



Unisys Australia Pty Limited
ABN 31 105 642 902

Telephone
61 2 9647 7777
Facsimile
61 2 9647 7000

Unisys Campus
Rhodes Corporate Park
1G Homebush Bay Drive
Rhodes NSW 2138
PO Box 288
Concord West NSW 2138

16 November 2007

Greenhouse and
Energy Reporting Taskforce
Australian Greenhouse Office
Department of the Environment
and Water Resources
GPO Box 787
Canberra ACT 2601
reporting@greenhouse.gov.au

To Whom It May Concern

SUBMISSION TO NATIONAL GREENHOUSE AND ENERGY REPORTING SYSTEM - REGULATIONS DISCUSSION PAPER OCTOBER 2007

Introduction

Unisys welcomes the opportunity to contribute to the development of the regulatory framework that will implement the National Greenhouse and Energy Reporting System and underpin a future national emissions trading framework. In so doing, we hope to assist the Department of the Environment and Water Resources in its deliberations, and inform public discussion on some of the issues raised.

We would be happy to expand further on the issues raised in this submission if it would be of assistance.

Background

Unisys is one of the leading information technology services companies worldwide with market leading credentials in security. In developing our submission, we have drawn on the specific work we do to help clients respond to the demands of a changing security environment, particularly in the fields of identity management and biometrics, system, network and infrastructure security and supply chain management, for both government and private sector clients. We have also drawn on our depth of experience in our core capabilities of consulting, systems integration, outsourcing, infrastructure and server technology. Additionally, our submission has been informed by key findings of the Unisys Security Index™ – Australia's only regular gauge of consumer attitudes towards a range of security issues¹.

We are committed to helping our clients secure their operations, giving visibility to see the impact ahead of investments, risk and decision points – this submission, the Unisys Security Index and our market footprint all attest to this commitment.

¹ The Unisys Security Index was developed with Newspoll and is conducted three times per year. The Index was initiated in Australia and is now conducted in 14 countries globally.

Context

The passing into law of the National Greenhouse Emissions and Energy Reporting Act ('The Act') on 28 September 2007 sets a significant precedent in the Australian business operating environment. The Act establishes, on a national basis from 1 July 2008, mandatory reporting for Corporations and other organisations on emissions and energy usage, once pre-determined threshold levels are triggered.

The Act paves the way for a future Australian Emissions Trading framework. The Act proposes to do this through a streamlined, single national reporting point for collection, storage and reporting on greenhouse emissions and energy consumption. The information collected is intended to serve a range of legal, financial, policy and community based imperatives, including:

- better inform policy, now and for the future
- to assist Commonwealth, State and Territory govt programs and activities
- to ensure compliance through application of permits, incentives, potential legal action
- to ensure that Australia meets its international reporting obligations
- provide the public and investor community with good Company level information
- facilitate a future emissions trading scheme and the provision of offsets

Without understating the significance of The Act from an environmental policy perspective, much of The Act is, in essence, about increasing the quality and consistency of information. The Act even specifies the ends to which this information will be put, including:

- to monitor, report & verify operation of the emissions trading scheme
- to be subject to external and internal audit
- to be disclosed publicly
- to be the basis for financial incentives and penalties, as well as potential legal action

The critical importance of establishing and maintaining the highest levels of data security, integrity and confidentiality if these outcomes are to be achieved cannot be overstated.

- Companies will need to be confident that potentially commercially and legally sensitive information is highly defensible and resilient to commercial manipulation or sabotage.
- Investors will need assurance that they are sufficiently informed about matters impacting personal and professional financial investment decisions.
- Public confidence in the initiative will be vital if it is to be seen as a credible measure designed to reduce emissions and uphold our international obligations.
- Government (Federal, States and Territories) will need confidence that the information recorded satisfies the above and also provides a robust basis on which to make future policy decisions.

Indeed, in tabling the Bill, Minister for the Environment and Water Resources The Hon Malcolm Turnbull, MP said "It is vital to any emissions trading scheme that we have *robust and comprehensive emissions data* and the legislation that I have introduced today provides the framework for the collection of that data."

It is this fundamentally important issue of security that we address in this submission.

Public Opinion and Security

As the nature of the global security environment has changed, so too have consumer attitudes towards it. In 2006 Unisys, with Newspoll, launched the Unisys Security Index™ – Australia's only regular gauge of consumer attitudes towards a range of security issues.² The Index is conducted three times per year and monitors public concerns towards 8 core security issues within four categories - financial, personal, national and internet relates issues. The Index enables us to monitor overall levels of concern (as an Index number out of /300), levels of concern against issue categories, and levels of concern on specific topics or questions.

The Unisys Security Index results show that today consumers think about many more issues when it comes to their security than traditionally has been the case. Longstanding issues of personal safety and financial security have been extended into areas such as identity theft, credit/debit card fraud, shopping and banking online and new forms of terrorism. Moreover, it is these contemporary issues which frequently rate as more immediate or pressing, with Australian consumers consistently indicating that identity theft and credit/debit card fraud are the leading two security concerns on each occasion the Index has been conducted.

This finding is reinforced by results of the 2006 Lowy Institute Poll which identified that improving the global environment was seen as the top-rated threats to Australia's vital interest, alongside international terrorism and the possibility of unfriendly countries becoming nuclear powers.³ Two thirds of respondents wanted steps taken now to tackle the problem of global warming even if the cost were high. One quarter thought we could deal with the problem gradually by taking steps that are low in cost. Almost none thought we should not take any steps that would have economic costs.

At the time of this submission, concerns about security amongst Australians are at higher levels than they have been at any time since June 2006. Security has assumed a level of significance in people's minds and in a much broader way than seen previously. More people today want to know what security measures are planned or in place.

This highlights the vital role that tangible and perceived security measures play in building confidence and trust with the people who interact with you and your systems. Here lies one of the most challenging aspects of security – whether you are talking about national security, security of information and identity – many of the most significant security measures are invisible to the average person.

How then, do you strike the right balance between security as a protector, and security as a builder of trust and public confidence? Too much security and you may reduce convenience and increase concerns. Too little and you risk not doing enough to protect them. The intangibles of confidence and trust are both hard won and easily lost.

Where, when and how you invest in security to protect and to build public confidence are vital decisions in responding to our new security threats and in maintaining our way of life. This challenge is as much a challenge for government as it is for business, and must today permeate everything that we do.

² www.unisyssecurityindex.com.au

³ <http://www.lowyinstitute.org/Publication.asp?pid=470>

Securing Our National Environmental Energy and Greenhouse Reporting Data

While Unisys is not intimately familiar with OSCAR – the Department of Environment Water and Resources' 'Online System for Comprehensive Activity Reporting' – we understand that it is intended that this will be the activity reporting system used under The Act, modified as necessary. There are a number of important issues that will need to be taken into account as part of this process, and these are developed below.

The Online Reporting System – expanding OSCAR

With The Act bringing a fundamental shift from voluntary to mandatory reporting, the activity reporting system obviously will need to accommodate a much *greater volume of data* through increased numbers of companies entering more data on a regular basis. The data volume will further increase as the threshold levels for reporting lower over time.

More significantly, the system will need to accommodate far *greater scrutiny of that data* - from companies, from auditors, from the public and the investor community, from different levels of government and potentially also other international governments. The data contained within the system may be legally, commercially and financially sensitive and must be defensible to the highest standards and resilient to deliberate manipulation for advantage, such as commercial sabotage.

Security in relation to data access is addressed in more detail below, suffice to say that because of the variety of interests vested in the data, built into the system will need to be a complex layering of levels of data access, geographically dispersed and varying from highly confidential to open or public access.

Defining these policy parameters early on – such as who has access and how much; how the data will be used in what circumstances – and before the reporting system is developed or modified, will be critical in ensuring that data collected from commencement of The Act is consistent and high integrity data in the future.

A further layer of complexity will be inherent in the *different levels of data aggregation* specified under The Act – many of which are still to subject to refinement, and could also be impacted by future policy adjustments by the Government of the day. Moreover, The Act itself is based on an evolving science, and many of the methodologies that will be used to determine penalties and incentives are not yet developed.

Importantly, as this is a new science, the reporting system will need to have sufficient flexibility to accommodate future adjustments and methodology changes without undermining the integrity of the information already collected. This capacity for flexibility will need to be balanced with the possibility of function creep and the potential for the reporting system to extend beyond the original intent of the policy and regulatory commitment it serves. These issues could further risk integrity of the system and confidence of those impacted by it.

There are some specific things that can be done to ensure that systems do not get distorted or perverted into doing something quite different. Strong operational policy, coupled with strong application of security protocols, developed and applied early on, are critical.

Recommendations:

1. *A framework model of the national reporting system should be developed as a first step. This model can then be tested and manipulated against policy parameters and the intent of The Act and ensure that a holistic approach to information security is paramount within the system.*

National Greenhouse And Energy Reporting System Regulations Discussion Paper

2. *Detailed policies and protocols – such as who has access to what data, how the data will be used in what circumstances should be defined early on and tested against the framework model.*

3. *A future system roadmap should be developed that can be tested against the framework model to enable these to be accommodated without risking the potential of future adjustments impacting future information integrity.*

4. *Key stakeholders from each of the target groups (investor community, commercial entities, auditors, as well as regulatory bodies at state and federal level) should be involved in the testing of the framework model, particularly data entry and reporting as an initial trust building measure.*

5. *The framework model should be tested for Security Certification compliance to ensure that the actual system withstands the highest external scrutiny and assurance, as well as changes and adaptations through the system lifecycle.*

Data Entry, Data Access and Lifecycle Data Integrity

As mentioned, maintaining careful parameters on security in relation to the entry and access of data in the system will be paramount if the system is able to accommodate what is a complex combination of public transparency, commercial confidentiality, different and variable levels of information aggregation and multiple levels of data entry, access and reporting.

Additionally, The Act reflects further potential complexity through the aggregation of a range of state/territory government programs as well as the longer term potential that OSCAR might link directly with other systems in terms of our international reporting obligations.

Careful and detailed policy definition and planning at the outset will be needed to define who has access, when, to what types of information, as well as who has the ability to run what types of reports, and ensure that the reports do not divulge more information than the user is entitled to.

Answers to the following sorts of questions will be critical in ensuring that the system is both secure and flexible from the outset:

- How will the general public view the information? Will this be a pre-prepared summary report or an online report from the reporting system 'real time'? How regular will reports be? Will they be pre-vetted through Departmental eyes first?
- How will the investor community receive their information? From the companies themselves? As a separate independent report from the reporting system? To what level of confidentiality? What about sector/industry-wide reports?
- Who will be allowed to produce reports? Companies who enter data? Federal Government, State / Territory Government? What level of scrutiny will corporate regulators such as ASIC have? Will other government bodies have the ability to interrogate the data directly?
- Will other governments / international bodies have direct access? Or access to summary information? Will they be able to interrogate the data directly?
- Will companies be allowed to produce reports only on their own data? On other company or industry data for benchmarking or other purposes? Will they be able to interrogate other company/industry data or just their own company data?

National Greenhouse And Energy Reporting System Regulations Discussion Paper

- Will the access rights be determined based on who a person is? Who they work for? Where they are located? Will they be required to meet pre-determined levels of security clearance?
- How will confidentiality requirements be enforced? What system of penalties will apply for breaches?
- How will end-to-end auditability be maintained on access? What levels of records will be required? Will there be different levels of compliance for different levels of access?

There are a variety of methods that could be applied for ensuring that only the people who are allowed to enter or access the data are able to do so, particularly in relation to the data subject to the highest levels of confidentiality. Answers to the above questions, and also factors of convenience for potentially large numbers of geographically dispersed people and organisations, will help shape the preferred response. Establishing the highest levels of confidence and trust will be of paramount importance.

One of the leading and most secure identity methods today is Biometrics – a technology that confirms a person's identity by checking their unique physical characteristics such as their voice, face or fingerprint. While the level of confidence it provides is very high, it may not be necessary to go to such lengths.

A range of other means is also available, including token based systems. The key is to consider security holistically to include a range of other processes and protocols that such methods operate within – such as existing clearance processes for Commonwealth Government public service employees. Importantly, this would also provide a fully auditable trail of any reports run or data change, enabling breaches to be dealt with to the full extent of the law if and when these take place.

It is worth noting that one of the significant risks of inadvertent or deliberate data breach and/or data fraud comes from within the organisation, even by those who are authorised to access a system. This highlights the importance of scoping all potential risk issues holistically and taking all potential information flows and risks into account.

Various steps can be taken to ensure that the information is protected throughout its lifecycle, such as encryption coding data within the system so that all stored reports sent by email, stored on local hard drives distributed via the web or stored on USB devices, remain as secure as the original data record. With the levels of complexity inherent in The Act, this potentially could be a very complex undertaking involving multiple levels of data - again reinforcing the need for as much of this detail to be determined early on so that the system to be designed with this in mind.

The starting point for high level data integrity is to ensure that it is high quality when entered. Further steps can be taken at the point of data entry to validate that information is complete, consistent and correct before it is confirmed for storage. It would make sense to design this system such that it identifies and appropriately manages data that is incomplete or inconsistent when entered. The key is knowing what data it is that you need to collect from the outset. The result can be a further trust building mechanism for users of the system.

Firewall and other secure network provisions are obviously a must in a security environment where viruses phishing, spamming and other network or email based security attacks are increasing in frequency and sophistication.

In any event, contingency planning is critical and should provide essential fallback or recovery mechanisms in the event that security is compromised, *however unlikely this is deemed to be*. Any strong system will plan and have fast response mechanisms in place for a future possible breach in security, while diligently protecting against one. This is detailed further below.

All of the above issues would typically be articulated in the *information policy*, rather than IT policy, and again based on the intent of The Act and the legal policies and protocols that will underpin it.

Recommendations:

6. *Policy and protocols on data entry and access should be well defined and in detail early on, which also can then be tested against the framework model as part of the system development process*

7. *A comprehensive information policy should be developed which (among other things) clearly specifies data quality drivers*

8. *Careful consideration should be given to the preferred means of securing identity for varying levels of data access.*

9. *Key stakeholders from each of the target groups should be involved in determining and testing security regimes for use in securing data entry and access to ensure a good balance between convenience and security and as a further trust building measure.*

10. *Inherent in the approach to the reporting system should be a holistic approach to security, that reflects: 'information security' rather than 'IT security', and has an appreciation of the full data lifecycle – from data, to information to knowledge.*

Data Storage

Security in relation to the storage of data is a third, critical element in planning – in terms of both primary and secondary (or backup) data storage.

Naturally, the physical security of the premises where the data is housed is paramount. The minimum standard of security should be that of the highest level classification of data housed in the system. The same techniques for securing online data entry and access should be in place at the physical premises where the data is housed, possibly enhanced with additional measures such as surveillance or closed circuit television, to enable enhanced confidence levels of identity verification, monitoring and access.

While we are not familiar with the data storage arrangements with OSCAR, it is worth noting that data storage needn't be within government premises. Many organisations today partner with providers in data storage needs to control costs, reduce risk, optimize operations and align IT and business goals. The more interconnected a company's business systems and processes are with external entities, the more feasible and desirable it is to have security services that reach beyond the confines of the corporate network. Far from neglecting security, such arrangements frequently enable owners of data to more easily access the security expertise and capabilities of partner organisations. The onus is on the owners of the data to hold partner organisations to account, to approach security holistically and as a core business issue, and to educate consumers and key stakeholders on the security measures that are in place.

It is vital to ensure that adequate provision is given to business continuity and a remotely located backup storage capability in the event of incident or disaster involving the primary storage site. A holistic approach will combine a comprehensive set of discovery, implementation services and industry-leading data protection solutions with high-performance technologies to address data corruption, loss of data, and rapid service recovery. It is vital to ensure that *all of the same security standards inherent in the collection and storage of data, are in place for your disaster recovery system.*

Finally, but not least significantly, it will be important to accord with the intent of The Act in the systems adopted to provide primary and secondary storage facilities. According to some estimates, every kilowatt used to power servers in data centre environments requires at least another kilowatt to cool it. Conversely, indications are that only an average of between 5 and 10 percent of a server's potential is typically used. By increasing the utilisation of existing server assets, significant reductions can be made to energy consumption and the carbon footprint. The key is to change and upgrade not only the physical hardware, but also the operational procedures, management processes and tools surrounding it too.

Recommendations:

11. Physical premises security should be approached holistically and equally – both for the primary and secondary storage sites.

12. A comprehensive approach to business continuity and disaster recovery should be scoped and tested against the framework model.

13. To accord with the intent of The Act, an energy and emissions friendly approach should be taken to data storage requirements through virtualisation and other “mature IT” approaches.

For further information please contact:



Allen Koehn
Managing Partner
Public Sector, Asia Pacific
Unisys Pty Ltd
allen.koehn@au.unisys.com

ph: +61 2 9647 7706

fx: +61 2 9736 8691

Please also visit our website at:

www.unisys.com.au/services/security