Internet businesses Amazon and eBay in February 2000. They were eventually found to be the work of a single teenager.
- In May 2000, an Australian computer hacker compromised the IT-based controls of a water system and caused the discharge of raw sewage into waterways on the Sunshine Coast.

- In July 2000, two computer programmers from Kazakhstan breached security on the global Bloomberg financial information network and tried to extort money from its owner.
- Since early this year, a large telecommunications company in New Zealand has come under sustained attack from an unknown opponent on the Internet, causing degraded service on the Internet in New Zealand.
- In April-May US and Chinese hackers engaged in a 'cyber-war' defacing numerous government and business web sites.

The vulnerability of New Zealand's critical infrastructure to attack over the Internet or via dial-up from anywhere in the world was established in the previous NIIP report.

Disruptions to critical infrastructure would at the very least inconvenience many thousands of New Zealanders, damage businesses and threaten employment. New Zealand would suffer damage to its reputation as somewhere to do business. At the other end of the scale, disruption to health, emergency or transport infrastructure could prove life –threatening.

The e-world offers new ways of serving customers and doing business. It also brings with it threats and risks. Keeping up with those threats and protecting against them is a significant issue for everyone who uses computers, particularly infrastructure providers and Government. A central capability to share timely security information with infrastructure owners and support them to make their systems safe can greatly reduce the likelihood of a major incident.

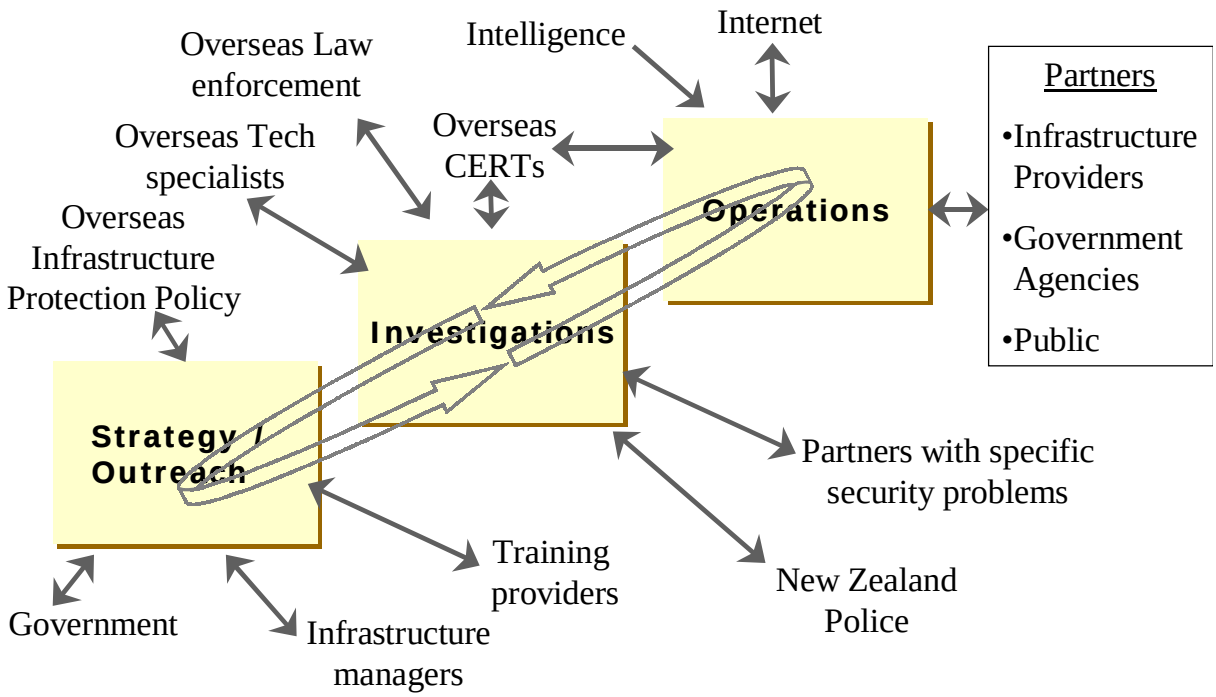
The proposed CCIP would mitigate the risk of infrastructure disruption by raising the skills and awareness of management and technical staff in infrastructure owners, and by providing timely information about risks, threats vulnerabilities. It might also reduce the number of attack through deterrence by improving the likelihood of identifying malefactors.

Other countries have moved to manage this risk already. The US, Canada and the UK all have infrastructure protection centres with the functions proposed for New Zealand operating now. Australia is planning one. These countries would welcome New Zealand co-operation in dealing with this global problem.

PROPOSED CENTRE FOR CRITICAL INFRASTRUCTRE PROTECTION

Functions and Relationships of the CCIP

The diagram below shows the functions of the proposed Centre for Critical Infrastructure Protection, its partners and main relationships.



Partners of the CCIP

The clients of the CCIP would be referred to as partners, as a reflection of their status as contributors of information as well as consumers.

In order of the level of service given, partners of the CCIP are proposed to be:

1. Critical infrastructure owners and operators, whether in the public or private sectors.
2. Government agencies not covered above.
3. The New Zealand public in general.

The relationship with partners is proposed to be somewhat different for each group. Critical infrastructure owners would be treated as partners, and possibly described as such. The intention would be to build confidence in the ability and integrity of the CCIP, and to encourage them to share confidential security information.

Government departments would be required to be partners of the CCIP and would be expected to provide IT security contacts to receive warnings and contribute information about IT based threats and incidents. Agencies in the wider state sector and local authorities would be encouraged to become partners also.

The New Zealand public at large would have access to a CCIP web page which would be kept up to date, summarising generally available information about IT threats and holding statistics and other resources useful to improve security.

Functions of the CCIP

CCIP functions are broken into three groups below. These represent a notional structure for the CCIP itself; although there is no necessity for its internal organisation to be along these lines.

Watch and Warn

The Watch and Warn function is a 24-hour function which watches developing threats, risks and vulnerabilities and warns the relevant staff in critical infrastructure operators and government departments. It provides a focal point for timely information about viruses, hacking attacks and newly discovered flaws in computer programs in New Zealand.

Its information would be derived from many sources, including from the open Internet, through relationships with counterpart organizations in other countries, from intelligence sources, and from its clients themselves.

When dealing with an incident, this function would liaise with counterpart organisations, with Internet and telecommunications providers, and with law enforcement agencies in New Zealand and overseas during the course of an incident. It would provide a point of contact for overseas agencies to contact New Zealand for incidents originating or passing through New Zealand, showing that IT attacks are taken seriously here.

As well as its warning and monitoring function it would provide a central point for Government to obtain an overall picture of the impact of an IT security scare on New Zealand as a whole, and on Government departments in particular. It would compile statistics on it attacks for New Zealand.

Investigation and Analysis

The investigation and analysis function would provide a way for threats and attacks to be researched, understood and catalogued. It would offer the capability for considered analysis of an attack, generally after the event.

Outreach, Strategy and Training

In this context, "outreach" means making contact with senior management of actual and potential client organisations and convincing them of the benefits of sharing information.

There would be a large international dimension to this function. The success of the CCIP would depend on it building relationships and credibility with overseas equivalents. The CCIP would need to negotiate terms of co-operation, and consider other jurisdictions when setting strategy. CCIP policies would need to be formulated to address international issues such as overseas requests for co-operation in respect of attacks apparently originating in New Zealand.

The training function would involve providing a "training broking" service, aimed at getting information security staff in client organisations access to approved high quality training in detailed

security issues.

Issues on CCIP Structure

Hours of Operation

The CCIP needs to deliver at least apparent 24x7 service – meaning that urgent contacts are answered whatever the time of day. Attacks occur frequently outside normal business hours, and vulnerabilities are discovered at any time and in any place. Even were it not for the nocturnal habits of some attackers, the global nature for the Internet and telecommunications environment makes it necessary to provide continuous cover.

This would require, at minimum, a seamless transfer of incoming contacts to an existing 24 hour centre – which would need security knowledge and clearances. Ideally, the CCIP would itself need to be staffed to provide a full 24x7 shift system. Unless located within another agency which already hosts 24x7 operations, this would require a minimum of two people present at all times on safety grounds.

The options for providing out of hours cover are explored as part of the local options below.

Access to Intelligence

Timely access to classified intelligence, among other sources, would be necessary to provide the greatest likelihood of successfully warning of a threat. This is the model used by other countries in respect of critical infrastructure. Relationships with counterpart organisations, which are necessary for effective operation, would be compromised if the centre did not have this access.

Having such access would require adequate physical security, and staff would need to be security cleared. These are requirements for prudent management of a CCIP in any case.

Forgoing intelligence access would thus harm the effectiveness of the CCIP without dramatically reducing costs. It will not be considered further.

Technical Support

The CCIP will need a high level of technical skills in house and available to it. Regardless of the location of the unit, the GCSB will need to be involved in the set up and ongoing operations of the unit, in order to provide the level of IT security skills required to protect the classified intelligence used within the unit, and potentially to assist with detailed analysis as needed. The unit and the GCSB will need to work closely together.

Options for Locating a CCIP

The CCIP would need to gain the confidence of private sector infrastructure owners that their sensitive security information is treated confidentially. It would also, as discussed above, need access to intelligence. Both of these point toward it being located in a part of central government.

The following location options are assessed below:

- A separate Department
- Department of the Prime Minister and Cabinet (DPMC)
- New Zealand Police
- Ministry of Emergency Management (MEM)
- New Zealand Defence Force (NZDF)
- SSC
- SSC with out of hours cover in GCSB
- GCSB

Analysis of these options is driven by the criteria of:

- **Effectiveness**, i.e. how well the proposed structure will permit the CCIP to achieve its objectives. This depends on the skills, tools and information available to the CCIP.
- **Perception** of the CCIP by partners, potential partners and overseas counterparts, especially in the areas of confidentiality and technical credibility. This is completely crucial to the effectiveness of the organisation. Although this criterion could be seen as just a component of overall effectiveness it is assessed separately because it is influenced by different factors from the other components.
- **Least cost**. Major cost drivers are the need for 24x7 operation and the security arrangements required.

Option	Benefit / Opportunity	Risk / Threat	Summary
Separate Department	+ Clarity of purpose with full focus on infrastructure protection + No other departmental distractions	– Runs counter to political direction; Cabinet has signalled intention to reduce number of agencies – Lead-time to operational effectiveness. Must build up organisation and credibility with 'partners' – Highest set-up and operating costs, PFA and infrastructure implications	Effectiveness MEDIUM Perception LOW Cost HIGH
DPMC	+ EAB already within DPM&C + DPM&C has some secure infrastructure	– Not an executive function, not core business – DPM&C not an operational Department, would be significant expansion of function – CCIP has little to do with servicing PM or Cabinet	Effectiveness MEDIUM Perception LOW Cost MEDIUM

Option	Benefit / Opportunity	Risk / Threat	Summary
Police	+ Tight linkage between computer crime and law enforcement. + CCIP investigative function complementary to existing police computer forensics function + CCIP likely to provide useful assistance to computer crime investigations + Security at least partly in place already	– Overseas experience shows collocation of law enforcement and CCIP as very poor fit. – CCIP functions may be subjugated to evidential / law enforcement needs – Powers of prosecution and so potential disclosure of sensitive / commercial information may lead to distrust by infrastructure owners, damage effectiveness – Forensics needs of CCIP may take lower priority to police requirements	Effectiveness MEDIUM Perception LOW Cost MEDIUM
MEM	+ CCIP / MEM mix consistent with Canada, and potentially UK (but not for some time, and UK question if Emergency Preparedness is yet ready) + MEM well focussed on business continuity processes + MEM already has organising, facilitating and training role for national and local emergencies	– Would be a major extension to MEM's traditional roles. – No inherent skill sets or structure for handling IT-related threats / attacks – Security issues – staff clearances, building security (hard in present ground floor location), communications links – How would mix of public and secure operations be managed?	Effectiveness LOW Perception MEDIUM Cost HIGH

Option	Benefit / Opportunity	Risk / Threat	Summary
NZDF	+ Protection of critical infrastructure is one of five key objectives of Govt's defence policy + Cyber space is 5th operational domain in military doctrine + Could be included in 7x24hr HQ NZJF structure + Canadian model has Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) within Department of National Defence	– Not core business for NZDF; role is defence against attack on infrastructure elements – Required skill sets different from traditional NZDF skills; could be accorded lesser priority during times of heightened operations – Can function be sustained & funded against other priorities & pressures? – NZDF not involved in 'information operations' (Info Ops); MOD is examining issue – Is function liable to be subjugated to Info Ops? Confusion between protective function (CCIP) and war-fighting role (Info Ops) - Civilian operational unit not a natural fit in NZDF Operational HQ - Could necessitate increased accommodation for HQ NZJF - Canadian siting due to historical associations, not necessarily appropriate to NZ	Effectiveness MEDIUM Perception MEDIUM Cost MEDIUM
Wholly within SSC	+ Already has cross-government function + If portal is managed from SSC, CCIP (and other operational items such as E-proc, SEE) could be incorporated within a single SSC operational unit	– SSC is not an 'operational' organisation, although portal will presumably need 7x24 staffed operation which might be managed within SSC. – Security issues – staff and building, mix of public and secure operations – SSC perceived as bureaucratic organisation? – Not core SSC business	Effectiveness HIGH Perception MEDIUM Cost HIGH

Option	Benefit / Opportunity	Risk / Threat	Summary
SSC, with out of hours cover in GCSB	+ Already has cross-government function + SSC already manages NZGO + E-procurement and SEE will also need ongoing admin / management + If portal at SSC, CCIP (and E-proc, SEE?) readily could be incorporated within a single SSC operational unit	– SSC is not an 'operational' organisation. – Security issues – staff and building, mix of public and secure operations – Discontinuities between contacts in –hours and out-of-hours; will be harder to manage and harder to form relationships with partners and overseas counterparts – Potential for negative public perceptions	Effectiveness MEDIUM Perception LOW Cost HIGH
Wholly within GCSB	+ Already has secure environment, staff all security cleared, has 24x7 operations and secure comms with overseas agencies. + Has necessary skill base. CCIP function is natural fit / compatible with GCSB Infosec Output + GCSB technical support is essential to CCIP function wherever sited + CCIP could / would be discrete Output Class. GCSB currently revising output classes. + Would be perceived to offer highest level of confidentiality for partners' information shared with CCIP.	– Potential for negative public perception (could mitigate by launching alongside new image for InfoSec function). – GCSB support is required for all options. This option alone makes GCSB involvement overt.	Effectiveness HIGH Perception HIGH Cost LOW

Recommendation

Based on the above the recommended location for the CCIP is **within the GCSB**.

COST OF CENTRE FOR CRITICAL INFRASTRUCTURE PROTECTION

Who should pay for the CCIP?

There are two options:

1. The CCIP's clients, or
2. Central government.

The CCIP will be most effective if it gets 100% uptake from infrastructure owners. It will need co-operation from infrastructure owners – that is, acceptance of partnership status – if it is to be able to provide the best information to assist them to protect themselves. It will also need a wide base of New Zealand organisations contributing information to gain quality information on actual attacks and threats. There is an element of the network effect: the greater the CCIP's coverage, the more use it will be to those it covers. Complete coverage of infrastructure owners is unlikely if a subscription model is employed. Those who might baulk at paying could be those who have the lowest appreciation of cyber-security issues.

Central funding of the CCIP by Government would reflect the Government's interest in ensuring that critical infrastructure is protected from developing threats, and that accountability for infrastructure protection rests with its owners. The equivalent bodies in the US, the UK and Canada all provide a free service to critical national infrastructure owners, and are centrally funded.

Government agencies are expected to be partners of the CCIP, but they will remain individually responsible for ensuring that their systems are adequately protected. The CCIP's services will assist the agencies, but they will need to maintain, or perhaps even increase, their ongoing expenditure on security. Requiring then to pay for the CCIP without an increase in baselines would result in agencies being expected to more with less.

Finally and perhaps most importantly, every individual in New Zealand is reliant on the services and facilities provided by or over the critical infrastructure and government has an obligation to ensure that these services and facilities remain available. For example, loss of the national power grid through cyber-attack would immediately assume the status of a national disaster. The cost of recovery would greatly exceed the cost of the 'insurance' of the CCIP.

The arguments in favour of central funding are sufficiently strong that a subscription model is not explored further.

Cost of the CCIP

A comprehensive budget cannot be prepared without detailed consultation with GCSB and Treasury. However, indicative costs suggest that the CCIP can be operated at a charge of about $1 million/year as shown in the following summary. Note that the FY01/02 estimates include set-up costs with staff joining progressively from September 2001 with full operational status being achieved in January 2002.

	FY 01/02	FY 02/03 and out years
Personnel	200	610
Operating	180	290
Capital	290	20

These figures are for the recommended option of a centre wholly within GCSB. Other possibilities have been costed, and are more expensive.

CONCLUSION

There is widespread evidence that the incidence of cyber-attack over the Internet is increasing at a substantial rate. To meet this threat New Zealand's major trading partners are implementing national centres aimed at detecting and analysing threats and providing early warning to potential target organisations. As was evidenced during the Y2K transition, New Zealand occupies a unique place in the world and a New Zealand centre for infrastructure protection would be welcomed as part on an international effort to combat cyber-threats.

This paper proposes that a Centre for Critical Infrastructure Protection be established within the Government Communications Security Bureau and that the Centre be centrally funded. The indicative cost for such a Centre, which will be extremely modest in comparison with overseas equivalents, will be in the order of $1 million.

RECOMMENDATION

Subject to the Minister's acceptance of the proposal it is recommended that:

a the E-government Unit be directed to prepare a Cabinet submission seeking approval to proceed with the establishment of the CCIP.

APPENDIX 1 - INTERNATIONAL CRITICAL INFRASTRUCTURE PROTECTION ARRANGEMENTS

This section of the report provides an overview of CCIP arrangements in other nations with which New Zealand traditionally has close ties. Information in this section is drawn from discussions with a number of the organisations during a recent visit by the Project Team, augmented from open source information. As an overall comment, no nation has yet got its CCIP structures totally effective (and given the nature of the problem CCIP is going to dictate evolutionary structures), but all nations are committed to the need for such entities. New Zealand is not far behind, but is uniquely placed to learn from the experiences of her friends.

United States of America

National Infrastructure Protection Center (NIPC)

The NIPC was established within the FBI in February 1998 in response to Presidential Decision Directive 63. Its mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures. It brings together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect the national critical infrastructures. Its functions are to:

- detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target critical infrastructures;
    - manage computer intrusion investigations;
    - support law enforcement, counter-terrorism, and foreign counter-intelligence missions related to cyber crimes and intrusion;
    - support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests; and
    - coordinate training for cyber investigators and infrastructure protectors in government and the private sector.

The NIPC has three functional units:

- The Computer Investigations and Operations Section (CIOS), responsible for coordinating and supporting computer intrusion investigations, providing and coordinating technical support to investigations involving computers and information technologies, and for managing a Cyber Emergency Support Team which helps respond to a cyber attack.
- The Analysis and Warning Section (AWS) is the hub for public-private sector information sharing and analytical work. It provides assessments and analyses of foreign and domestic threats, exploited vulnerabilities, and exploitation techniques. It provides direct analytical support for computer investigations, and serves as the information clearinghouse for research and analysis and unlawful acts on the nation's infrastructures It also has a 24-hour, 7-days a week Watch Operations Center which maintains connectivity with national and international partners to detect cyber threats and disseminate timely assessments, alerts and advisories.
- The Training, Outreach, and Strategy Section (TOSS) supports training and continuing education of cyber investigators in federal, state and local law enforcement agencies; and of personnel in the public and private sector involved in infrastructure protection. It also coordinates outreach efforts between government agencies, industry, and

academia, which are necessary to encourage the sharing of information about foreign and domestic threats, vulnerabilities, and technological developments.

Information Sharing and Analysis Centers (ISACs).

Private-sector, industry-based ISACs are essential components of the US Government's critical infrastructure protection strategy. Their function is to gather and analyse industry-provided information on threats and incidents and to share this information with government entities, particularly with the NISC. ISAC members also have access to information and analysis relating to information provided by other members and obtained from other sources, such as other vertical sector ISACs, law enforcement agencies, technology providers, and security associations such as CERT. The Millennium Solution Center ISAC (MSC-ISAC) is serves the US Government sector.

Response Organisations

There are a number of separate agencies, in government, industry and academia, that contribute to CCIP. The function of these organisations is more targeted at responding to incidents rather than taking on a NISC-type role, but they are all complementary to the overall mission of CCIP. These organisations include:

Computer Emergency/Incident Response Teams (CERTs).

The original CERT, now CERT®/CC, was established at Carnegie Mellon University. It is a center of Internet security expertise and is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT®/CC studies Internet security vulnerabilities, responds to computer security incidents, publishes a variety of security alerts, undertakes research for long-term changes in networked systems, and develops information and training to help improve security at customer sites. A network of some 70 CERTs now extends throughout the world with AusCert at Brisbane being the nearest to New Zealand (see below).

Federal Computer Incident Response Center (FedCIRC).

The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government. It provides the means for Federal agencies to work together to handle security incidents, share related information, solve common security problems and to collaborate with the NIPC for the planning of future infrastructure protection strategies and reaction to activities that pose a threat to the critical infrastructure. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense, Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments into a virtual security team.

Australia

The cornerstone of the Australian Commonwealth Government's approach to infrastructure protection is the development of a secure and trusted electronic environment with the primary responsibility for critical infrastructure protection assigned to the Attorney-General's Department. An updated threats and vulnerabilities assessment is now being finalised and major recommendations to government on the way ahead are in preparation. It is reasonable to assume that these recommendations will build on the 1998 Interdepartmental Committee recommendation that a formal structure be established to coordinate infrastructure protection.

AusCERT. In additional to government initiatives the Australian Computer Emergency Response Team (AusCERT) operates as an operational arm of the University of Queensland. AusCERT began operations in 1993 and acts as a coordinating centre, advisory capability, centre of expertise and a portal to its contacts throughout the world. It is funded primarily through membership fees, with some additional income from value added services such as research, training and education. It has a strong focus in the Asia-Pacific region and is recognised throughout the world for its expertise. AusCERT's mission is to support and improve community awareness, representation and communication regarding computer security, both locally and internationally, by being the leading source of impartial and reliable computer security information and expertise for our members.

United Kingdom

National Infrastructure Security Co-ordination Centre (NISCC)

NISCC is an interdepartmental organisation set up to co-ordinate and develop existing work within Government departments and agencies and organisations in the private sector to defend the CNI against electronic attack. NISCC operates under a Director, who is a member of a Management Board chaired by the Home Office. The other members of the Board are drawn from the Cabinet Office, CESG, the Security Service, MOD and the Police. NISCC's small core staff are from various parent departments contributing to the CNI protection programme. It co-ordinates a programme of work consisting of activity carried out by its core staff, and work carried out under the auspices of various government departments (but contributing directly or indirectly to the overall CNI programme)

NISCC is responsible for co-ordinating:

- dialogue with owners of CNI systems to identify the most critical systems and work with them to reach a level of assurance about the protection of these systems;
- alerts or warnings of attack;
- assistance in response to serious attacks;
- information about the threat;
- specialist protective security advice and expertise;
- NISCC aims to establish partnerships with CNI providers and is not regulatory.

One of the main purposes of the NISCC is to establish a long term partnership with those companies that provide CNI services in order to help protect them from electronic attack. To maintain the continuing provision of CNI services supported by IT systems, it is essential that appropriate and proportionate protective security measures are in place and that staff are aware of the risks and are well-trained. Where appropriate, NISCC will help CNI companies protect those systems which are a part of the CNI. NISCC aims to build a lasting relationship, so will continue to provide updated advice and threat information as the threat develops and as dependency on interconnected IT systems grows.

Unified Incident Reporting and Alert Scheme (UNIRAS)

UNIRAS is run by NISCC and draws on technical support from CESG, the UK national technical security authority. Its original customers were government departments and agencies. Recently this has been expanded to include companies holding sensitive Government contracts, and most recently CNI organisations. It:

- receives reports of significant electronic attack incidents, threats, new vulnerabilities and countermeasures from its customer base and other commercial, Government and international sources. It then validates, sanitises (where appropriate) and disseminates the information back to its customers through e-mail alerts and warnings
- provides a helpdesk for its customers, giving advice on IT security incidents, particularly Internet-related problems;
- co-ordinates the NISCC's Electronic Attack Response Group (EARG), which responds to serious electronic attack incidents affecting the CNI;
- is the UK Government CERT (Computer Emergency Response Team) and is an active member of the international Forum of Incident Response and Security Teams (FIRST);
- collates reports on IT security incidents supplied by its customers and issues regular statistics. These reports are suitably sanitised to protect commercial or departmental sensitivities.

Canada

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

In April 2000, drawing on lessons from the Y2K roll-over period, the federal government created an interdepartmental Task Force housed in the Department of National Defence with the mandate to develop proposals for a national critical infrastructure protection policy framework. The Task Force held extensive consultations with the private sector, other levels of government, and with international partners, including the United States. In February 2001 the Prime Minister announced the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness. OCIPEP reports to the Minister of National Defence and encompasses the previous functions of Emergency Preparedness Canada.

OCIPEP is to develop and implement a comprehensive approach to protecting Canada's critical infrastructure, and provide provide national leadership to help ensure the protection of this infrastructure - in both its physical and cyber dimensions and regardless of the source of threats and vulnerabilities. The Office will also be the government's primary agency for ensuring national civil emergency preparedness.

The functions of OCIPEP are to:

- build partnerships with the private sector, the provinces, territories and municipalities, and key international partners, the US in particular;
- promote dialogue among Canada's critical infrastructure owners and operators and foster information sharing on threats and vulnerabilities;
- provide a focal point for the federal government's own cyber incident analysis and coordination efforts and support federal departments and agencies in meeting their responsibilities for protecting their IT systems and networks;
- promote other areas of cooperation such as raising awareness, enhancing education and training, and promoting information technology security research and development; and achieve an appropriate level of national civil emergency preparedness.

In announcing its establishment the Prime Minister stated: “The creation of this Office accords closely with government priorities in three areas: Connecting Canadians, Government on Line, and Strong and Safe Communities. The success of E-commerce and Government on Line will depend on establishing consumer and client trust in the security and privacy of information networks and their information exchanges. Strong and safe communities will benefit from assured emergency and government services and from the ability of law enforcement to deal with serious crime, including cyber-crime. The Office will support the efforts of those engaged in implementing these priorities.”