



**Australian Government**  

---

**Attorney-General's Department**

**Security and Critical  
Infrastructure Division**

**Cyber Storm II**  
**National Cyber Security Exercise**  
**Final Report**

# Contents

<b>Executive Summary .....</b>	<b>3</b>
<b>1. Introduction.....</b>	<b>4</b>
<b>2. Background .....</b>	<b>6</b>
2.1 Purpose.....	6
2.2 Concept .....	6
2.3 Scope.....	6
2.4 Objectives .....	7
2.5 Scenarios .....	7
2.6 Media Outreach.....	7
2.7 Planning and Execution .....	7
2.8 Security Policy .....	10
<b>3. Significant Findings .....</b>	<b>12</b>
<b>Annexe A: Participating Organisations.....</b>	<b>19</b>

## Executive Summary

As an outcome of a 2006 review of e-security arrangements, the Attorney-General's Department was tasked to develop a cyber exercise program to improve the ability of governments and critical infrastructure owners and operators to manage incidents affecting the National Information Infrastructure. As part of this role, the Attorney-General's Department coordinated a national cyber exercise, Cyber Storm II.

Cyber Storm II was structured and executed as a large-scale national exercise within an international framework. Canada, New Zealand, the UK and the US were participants. Australia's participation was second only to the United States, and involved Australian Government agencies, state and territory governments and the largest contingent of private sector organisations ever involved in an Australian Government-sponsored exercise. The exercise structure allowed participants to exercise their internal incident response and communications in a national framework that allowed external communications to be more than notional and which encouraged a collaborative response.

Cyber Storm II was conducted as a "no-fault" exercise. Its purpose was not to obtain a stock-take of participant's internal crisis management arrangements. Nor was the exercise a test of the resilience of participant's networks to cyber attack. The starting point for the exercise was that the adversary had sufficient time, money and motivation to penetrate any network.

Many participants recognised that the global exercise framework provided by Cyber Storm II was an extremely cost-effective way of conducting an in-house cyber exercise.

The exercise proved that the major elements of the national response arrangements are sound, but as expected also found a number of areas where improvement would be possible. This report captures key findings and participant's observations as they relate to cyber incident response.

The key findings are that crisis arrangements must be regularly reviewed and tested; established relationships facilitate rapid information sharing during a crisis; crisis communications procedures must be predicated on accurate and appropriate points of contact and formalised; cyber crises require tailored responses that take into account multiple inter-dependencies; and incident response is assisted by having clear escalation thresholds.

# 1. Introduction

Recognising the increasing reliance of government, business and home users on information and communication technologies, the Australian Government established the E-Security National Agenda (ESNA) in 2001 to create a secure and trusted electronic operating environment for both the public and private sectors. As an outcome of a 2006 review, the Attorney-General's Department was tasked to develop a cyber exercise program to improve the ability of governments and critical infrastructure owners and operators to manage incidents affecting the National Information Infrastructure. As part of this role the Attorney-General's Department coordinated a national cyber exercise, Cyber Storm II, which formed part of a larger international exercise and was designed to align with national e-security objectives.

In February 2006 the US Department of Homeland Security (DHS) National Cyber Security Division conducted the first US National Cyber Exercise, Cyber Storm, as part of its own national cyber exercise program. The Australian Government participated in Cyber Storm, conducting a discussion exercise. The second US national exercise was scheduled for March 2008, and the US invited Australia, Canada, New Zealand and the United Kingdom to participate.

Cyber Storm II was structured and executed as a large-scale national exercise within an international framework. This structure allowed participants to exercise their internal incident response and communications in a national framework that allowed external communications to be more than notional and which encouraged a collaborative response. It provided a unique opportunity for stakeholders across the spectrum of e-security and critical infrastructure protection in Australia to participate in a global cyber exercise aimed at testing the decision-making which underpins any technical response. Cyber Storm II participants included Australian Government agencies, State and Territory governments, industry groups and private companies drawn from the IT industry and four critical infrastructure sectors - Water, Banking and Finance, Energy and Communications. Each participating organisation designed their exercise play to meet internal objectives while utilising the international framework and the extensive player set to realistically test their response and recovery to a large-scale cyber attack.

The exercise was conducted from 10-14 March 2008. The Australian component of Cyber Storm II was coordinated by an Australian Exercise Control Centre (AuExCon) established near Melbourne. Participants played the exercise from their usual work places using, where possible, normal communications channels.

This report is a consolidation of findings, observations, and lessons learned throughout the planning and execution of Cyber Storm II. It is a compilation of observations provided by participants in a 'hotwash' debrief held immediately after the exercise, and in more formal one-on-one debriefings conducted in the weeks following the exercise.

There are three points to bear in mind while reading this report:

- i. Cyber Storm II was conducted as a “no-fault” exercise. The purpose of Cyber Storm II was not to obtain a stock-take of participant’s internal crisis management arrangements;
- ii. Cyber Storm II was not a test of the resilience of participant’s networks to cyber attack. The starting point for the exercise was that the adversary had sufficient time, money and motivation to penetrate any network; and
- iii. the findings and supporting comments in this report represent a wide range of opinions from a diverse player set. All are generalised to some extent – some are common observations, others the views of one or two players. This report should be read from the perspective of “could this apply to my organisation” rather than “who said that”.

## **2. Background**

### **2.1 Purpose**

Australia's first national e-security exercise was designed to support the goals of the Australian Government's E-Security National Agenda, encourage information sharing across various boundaries, and importantly, to facilitate participating organisations to meet their own internal objectives.

The exercise enabled participants to test their response and recovery capabilities, test their information sharing arrangements and to promote awareness of e-security within their own organisation. The exercise scenarios were based on participants' objectives and designed to stimulate technical, operational, communication and/or strategic responses to cyber incidents with a view to reviewing and refining current arrangements.

### **2.2 Concept**

Planned in close coordination with, and driven by, its stakeholders and participants, the exercise focused on a series of cyber-specific events which were intended to escalate to a level requiring a coordinated national response. The adversary in Cyber Storm II utilised coordinated cyber attacks on the selected sectors to meet a specific political and economic agenda. A basic assumption within the exercise was that the adversary had sufficient resources and motivation to mount and successfully execute these attacks. The resulting impact on global cyber infrastructure, and associated physical infrastructure, was designed to prompt coordinated responses from the Australian Government and from within relevant industries, and to emphasise the interdependencies that exist in critical infrastructure and the national information infrastructure.

### **2.3 Scope**

The scope of the exercise was defined to maximize the participants' ability to assess, test or validate:

- the full range of incident response and recovery mechanisms (technical, operation and strategic),
- the spectrum of players involved from multiple sectors, across government and the private sector,
- internal and external communications of organisations and sectors and with government, and
- the need for continuing improvement to cyber security procedures and processes.

## 2.4 Objectives

As a stakeholder-driven exercise, the objectives of participating organisations are broadly summarised to include the following objectives:

- to examine internal capabilities to respond to, and recover from, a cyber attack,
- to validate, examine and exercise information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information,
- to promote awareness and education of appropriate points of contact and correct procedures to use when responding to a cyber incident, and
- to exercise, examine and validate international communication, cooperation and collaboration between participating governments.

## 2.5 Scenarios

Australian participants played varying combinations of 12 scenarios, some of which were intended to provoke international play. Scenarios were designed largely by the participants to meet their internal exercise objectives. All elements of these activities were simulated and did not impact any live networks - there were no physical consequences as a result of any of the scenarios. Scenarios ranged from widespread internet degradation, to attacks on Supervisory Control and Data Acquisition (SCADA) systems, through to the compromise of a Certificate Authority.

## 2.6 Media Outreach

The communication 'real world' media strategy to promote Australian participation in Cyber Storm II was prepared by the Public Affairs Branch of the Attorney-General's Department. The communication strategy was developed to:

- increase awareness of e-security issues;
- promote Australian involvement in Cyber Storm II;
- publicise the event; and
- manage media issues as they arose.

Australia's participation in Cyber Storm II was conducted in accordance with existing national security arrangements with the aim to build on the outcomes of the first Cyber Storm exercise. The Australian Government has a close working relationship with the business community and Cyber Storm II aimed to further develop that relationship.

## 2.7 Planning and Execution

Cyber Storm II planning took 18 months. The Attorney-General's Department provided a framework in which participants could run an internal e-security exercise in conjunction with many of their suppliers and/or customers. The main

benefit was that external relationships, so often notional in a purely internal exercise, could be tested.

This planning period was valuable not only to facilitate a world class exercise, but also as it enabled robust information sharing, and encouraged private-public sector relationships and coordination across industries and between competitors. Many participants also noted that the design process assisted them to engage various disparate sections of their organisation, creating convergence between business interests and technical expertise in crisis management communication.

Others noted that the mere fact of participating in the planning process caused them to review (and in many cases repair) existing plans and processes.

#### *The Master Scenario Event List (MSEL)*

The MSEL provided the unfolding exercise scenario inputs in a manageable and observable format. This list was comprised of individual events, referred to as MSEL injects, that were “injected” into play throughout the exercise in various forms. Scripts for phone calls, emails, faxes and news media articles were developed. The MSEL injects also contained the expected player actions to assist the planners and observer/controllers in measuring player response. While much of the information in the database was scripted, the members of exercise control sometimes had to execute dynamic play in direct response to actual player actions. Key exercise control planners from participating organisations were intimately familiar with their respective organisation’s business, making them uniquely qualified to simulate the adversary, similar to the role of a “red team.” Assuming this kind of role provided the flexibility to increase or decrease the intensity of attacks or alter attack vectors.

The MSEL management process utilised a software tool provided by the US Department of Homeland Security.

Milestones in the planning process were marked by planning conferences. The following is a breakdown of the 18-month planning and design period.

#### *Concept Development Conference (CDC) to Initial Planning Conference (IPC)*

In December 2006 the US held a concept development conference that gathered stakeholders, including Australia, to set out the exercise scope, goals, and objectives. The US exercise was planned using the concept of exercise ‘threads’ - working groups that consolidated planning for each critical infrastructure sector involved in the exercise. Planners in the US worked in eight threads representing the chemical sector, the transportation sector (specifically rail and pipelines), Federal, States, international, information technology/communications (IT/Comms), law enforcement/intelligence (LE/I), and public affairs. The dedicated participation of the Federal and public affairs threads were a result of needs identified in Cyber Storm I. Australia followed this model, creating planning threads for banking and finance, water, electricity, communications, information technology, government and public affairs.

In March 2007, the growing Cyber Storm II community met in Washington at an IPC to finalise objectives and develop primary scenario paths. The IT/Communications thread produced a scenario menu which catalogued potential

scenarios, and the Law Enforcement/Intelligence (LE/I) thread began crafting the adversary for the exercise. Australia was represented at this meeting in the US IT/Communications, LE/I and international threads.

In May an Australian IPC was held in Sydney. The point of the conference was to introduce the planners from the various participating organisations and to finalise exercise objectives for each of the participant's internal exercises.

#### *IPC to Midterm Planning Conference (MPC)*

Planners focused on scenario concept design and development during this period, with threads beginning to craft scenarios that met their objectives and examined perceived vulnerabilities. A 'trusted agent' community, bound by signed agreements, enabled the sharing of sensitive information across industry and government via the US Computer Emergency Readiness Team (US-CERT) portal. By the MPC, scenario concepts were formed and in the US the adversary framework was established.

#### *MPC to Final Planning Conference (FPC)*

Planners continued to develop depth in scenarios by confirming attack vectors, adversary requirements, business impacts and expected player actions. In the US, LE/I planners worked with other threads to assist shape malicious activity and coordinate adversary relationships. At the FPC, planners were required to report their progress on scenario injects to reconcile timing and other conflicts. In most cases, this was not actually achieved until the Final MSEL Conference (FMC). At the FPC, exercise planners were also familiarised with exercise mechanics issues such as establishing player sets and exercise contact lists, and the role of Observer/Controllers. Planners at the MPC were also trained in the use of the MSEL management tool.

#### *FPC to Final MSEL Conference (FMC)*

Following the FPC, planners began inputting scenario content into the MSEL tool. Thread meetings were held for various sectors in order to foster coordinated and coherent scenario development. In February 2008 planners met at the FMC to complete an inject-by-inject review of the exercise scenarios. Planners also learned about exercise control mechanics and protocols and Observer/Controller training requirements.

#### *Pre-Exercise build-up (Pre-Ex) and Execution*

The pre-ex period, which began in February 2008, was designed to prompt the identification and discussion of information sharing requirements between participating law enforcement, intelligence and private sector communities in preparation for the exercise.

The exercise was conducted in March 2008. AuExCon, located in the Yarra Valley, served as the national coordinating body for the Australian exercise. USExCon was located in Washington DC. AuExCon was in frequent contact with the US ExCon regarding the exercise mechanics and in order to facilitate international exercise play. The concept of a centralised coordinated exercise with decentralised execution was designed to be both practical and realistic for the players involved in the exercise across Australia and internationally.

At AuExCon, 45 individuals representing public and private sector organisations, sectors and industry groups monitored exercise play at the external locations through regular contact with observer/controllers via phone and email. Exercise control staff also responded to requests for information from players, coordinated real-time injects to facilitate play and supported all stakeholders to ensure objectives were met. Some Exercise control staff also simulated those entities not represented in the player set and notional companies.

The Cyber Storm II MSEL was the driver for the entire exercise. It was the MSEL injects that set the pace of the exercise and elicited player responses

Each thread leader was responsible for making coordinated and informed thread decisions. Thread leaders monitored MSEL injects and overall thread play. They also worked closely with the Exercise Managers, who also monitored upcoming injects, coordinated injects with each thread, verified the timing and validity of injects, and ultimately sent injects to players. As Cyber Storm II unfolded, the exercise design provided thread leaders and planners the flexibility to create new MSEL injects or alter existing injects to facilitate a logical game flow. These new or altered injects went through the same coordination process with subject matter experts in the relevant threads prior to dissemination, albeit on an expedited timeline. Planners and observer/controllers tracked inject edits and status changes throughout the exercise through the MSEL management tool and discussions with exercise control personnel.

Given the time zone differences, play ranged from 0700hrs to 2300hrs during the course of the 3-day exercise, though the majority of play occurred between 0800 hrs and 1800hrs, Australian Eastern Summer time. At the conclusion of each day's play, thread leaders and the exercise management team met to assess key issues, exercise conditions and to provide a summary of the day's play in preparation for the following day. On the last day, exercise control staff, the exercise management team and most observer/controllers attended a 'hotwash' debrief session at AuExCon to gather initial observations of the exercise play and key lessons learned.

## **2.8 Security Policy**

The goal of Cyber Storm II information security policy was to ensure that any sensitive information shared during the exercise was only used for the stated objectives. The willingness of participants to disclose potentially sensitive information was one of the key factors in the success of the exercise, since it allowed:

- the development of plausible, realistic and meaningful scenarios to maximise the value of the exercise,
- planners to understand the implications of specific attacks on their infrastructure, and
- planners to understand the responses expected from other planners and players from an organisational perspective.

The Cyber Storm II information security policy involved a multi-layered approach that included creating a trusted community and a secure network environment for exercise planning and execution.

A Trusted Agent Agreement (TAA) was signed by all planners in Australia and essentially required individuals to comply with the US Department of Homeland Security Management Directive 11042.1: “Safeguarding Sensitive but Unclassified (For Official Use Only) Information.” Australian planners signed a version of the agreement consistent with applicable Australian law and all planners world wide signed a version of a similar agreement. Australian Government employees signed an acknowledgement of their responsibilities under both the *Public Service Act 1999* (Cth) and the *Crimes Act 1914* (Cth).

The obligations imposed upon exercise planners included a duty not to disclose any content containing any patent, trademark, trade secret or any other proprietary rights of any party. These obligations did not alter the obligations or release signatories from their responsibility to comply with contractual or fiduciary arrangements, obligations, or applicable international or Australian laws relating to the disclosure of sensitive information.

Participants also agreed to adopt practices designed to reduce the possibility of security breaches and the introduction of malware into exercise systems and databases. All participants in the Australian national exercise have complied with these agreements for the duration of the planning, execution and “after action” processes.

### **3. Significant Findings**

Observations recorded during the exercise and in the post-exercise debriefs revealed several significant findings. Comment on these arrangements focused on communication and escalation paths, organisational roles and responsibilities, and information sharing and coordination among organisations. The findings were determined with reference to the overarching objectives of the exercise and the findings included in this report reflect those that are applicable to both the private and public sector. Observations by individual organisations or sectors are grouped below to support these significant findings.

Many participants noted that merely planning the exercise prompted internal reviews and modifications to their existing crisis arrangements.

**Finding 1: Effective response is enhanced by routinely reviewing and testing Standard Operating Procedures (SOPs), Incident Response Plans and /or crisis management arrangements.**

*Effective response to a cyber crisis is significantly enhanced by having tested procedures or arrangements, in which crisis-management relationships in the cyber response community are regularly reviewed to solidify communications paths and clarify organisational roles.*

**Observations:**

- a. Coordinated responses to an e-security crisis are required across the critical infrastructure protection community. Processes were often found to be oriented toward the mitigation of, and response to, physical threats. More tailored and coordinated security response measures are needed to address cyber incidents, particularly when cyber threats have impacts across sectors.
- b. Participants noted that their own internal response mechanisms could be improved. Clarification of escalation procedures internally and externally, in addition to the identification of a communication plan to facilitate closer working relationships between business areas within organisations, were two common themes.
- c. Participants noted that in some circumstances formal processes tended to be circumvented under pressure or were not activated in a timely manner.
- d. Organisations that acted as information clearing houses or coordination bodies were under intense pressure during the exercise due to the number of scenarios. Where formal protocols existed, under stress these tended to give way to informal processes. During a crisis the balance between formal and informal information sharing is likely to favour informal communication in order to facilitate rapid responses. It was also noted that informal processes outside of standard procedures could allow information to be lost.
- e. Many participants stated that a key value of Cyber Storm II was the opportunity it provided to test their internal procedures in a realistic scenario that included external stakeholders. This external element enabled organisations to assess their procedures more accurately and many participants cited this as a major benefit of Cyber Storm that cannot be replicated by exercising internally.

**Finding 2: Non-crisis interaction among key stakeholders enhances effective crisis response during an incident.**

*More frequent, non-crisis interaction between various stakeholders involved in protecting the national information infrastructure will enhance real world response capabilities. Established relationships facilitate rapid information sharing among community members and must include relationships across sectors, with suppliers, with vendors and with incident response organisations.*

**Observations:**

- a. The coordinated attacks simulated during Cyber Storm II highlighted the importance of pre-existing relationships between organisations prior to a crisis. This was particularly important in developing accurate situational awareness. Participating organisations commented that maintaining situational awareness across related critical infrastructure sectors during a cyber attack was critical to ensuring effective response and recovery.
- b. Many participants reported that the exercise assisted in developing stronger relationships across and within sectors. A common theme was that the 18 month planning process allowed relationships to be built up that would help in a genuine crisis. Most participants found Cyber Storm II to be a trust-building exercise which will lead to greater information sharing and closer cooperation between participants in the real world.
- c. Participants noted that the internal communication between business areas in their organisation improved during Cyber Storm II. Participants also commented that the exercise, both in the planning and the execution, forced the organisation to engage across the whole business to address issues. This drove home the need to routinely engage with different business groups on cyber issues and as a result some organisations have already begun to identify an internal communication plan to facilitate closer working operations between different business areas. One participant found that the exercise identified many working groups that are dealing with substantially the same issues but were not aware of the commonality (due to the scale of the business).
- d. Many participants relied on sector-specific relationships (developed through Infrastructure Assurance Advisory Groups, for example) as focal points for sharing information during the exercise. In a coordinated attack, the underlying questions are how to contact another organisation similarly affected and who to contact within that organisation. This is especially true where there is no pre-existing relationship. Existing relationships are crucial as organisations are not able to create trusted relationships in the centre of a crisis.
- e. Interaction between participating private organisations and Australian Government agencies differed greatly between sectors. Some players noted that internal education on engagement with Government and law enforcement agencies would be undertaken following the exercise. Interaction outside established lines of communication between industry and law enforcement was a beneficial outcome of the exercise.

**Finding 3: Crisis communication procedures, predicated on accurate and appropriate points of contact, must be formalised within contingency planning.**

*Communication during a crisis significantly impacts the timeliness and effectiveness of responses. A unity of effort can be more effectively maintained when there is a clear understanding of roles and responsibilities and the interfaces between them.*

**Observations:**

- a. Greater clarity of roles and responsibilities at every level of response will greatly increase the ability of organisations to harness their own resources to address incidents. Coordination and cooperation internally within organisations was most efficient when roles and responsibilities were clearly defined. Likewise, communication between organisations was most effective when organisations had already identified who was responsible for what areas within external organisations.
- b. The exercise enabled players across sectors and government bodies to test and, in some cases, develop crisis communication procedures to respond to a cyber security incident. It was a common finding that crisis management procedures were oriented towards mitigating physical threats and that cyber incidents will require additional contacts within an organisation. Raising awareness around cyber incident response and how it differs from other emergency management responses was a valuable exercise outcome for many players and participants have indicated that they will further promote e-security education internally.
- c. A tangible result from the exercise for one participant was identification of the appropriate person to attend crisis management meetings during an e-security incident. This organisation found that during the exercise those attending the crisis meeting did not have the appropriate expertise. They identified a need for a high-level decision maker supported by a technical expert. This person has since been appointed
- d. Another participant discovered that their contractual arrangements outlining crisis communications did not reflect reality. The organisation has already reviewed these disparate arrangements and refined the protocols (including updating contact lists), to ensure consistency of real practice with SOPs.

**Finding 4: Cyber crises require a tailored response that takes into account multiple interdependencies.**

*The borderless nature of cyber attacks, and the speed with which they can escalate across infrastructure sectors, was demonstrated in Cyber Storm II. Contingency planning must include potential flow-on effects.*

**Observations:**

- a. Organisations noted that participation in the exercise was critical in exploring unforeseen interdependencies and escalation paths within and across sectors. An important learning was the need to formalise lines of communication between Government and industry to ensure that the scope of any problem is properly understood to enable a coordinated and effective response.
- b. Interdependencies within organisations were also explored during the exercise. Some industry players noted that a key value of the exercise was the opportunity it provided to stimulate the convergence of business and technical expertise in responding to incidents. Cyber Storm II was the impetus for ensuring more effective communication within separate functional areas for many organisations. A major benefit for one player was demonstrating the need to routinely engage with different functional areas on cyber issues.
- c. Several participants observed that more interaction across borders and sectors will improve the response capabilities of all concerned. One participant commented that Cyber Storm II amply demonstrated the benefit in “more people from more areas talking more often” about cyber security.
- d. One participant found that interdependencies existed within their own disparate functional business units, in addition to those discovered across sectors. For example, communication interdependencies were illustrated in relation to SCADA systems where visibility and ability to manage SCADA systems are compromised once communications are affected. When power supplies are affected by SCADA problems, the communications systems fail to function. One organisation has identified the need to test interdependencies in internal systems and between sectors in more depth in future exercises as a priority.
- e. Another participant noted that a unique benefit of the exercise was the opportunity to detect new areas of possible risk by observing the play of others. They gathered invaluable information from watching the finance sector exercise.

**Finding 5: Developing internal reporting and external notification thresholds assists in effective incident response by creating better situational awareness.**

*Identifying the problem, rather than simply addressing the symptoms, is critical to effective cyber incident response. In order to ensure situational awareness within and between organisations, clear notification thresholds should be developed and promulgated so that technical incident responders know when escalation internally or externally is necessary.*

**Observations:**

- a. It was a common finding amongst participants that IT incident responders tend to focus on managing incidents rather than addressing the wider problem and its ramifications. A common observation was the tendency among IT incident responders to instinctively minimise the scale of the problem and to focus on what they knew or could manage when reporting to management. Many participants noted a need to educate incident responders to brief management on the limits of their understanding of problems, and the possible broader exposure faced by the organisation.
- b. The natural tendency to minimise the scale of the problem was also found to be true in many crisis committee meetings that were convened during the course of the exercise. Incident management meetings need to ask what the exposure 'might' be at worst case and develop strategies to minimise impact. They need also to be able to accept that the responders may not have all of the answers.
- c. A common problem, particularly in coordination centres, was that while responding to multiple incidents the responders failed to realise that there was a crisis. The focus tended to be on what was broken or performance metrics.
- d. One player stated that an exercise outcome was the clarification of guidelines to support escalation of IT security incidents with narrow spectrum impact to high priority status. This same company will also modify their crisis response plans to ensure that regular status updates are provided from crisis management teams to incident responders and vice versa.

**Finding 6: Attempts to facilitate an interactive international game were hampered by time zone differences, isolated scenario building and unexpected player actions.**

*International play was not extensive in the Australian national exercise. A longer pre-exercise build up, a longer exercise duration (to account for the 18 hour difference between Wellington and Washington) and more international communication during the exercise planning phase will need to be incorporated into Cyber Storm III.*

**Observations:**

- a. Attempts to facilitate international cooperation and communication through the Certificate Authority compromise were not successful. Despite high-level efforts made by planners, the scenario did not escalate as planned and resulted in limited communication and coordination within the international community during the exercise.
- b. International play was severely hampered by the time difference. In essence the US exercise started a day later than the Australian exercise which meant that Australian play was winding down while the US play was winding up.
- c. Through the planning process, participants gained insight on how each nation or international organisation would respond to a cyber incident. Many participants commented that, with the benefit of hindsight, they would have planned and executed their scenarios differently to engage their own international partners. They did not fully capitalise on the framework and opportunities that Cyber Storm II provided to exercise as broadly as they could have.
- d. Players noted that the interactive international elements of Cyber Storm II were very appealing and an impetus for their involvement. For many organisations, participation in Cyber Storm III will depend on their ability and readiness to capitalise on the opportunity afforded by the international framework of the exercise. Many players noted that, in hindsight, they didn't have the perspective to involve their international partners in Cyber Storm II as it was a completely new concept and they were unfamiliar with the likely execution of the exercise. They agreed that Cyber Storm III will allow them to build on these lessons and incorporate their international partners in the planning and design of Cyber Storm III.
- e. Some players noted that greater involvement with and interaction between Australia and New Zealand in particular should be pursued as part of any Cyber Storm III given the commonality of the issues and players.

## **Annexe A: Participating Organisations**

This list does not include six organisations that wish to remain anonymous.

### *Non-government Participants*

AusCERT  
AusRegistry Pty Ltd  
Australia and New Zealand Banking Group Limited  
The Australian Domain Name Administrator  
Australian Securities Exchange  
CISCO Systems Australia  
The Commonwealth Bank of Australia  
Country Energy  
Ergon Energy Corporation Ltd  
Energex Ltd  
Energy Networks Association  
Insurance Australia Group  
Internode Systems Pty Ltd  
Melbourne IT Ltd  
Microsoft Australia  
National Australia Bank  
Powerlink Queensland  
Singtel Optus Pty Ltd  
Suncorp Metway Ltd  
Telstra Corporation Limited  
Westpac Banking Corporation  
Woodside Energy Ltd

### *Observers*

Attorney-General's Department – Emergency Management Australia  
Bank of Queensland  
Bendigo Bank  
Citigroup  
Foxtel  
IT Security Experts Advisory Group  
National Electricity Market Management Company  
QANTAS Airways Ltd.

### *Commonwealth Agencies/Departments*

Attorney-General's Department  
Attorney-General's Department – GovCERT.au  
Attorney-General's Department – Protective Security Coordination Centre  
Australian Communications and Media Authority  
Australian Federal Police  
Australian Security Intelligence Organisation  
Centrelink  
Customs  
Defence Signals Directorate  
Department of Broadband, Communications and the Digital Economy  
Department of Defence

Department of Finance and Deregulation  
Department of Foreign Affairs and Trade  
Department of Immigration and Citizenship  
Department of Infrastructure, Transport, Regional Development & Local  
Government  
Department of Prime Minister & Cabinet  
Department of Resources, Energy and Tourism  
Office of National Assessments

*State Government*

SA Department for Transport, Energy & Infrastructure  
SA State Emergency Management  
WA Department of Premier and Cabinet  
WA Department of Treasury and Finance – ServiceNet