

11 February 2001

Hon. Trevor Mallard

**MEDIA STATEMENT:**

**Government Addressing Cyber-Crime & IT Based Threats**

State Services Minister Trevor Mallard has ordered a programme of work to improve protection for New Zealand's critical infrastructure from cyber-crime and other IT-based threats such as computer "hacking" and viruses.

Trevor Mallard said the programme was aimed at anticipating risk, improving protection, and guarding against IT-based risks that could have an impact on New Zealand's national welfare or New Zealand's international standing.

Trevor Mallard said the programme included:

- Determining whether New Zealand should have its own unit to monitor IT security and risks on a day to day basis, and to provide advice and training on securing infrastructure from cyber-attacks.
- Advice to the Government on potential improvements to New Zealand law, and New Zealand's role in international treaties, particularly to outlaw 'denial of service' attacks over the Internet. The Ministry of Justice is already considering legislation on this matter.

The Minister said he had received a report – prepared by the State Services Commission's E-government Unit – that assessed the main cyber-risks to New Zealand's critical infrastructure.

The report assesses levels of risk due to IT-based threats in finance and banking; transport; electric power; telecommunications and the Internet; oil and gas; water; and critical State services that support national safety, security, and income.

Trevor Mallard said the overall picture painted by the report was encouraging.

"Nonetheless, I have drawn the report to the attention of Ministers responsible for agencies or departments discussed in the report, so that they can seek reassurance as to levels of risk and measures to address that risk, where they see it necessary.

"I anticipate that some Ministers will seek reassurance from agencies for which they are responsible that they are prudently managing these risks.

"The most important thing is that New Zealand takes steps to anticipate risks in this area, and joins the international community in cooperative efforts that will enhance protection of infrastructure and make enforcement easier wherever cyber-crimes are committed."

The Minister said the work that he had already agreed to was part of existing departmental outputs. No extra funding was required.

Trevor Mallard said the report was being made public because the Government believed that citizens should have the maximum amount of information about the management of risks to New Zealand's critical infrastructure.

The report looked at information-based threats to national welfare.

"The immediate role for the Government is to manage the main national risks, to New Zealand and New Zealanders, that come from cyber-crime or IT-based crime," he said.

Attached: Recommended strategy which the Minister has agreed to.

The report is available on the State Services Commission website: [www.ssc.govt.nz](http://www.ssc.govt.nz)

---

### **Reporters, please note:**

- The Minister is available to answer questions on the report between 6.00pm and 7.00pm. Please contact Moerangi Vercoe on 025 270 9194 to arrange.
- Questions on technical points in the report can be addressed to Colin Jackson, State Services Commission, ph 495 6746.

### **Recommended Strategy**

The protection of critical national infrastructure from information related threats is an issue which merits taking notice, and is being taken seriously by other western nations. While owners of critical infrastructure in New Zealand are conscious of the need to protect it, this report has raised some concerns over specific issues. The recommendations below are aimed at providing infrastructure owners with the tools and information they need to protect against information related threats, and to promote cooperation toward a common view of infrastructure protection.

### **Recommendations**

The E-government Unit should investigate the establishment of a New Zealand-based security monitoring and incident handling organization with the following functions:

- provide timely information to critical infrastructure owners and government departments about threats, actual attacks and recovery techniques

- build local capability in incident handling and security research
- monitor global security issues and gather IT security intelligence
- build relationships with similar organisations, e.g. CERT.
- promote cooperation among clients in respect of IT security
- maintain statistics and incident databases
- promote standards and tools for IT security and risk management
- communicate to raise provider and public awareness of computer security issues
- maintain a model security service level agreement for use in outsourcing arrangements
- encourage production and adoption of relevant standards
- facilitate independent security/protection audit capability,

**Rationale:** By providing a New Zealand based centre of expertise the IT security skills and awareness of infrastructure providers and government departments can be bolstered.

Government should consider harmonising computer crime legislation with that of other Western nations and participating in international cybercrime treaties. Furthermore, the Bill on this matter currently before the House should be extended to address denial of service attacks.

**Rationale:** There is currently little deterrent against casual attack on infrastructure. Improving our computer law will help. Furthermore, other jurisdictions are more likely to help with trans-border crime if New Zealand's legislation parallels their own.

The New Zealand Police should consider what is necessary to investigate computer break-ins and related attacks and prosecute perpetrators. This would involve:

- building investigative capability, while maintaining respect for privacy of Internet users; and
- building relationships with law enforcement authorities responsible for pursuing malefactors across national borders and co-operating with other countries who wish to pursue here.

**Rationale:** There is currently little deterrent against casual attack on infrastructure. Improving our computer law will help. Furthermore, other jurisdictions are more likely to help with trans-border crime if New Zealand's legislation parallels their own.

Establish an ongoing cooperation programme between owners of critical infrastructure and Government.

Invite Responsible Ministers to write to critical infrastructure owners asking them to declare their support or otherwise of relevant security standards.

Engage critical infrastructure providers at a senior level on the subject of IT threats to ensure that all infrastructure owners undertake and maintain formal risk analysis and management of information-related and physical threats.

Direct the State Services Commission to review the state of critical infrastructure protection after 12 months.

**Rationale:** This will seek and maintain the commitment of infrastructure-owning organizations to an adequate level of protection, and will show the government's commitment, on behalf of New Zealanders to the issue.

Invite Transpower to lead a power industry infrastructure protection group, possibly as part of the group in recommendation d, to provide knowledge and cooperation in respect of infrastructure protection among power industry players, particularly lines companies.

**Rationale:** This is a highly competitive and technically complex industry with many players, some of whom have effective monopolies over power distribution in large areas. There is little or no evidence of cooperation in security or infrastructure protection matters. Transpower is uniquely positioned to assist the industry.

Through the State Services Commission, direct government agencies to adopt specified appropriate IT security standards.

**Rationale:** As part of the movement toward e-government, the Government needs assurance that its own agencies are taking prudent steps to manage their own IT security. Though many of the large and critical agencies have already adopted relevant IT security standards, there are others who may lack understanding of the issues or technology.