QUT isi
Information Security Institute

E-Government - an Information Security Perspective

Professor Ed Dawson
Professor Emeritus, Information Security Institute
Dr Jason Reid
Senior Research Fellow
Faculty of Science & Technology
Ph: 07 3864 9551
Fax: 07 3221 2384
Email: e.dawson@qut.edu.au

Presentation Overview

- Overview of the ISI
- Introduction & background to E-Government
- E-government and security
- Risk management for information security
- Information assurance frameworks
- Privacy compliance
- Identity management and authentication
- Smart cards
- Biometrics
- Legal & Risk issues in E-Government

Presentation Overview contd.

- Case Study: Security and legal frameworks for E-tendering
- Case Study: High assurance ICT for E-Government
- Case Study: Information sharing for CIP
- Research Challenges

ISI Overview

History

- Information Security Research Centre founded in 1988
- Research in Information Technology Security
    - Cryptology
    - Network Security
    - Trusted Computing
- Information Security Institute formed in 2005

Collaborative Research

- Faculty of Built Environment and Engineering
- Faculty of Business
- Faculty of Science & Technology
- Faculty of Law

Aim

Conduct cross-disciplinary research in the areas of:

- Information Technology
- Law
- Business
- Engineering

to answer information security, information protection and technology policy challenges that confront business, government and the community as a whole

Personnel

- 41 Researchers
  - 13 Professors
  - 5 Associate Professors
- 89 Postgraduate Research Students

6 Domains

- Cryptology
- E-Business and E-Government
- Governance, Law and Policy
- Network Security and Digital Forensics
- Speech, Audio, Image and Video Technology
- Risk and Crisis Management

Cryptology

- **Research Areas**:
  - Analysis and Design of Symmetric Ciphers
  - Analysis and Design of Public Key Algorithms
  - Issues in Global Public Key Infrastructure
  - Proofs and Specifications for Cryptographic Protocols
  - Efficient Software Implementation
  - Cryptographic Protocols for Control Systems
  - ID-Based Cryptography

E-Business and E-Government

- **Research Areas:**
  - Secure Electronic Auctions
  - Electronic Contracting
  - Electronic Land Dealing Systems
  - Electronic Banking
  - E-Tendering
  - Secure Electronic Voting
  - e-Litigation – a “best-practice” Model
  - Electronic Government Information

Governance, Law and Policy

- **Research Areas:**

  - Policy Frameworks for National Infrastructure Governance
  - Legal Frameworks for Protection of NCIP
  - Competition Policy and Regulation
  - Privacy Law and Policy
  - Technology Governance
  - Information Security Standards
  - Privacy and FOI Issues

Network Security and Digital Forensics

- **Research Areas:**
  - Control Systems
  - Computer Network Vulnerability Assessments
  - Network and System Event Monitoring
  - Web Services and SOA Security
  - Incident Response
  - Fraud and Misuse Detection
  - Cross Domain Solutions
  - Trusted Computing
  - Computer Forensics

Speech, Audio, Image and Video Technology

- **Research Areas:**
  - Speaker Verification and Identification
  - Multi Camera Video Surveillance
  - Multi Microphone Audio Surveillance
  - Face Verification and Identification
  - Multi-Biometic Systems
  - Person Tracking in a Crowd and Activity Detection
  - Biometric Policy
  - Biometric Smart Cards
  - Perimeter Protection

Risk and Crisis Management

- **Research Areas:**

  - Threat, Vulnerability and Risk Analysis in the Private and Public Sectors
  - Business Continuity Planning and Crisis Management
  - Resilience and interdependency Modelling in Critical Infrastructure

ISI Research in Security and E-Government

- **CRC for Construction Innovation Projects 2005-2007**
  - Security and Legal Frameworks for Electronic Tendering.
  - Security and Legal Frameworks for Electronic Contracts
  - Researchers from IT and Law
  - Partners:
    - Department of Public Works
    - Queensland Department of Main Roads
    - Brisbane City Council
    - Crown Law
    - Large Construction Companies

ISI Research in Security and E-Government

- **CRC for Smart Services Projects 2006-2009**
  - Heterogeneous System for Electronic Government.
  - Security, Legal, Business Continuity Issues
  - Researchers from IT, Law, and Business
  - Main Partner:
    - Queensland Government

ISI Research in Security and E-Government

- **Australian Research Council Research Grant 2007-2009**
  - Security and Legal Frameworks for Virtual Information Sharing Networks
  - Researchers from IT and Law

ISI Research in Security and E-Government

- **Australian Government 2002, 2005, 2008**
  - Research Challenges in Information Security

E-Government

Background and Overview

Background

- The growth and rapid adoption of the Internet has greatly changed how all organisations deal with their respective stakeholders.
- Electronic delivery of Government services (E-Government) was being thought about prior to WWW, but in last 15 years the migration by governments globally to electronic service delivery has been substantial.

Background (contd.)

- Government collected information is diverse and varied.
- Originally the collection was for primarily for internal usage.
- Governments are commonly arranged through agencies or departments which have the authority to manage a particular legislative regime; eg:
  - Department of transport deals with roads, and other infrastructure development
  - Department of health concentrates of health issues within the community
  - Department of Natural resources deals with land development including mines and sometimes water resources.
- It is not uncommon for government agencies to collect basically the same information at different times, under different circumstances, and by different means.
- This is inefficient and frustrating for citizens and businesses

What is E-Government?

E-Government: “Refers to the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government.”

Source: E-Government: Analysis Framework and Methodology, OECD Public Management Service, Public Management Committee, 2001.

Another Definition

“The continuous innovation in the delivery of services, citizen participation and governance through the transformation of external and internal relationships by the use of information technology, especially the Internet”

Source: Roy, J., E-Government in Canada: Transformation for the Digital Age, Ottawa: University of Ottawa Press, 2006.

“The real benefit of e-government lies not in the use of technology per se, but in its application to processes of transformation”

Source: UN E-Government Survey 2008, United Nations, New York 2008, available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf

E-Government Modes

- Government to Citizen (G2C)
- Government to Government (G2G)
- Government to Business (G2B)

E-Government Prerequisites

- The potential of e-government hinges upon three prerequisites:
  - a minimum threshold level of technological infrastructure
  - human capital and
  - e-connectivity for all
- E-Government programmes will be effective and inclusive of all citizens only if all have functional literacy and education which includes:
  - knowledge of computer and Internet use
  - access to an Internet connected computing device
- Accomplishing this is a key challenge of e-government development

E-Government Drivers

- Service delivery is currently not citizen-focused
- Services could be delivered more efficiently
- Public sector data stores are a valuable resource
- They are collected and maintained at considerable public expense
- Currently not effectively utilised
- This creates strong drivers to make data more widely available:
  - Within government
  - Across different levels of government
  - To the public and commercial sector

Benefits of E-Government

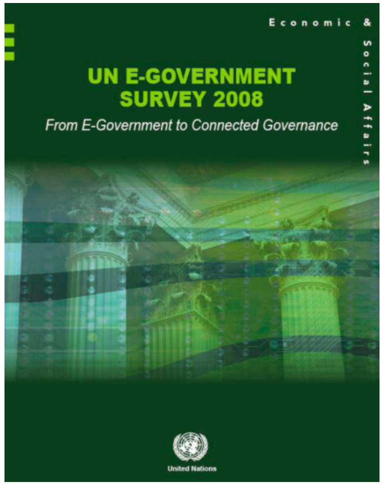
ICT-enabled connected governance contributes to:

Internally

- Avoidance of duplication
- Reducing transaction costs
- Simplifying bureaucratic procedures
- Greater efficiency
- Greater coordination and communication
- Enhanced transparency
- Information sharing between agencies
- Security of information management

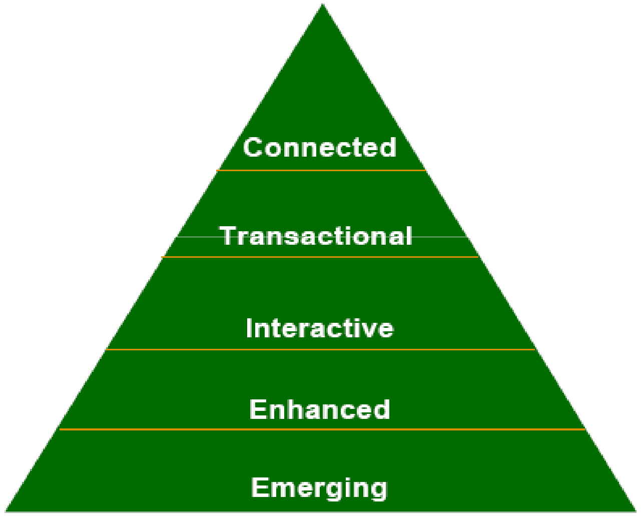
Externally

- Faster service delivery
- Greater efficacy
- Increased flexibility of service use
- Innovation in service delivery
- Greater participation
- Greater citizen empowerment
- Citizen participation


Economic & Social Affairs
UN E-GOVERNMENT SURVEY 2008
From E-Government to Connected Governance
United Nations

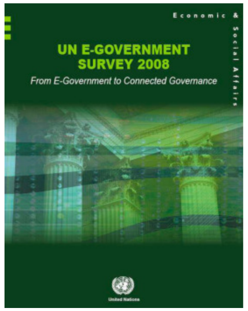
Phases of E-Government Development

1. **Emerging** - static web pages for individual departments - little useful information
2. **Enhanced** - online access to electronic versions of reports, laws and regulations, newsletters, download forms
3. **Interactive** - submit some applications online
4. **Transactional** - most services available 24/7 online. Citizen-centric portal. Supports electronic payment
5. **Connected** - integrated back office with horizontal connections (across agencies at same level) and vertical connections (across different levels of govt.)

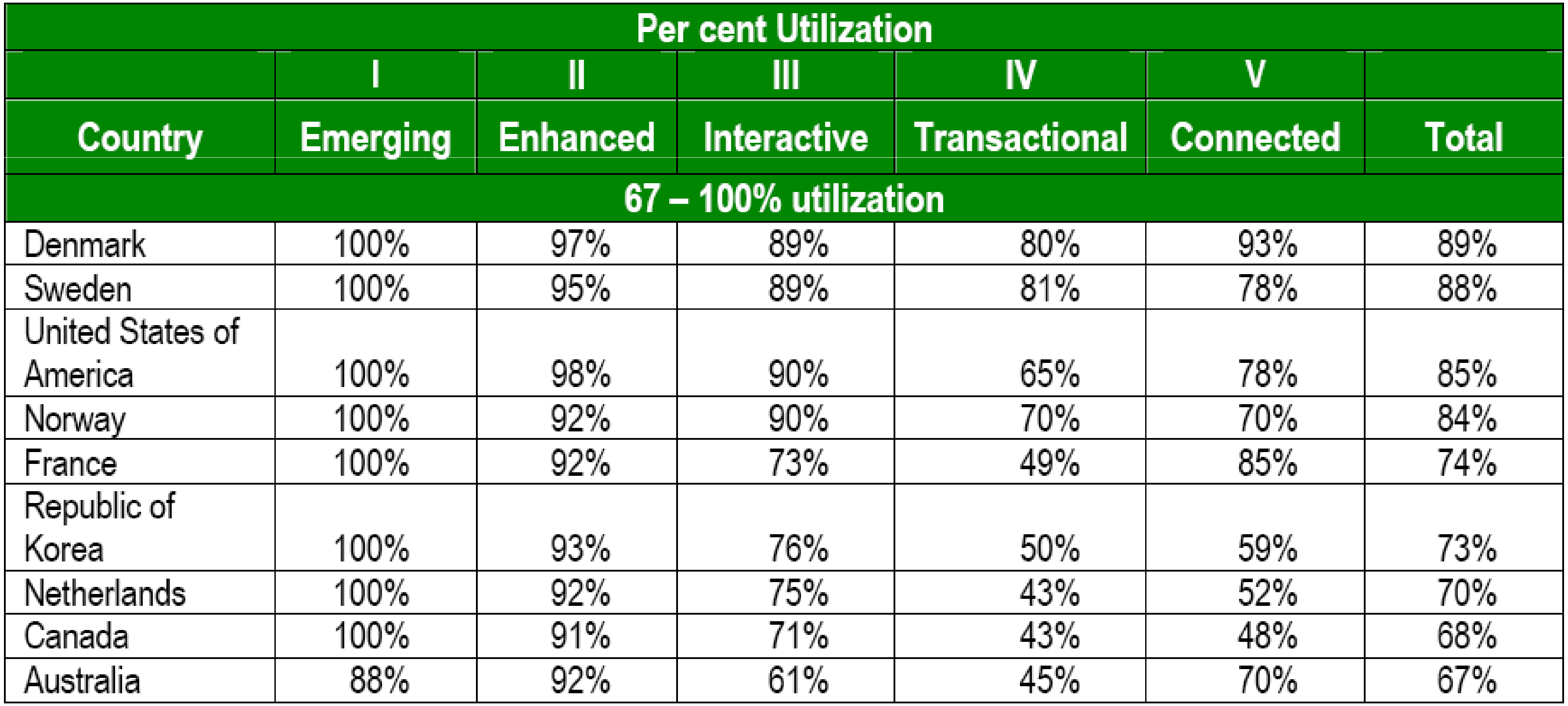


Source: UN E-Government Survey 2008, United Nations, New York 2008, available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf

E-Government Maturity

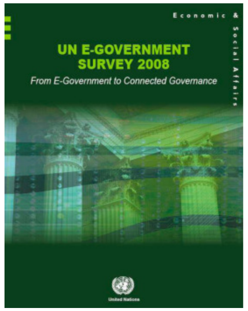

Economic & Social Affairs
UN E-GOVERNMENT SURVEY 2008
From E-Government to Connected Governance
United Nations

- Top UN Countries ordered by phases of e-government development
  - Utilization is services provided electronically as percentage of total services

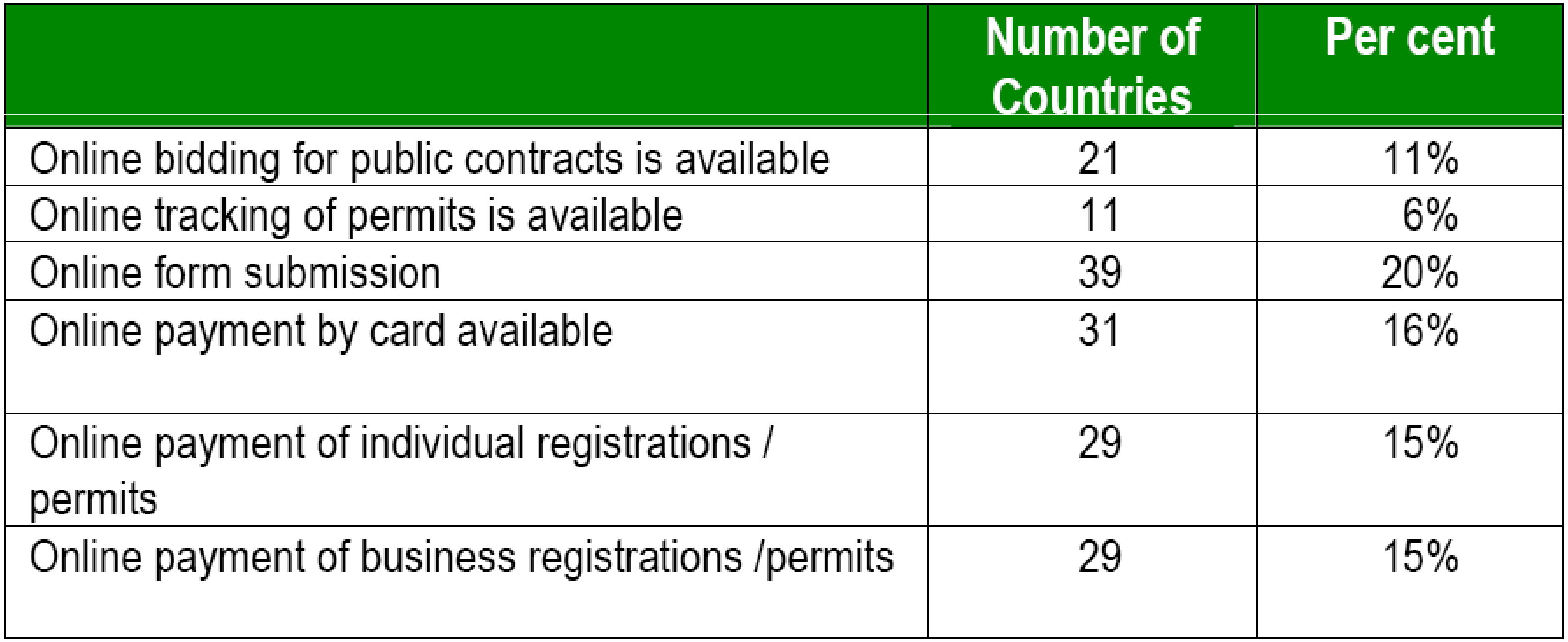


Per cent Utilization						
	I	II	III	IV	V	
Country	Emerging	Enhanced	Interactive	Transactional	Connected	Total
67 – 100% utilization						
Denmark	100%	97%	89%	80%	93%	89%
Sweden	100%	95%	89%	81%	78%	88%
United States of America	100%	98%	90%	65%	78%	85%
Norway	100%	92%	90%	70%	70%	84%
France	100%	92%	73%	49%	85%	74%
Republic of Korea	100%	93%	76%	50%	59%	73%
Netherlands	100%	92%	75%	43%	52%	70%
Canada	100%	91%	71%	43%	48%	68%
Australia	88%	92%	61%	45%	70%	67%

E-Government Uptake


Economic & Social Affairs
UN E-GOVERNMENT SURVEY 2008
From E-Government to Connected Governance
United Nations

- Number of countries whose national website offers transactional services
  - 2008 survey of 191 UN member nations



	Number of Countries	Per cent
Online bidding for public contracts is available	21	11%
Online tracking of permits is available	11	6%
Online form submission	39	20%
Online payment by card available	31	16%
Online payment of individual registrations / permits	29	15%
Online payment of business registrations /permits	29	15%

Source: UN E-Government Survey 2008, United Nations, New York 2008, available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf

E-Government Challenge - Data Silos

- Most data collected by public sector is still stored in agency silos that are not effectively interconnected
- Causes considerable handling inefficiency, out-of-date, erroneous, duplicate data
  - Ad hoc sharing without formal process and procedure is common (e.g. burn it on a CD and post)
  - Ad hoc arrangements can be dangerous!
    - UK Nov 2007 - CD containing the entire database of 25 Million child benefit recipients maintained by Her Majesty's Revenue and Customs (HMRC) lost in the post enroute to the National Audit Office
    - The data was not encrypted

Toward Connected-Up Government

- Current scenario:
  1. A set of autonomous information repositories
  2. Independent security frameworks for each information repository
  3. Separate authentication and authorisation frameworks for each information repository
- Main challenge is how to integrate existing possible heterogeneous systems while preserving their autonomy

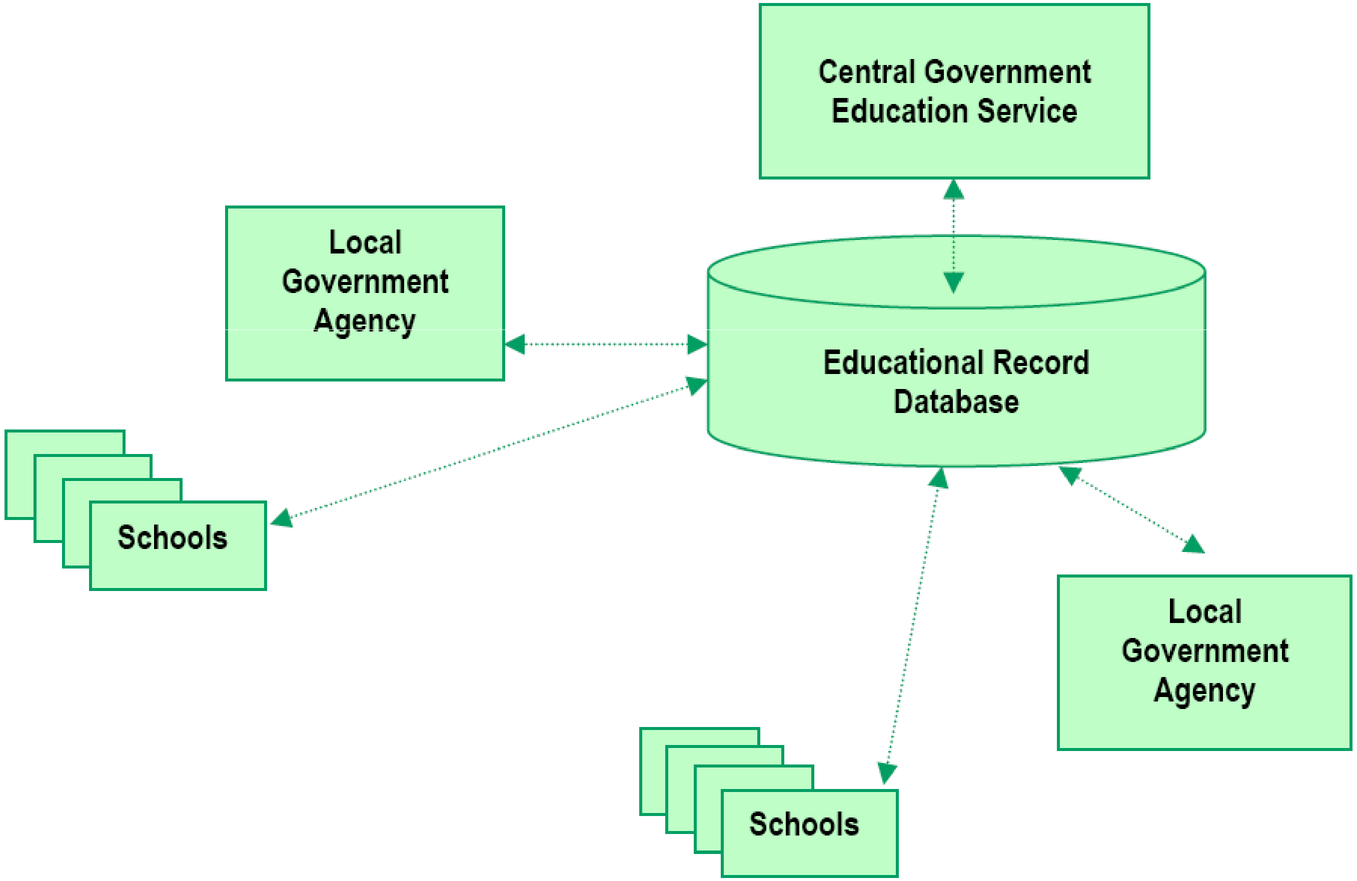
Back-Office Re-engineering

- Current silo-based back-office design hinders delivery of e-services:
  - Back office systems control the internal operations of a department or agency
  - Not generally visible to the public
  - Not originally designed to interact with external entities
  - Not originally designed to interact with other govt. departments!
- Delivery of citizen-focused e-services is not possible without integration of *back-office* government systems

Back-Office Re-Engineering

- There is a need to re-engineer back-office processes to deliver services that reflect the needs of citizens and business
  - Support horizontal cooperation/integration between agencies at the same level
  - Support vertical cooperation/integration between different levels of government
  - Support cooperation/integration with external stakeholders (including the commercial and private sector)
- Service Oriented Architecture (SOA) and Web Services are the dominant re-engineering pattern/technology/framework

Vertical Integration Example

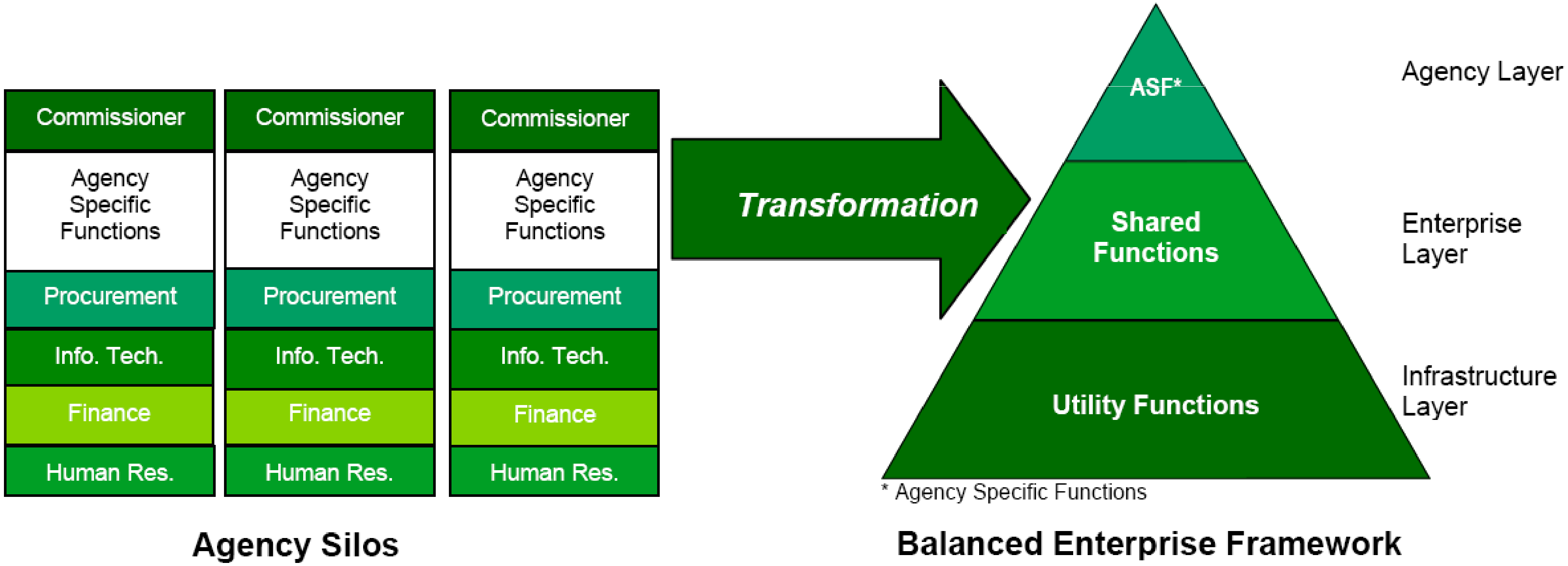

Central Government Education Service
Local Government Agency
Educational Record Database
Schools
Schools
Local Government Agency

Source: UN E-Government Survey 2008, United Nations, New York 2008, available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf

Connected-Up Government

"An effective connected government is about a 'bigger and better' front-end with a 'smaller and smarter' back-end".

Source: Jeremy Millard. ePublic services in Europe: past, present and future: Research findings and new challenges. Available at ftp://ftp.cordis.europa.eu/pub/ist/docs/epublic-services.pdf



Commissioner	Commissioner	Commissioner
Agency Specific Functions	Agency Specific Functions	Agency Specific Functions
Procurement	Procurement	Procurement
Info. Tech.	Info. Tech.	Info. Tech.
Finance	Finance	Finance
Human Res.	Human Res.	Human Res.

Agency Silos

Transformation

ASF*	Agency Layer
Shared Functions	Enterprise Layer
Utility Functions	Infrastructure Layer

* Agency Specific Functions

Balanced Enterprise Framework

Graphic source: UN E-Government Survey 2008, United Nations, New York 2008, available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf

Connected Government Challenge - Controlled Sharing

- Installing pipes to let the data flow is easy
- The hard part is controlling the flow - ensuring only authorised people have access for authorised purposes
- The bulk of electronic data stored by government is sensitive but unclassified.
  - For internal use
  - But only accessible where there is a ‘need to know’
- Advantage of Silos: indirectly enforce ‘need to know’
- How do you enforce ‘need to know’ when the data pipes of connected up government are installed?
  - ‘Need to know’ changes very quickly
  - How can the system keep up without expensive security administration?
  - Need to strike the right balance between availability and security - this is not easy!

E-Government & Security

Importance of Security for E-Government

“There may well be sound reasoning for governments taking a more cautious and gradual approach than their private sector counterparts, much of it security-related. The political risks of security breaches in government are often perceived to be far more serious than proportionally similar risks in the private sector context - a comparison most often attributed to the significantly greater holdings of personal and sensitive information”

Joshi, J. B. D., Ghafoor, A. and Aref, W. G. Security and Privacy Challenges of a Digital Government. In Advances in Digital Government – Technology Human Factors and Policy. Kluwer Academic Publishers, Boston 2002

Information Security

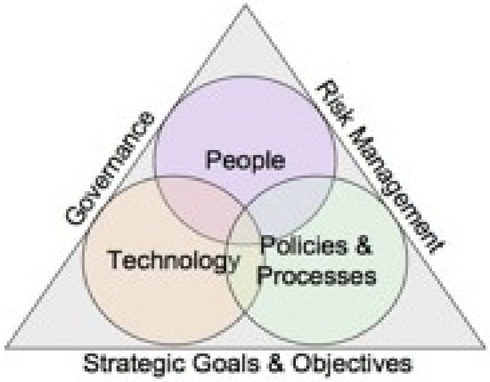
Definition: “the protection of information from a wide range of threats in order to ensure business continuity, minimize business risks, and maximize return on investments and business opportunities”

Source: AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management

Information Assurance

- Includes traditional information security:
  - – Processes that protect information and information systems by ensuring
    - Confidentiality, Integrity, Availability
- Plus greater emphasis on
  - + privacy protection
  - + governance and compliance
  - + Business continuity management
- Guided by strategic risk management

Information Assurance



- Information assurance is information security:
  - Practised in an organisational setting
  - As a continuous process (not implement and forget)
    - Continually evaluate the effectiveness of countermeasures as the environment changes
  - Less about tools and techniques
    - Emphasize defense in depth principles (people, processes and technology)
  - More about resilience and compliance

An Information assurance approach is vital for successful E-Government

IS to IA

- Why has there been a transition from information security to information assurance?
  - Common understanding of IS did not emphasize the **ongoing** nature of the process enough
  - Risk management did not inform IS practice sufficiently
    - Serious risks that had not yet resulted in harm were ignored
  - Perspectives of all stakeholders not given sufficient weight e.g. privacy
  - Much of what is known is not put into practice
    - Compliance and governance aims to address this

Information Security Objectives

- The preservation of **confidentiality** (ensuring that information is accessible only to those authorised to have access),
- The preservation of **integrity** (safeguarding the accuracy and completeness of information and processing methods)
- The preservation of **availability** (ensuring that authorised users have access to information and associated assets when required).

Source: AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management

Security Services: Authentication

- Prerequisite to ensuring all access is *authorised* and *accountable*
- For higher sensitivity information/services multifactor authentication required
  - – Passwords alone susceptible to phishing and keystroke logging
  - – Hardware tokens (usb, smart card, one time password generator)
    - provide higher assurance of claimed identity
    - Challenge: more expensive and harder to manage

Security Services: Access Control

E-Government systems need to make sure that the right people have quick access to the right information without exposing a risk that information might leak to unauthorised persons

- Consequences of public disclosure of sensitive and personal information
  - Sensational media reports of vulnerability that alarm the public
  - Security breaches damage public confidence
  - Affected individuals suffer inconvenience, financial loss or worse!
- needs flexible access control models to make security administration more efficient

Access Control (contd)

- E-Government systems host a large number of users from 100’s of different departments and organisational entities (citizens and government employees)
- Employees have access based on ‘need to know’
  - ‘Need to know’ is based on their role within their organisation
  - Access rights need to change as roles change
  - Rights need to be revoked when employment changes
- Major Challenge: keeping access rights for individuals up-to-date as they change roles and employers
- Solution: Federated identity and attribute management – tap into standards-based identity management systems of participating organisations
  - Access policy languages (e.g. XACML) that express authorisation policies as predicates involving attributes of subjects, objects and the environment

Risk Management for Information Security

Risk Concepts

- *Assets*: things of **value** worth protecting
- *Threats*: potential damaging **events** that put assets in danger
- *Impact*: the potential **outcome** of a threat that materializes and causes harm to assets
- *Vulnerabilities*: **characteristics** of operational procedures or systems that will allow a **threat to materialise** and exploit an asset, causing an impact
- *Risk* = F(Impact, Likelihood)
- *Likelihood* = F(Probability of threat event, Probability that controls fail)

Source: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

Risk Management Process

- High level view of a commercial risk management process:
  1. Identify information assets
  2. Identify threats to assets
  3. For each threat, identify and quantify the impact if the threat materialises
  4. For unacceptable impacts, identify vulnerabilities that could allow associated threat to materialise
  5. Select possible controls to reduce threats, vulnerabilities or impacts
  6. Assess costs and benefits (e.g. impact reduction) of potential controls
  7. Apply controls that have net benefit

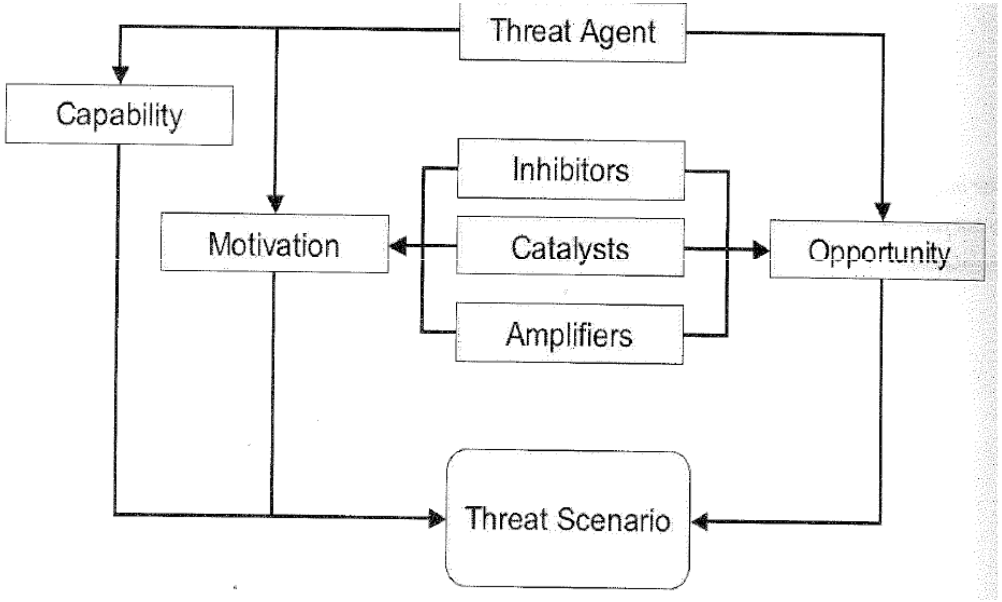
Source: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

Threat Assessment

- Detailed threat assessments are very difficult to do rigorously:
  - Statistical analysis is of little use for estimating threat probability for infrequent events
  - Past events are not necessarily a good indication of future events
  - Considering potential threat scenarios can help
  - This is an active research area

Threat Scenario Framework

- Inhibitors - factors that deter the threat agent e.g. fear of detection & prosecution
- Catalysts - Events or circumstances that trigger the threat agent to act e.g. employment termination, gambling debts
- Amplifiers - Factors that encourage agent to act - e.g. availability of easy to use malware kit



Source: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

Threat Agents

- Natural events - floods, storms
- Accidental events - fire, explosion, structural collapse
- Technical failures - from wear and tear or poor design
- Individuals - human error, malicious acts
- External organisations - organised crime syndicates, competitors, state sponsored groups

Source: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

Threat Domains

- Internal People: losses caused by:
  - human error,
  - malicious violation of internal policies,
  - negligent violation of internal policies
- Processes: unintentional losses caused by:
  - Deficiencies in procedures/processes
  - Absence of procedures/processes
  - Failure to follow procedures/processes

Source: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

Threat Domains & Agents (cont.)

- Systems: unintentional losses caused by:
  - Unforeseen breakdown of technical systems (caused by ‘wear and tear’)
  - Insufficient resilience in technical systems (caused by poor design or implementation)
- External Events: losses caused by:
  - Natural disasters
  - Unintentional man-made disasters
  - Malicious actions of third parties
  - Negligent actions of third parties
  - Legitimate actions of third parties (with conflicting interests)

Source: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

Information Assurance Frameworks

- Examples of IA frameworks include:
  - ISO/IEC 27002
  - SABSA
  - FISMA

ISO/IEC 27002

- AS/NZS ISO/IEC 27001:2006 Information security management systems - Requirements
  - “provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)”.
  - “This Standard can be used in order to assess conformance by interested internal or external parties”.
- AS/NZ ISO/IEC 27002:2005 Code of practice for information security management
  - "establishes guidelines, and general principles for initiating, implementing, maintaining and improving information security management in an organisation"

SABSA

- "SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.”

Source: SABSA Website http://www.sabsa-institute.org/the-sabsa-method/sabsa-overview.aspx

SABSA Model

- “SABSA is a six-layer model covering all four parts of the IT lifecycle: Strategy, Design, Implementation and Management & Operations”
- SABSA has been designed to meet a wide variety of Enterprise needs including
  - Risk management
  - Information assurance
  - Governance, and
  - Continuity management

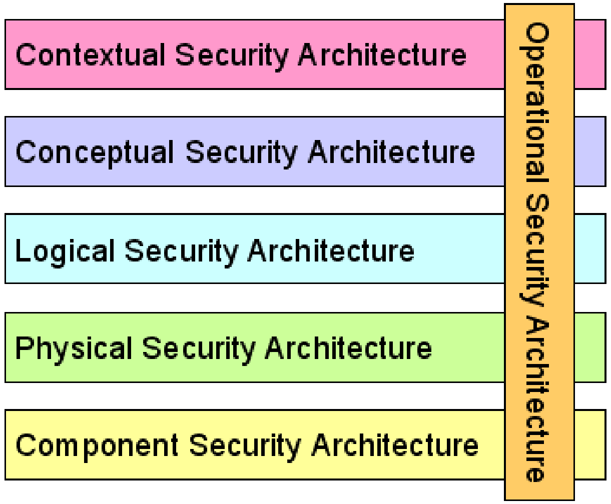

Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Operational Security Architecture

Image Source: http://www.sabsa-institute.org/the-sabsa-method/the-sabsa-model.aspx

SABSA References

- Original article: John Sherwood, SALSA: A method for developing the enterprise security architecture and strategy, Computers & Security, Volume 15, Issue 6, 1996, Pages 501-506 available at http://www.sciencedirect.com/science/article/B6V8G-3VWC5P1-6/2/2da03492bf34a2f6bea85b32ca323e46
- The SABSA model is presented in a book: J. Sherwood, A. Clark, & D. Lynas "Enterprise Security Architecture: A Business Driven Approach", CMP, 2005.

FISMA

- US has passed legislation to make information security management in federal agencies mandatory:
  - Title III of the E-Government Act (2002) - *Federal Information Security Management Act (FISMA)* requires each federal agency to:
    - develop, document, and implement an agency-wide information security program
    - For systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Source: http://csrc.nist.gov/groups/SMA/fisma/overview.html

FISMA

- FISMA framework includes:
  - Standards for categorizing information and information systems by mission impact
  - Standards for minimum security requirements for information and information systems
  - Guidance for selecting appropriate security controls for information systems
  - Guidance for assessing security controls in information systems and determining security control effectiveness
  - Guidance for certifying and accrediting information systems

Source: http://csrc.nist.gov/groups/SMA/fisma/index.html

Privacy Compliance for E-Government

Managing Personal Information

- Privacy compliance is a major security driver for E-Government
- Government agencies store lots of information about people
- Personal information needs to be handled according to relevant privacy regulation:
  - Generally based on Information Privacy Principles (IPPs) contained in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*
- IPPS regulate the way Government agencies collect, store, use and disclose personal information about individuals

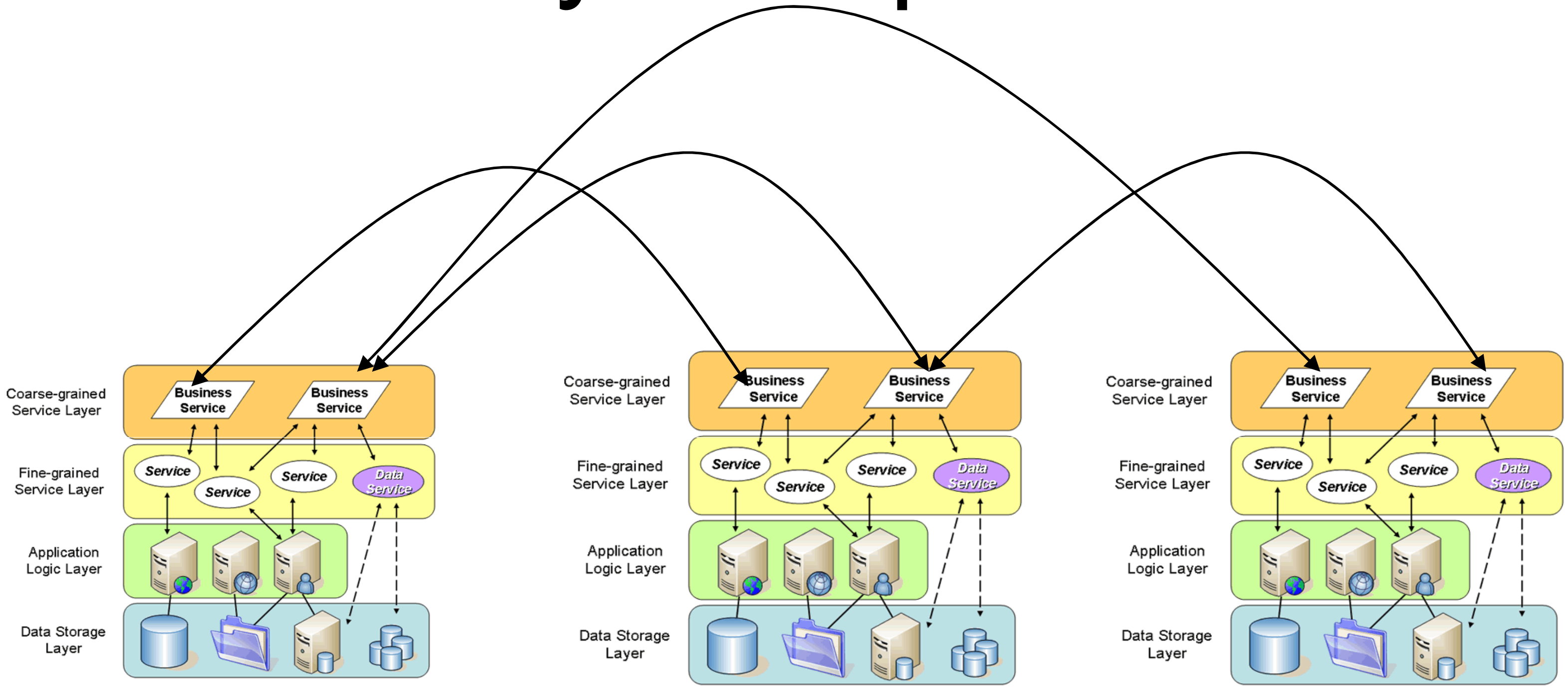
Purpose of Collection & Disclosure

- **Purpose Specification Principle** – Agencies must inform individuals who provide personal information of:
  - *the **purpose** for which the information is being collected*
  - *whether the information will be **disclosed** to another agency or organisation*
- **Security Safeguards Principle** – Agencies must protect records against loss, **unauthorised access**, use, modification or disclosure

Use Must be Consistent with Disclosed Purpose

- **Use Limitation Principle** - information that was obtained for a particular purpose shall not be used for any other purpose unless:
  - *the individual concerned has consented to use for the other purpose*
  - *Another relevant exception applies (e.g. imminent threat to life, law enforcement etc.)*

Connected-up Govt Makes Privacy Compliance Difficult



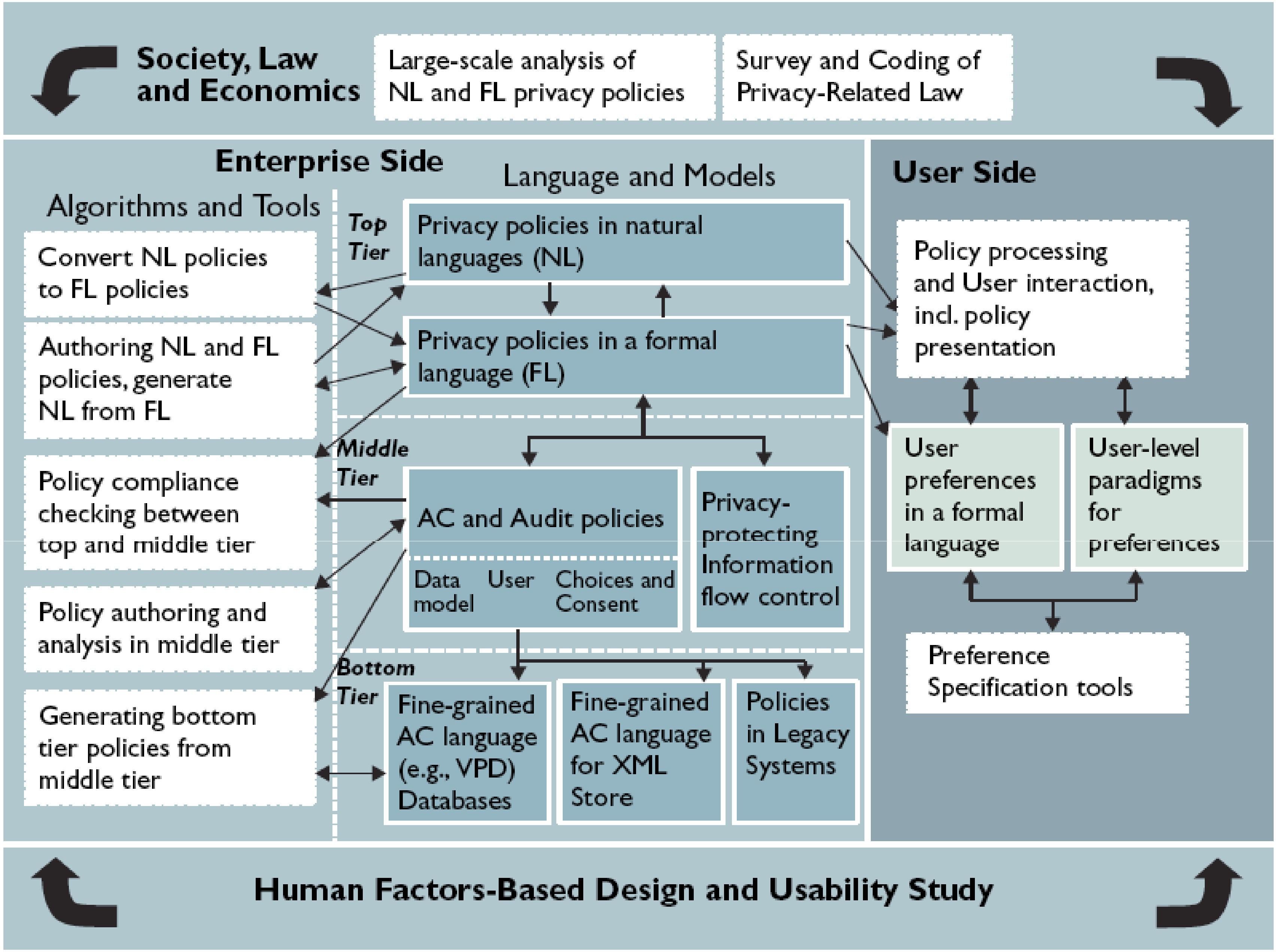
- SOA/Web services architecture supports dynamic composition of applications and services
- BUT dynamic flexibility makes information privacy compliance **difficult**
  - information can be used for **unanticipated purposes** by **unanticipated entities**

Compliance Problem

- How to ensure **privacy compliance** in the era of Web Services/SOA, connected-up government
  - Information can be easily searched for and accessed by entities other than the collecting agency
  - New applications can be dynamically composed
- Requirement: architecture and methods to automatically determine and enforce
  - Whether a **new purpose** is consistent with **disclosed purpose**?
  - Whether information about individuals can be disclosed?
  - This is an active research topic

Elements of the Solution

- Purpose metadata
  - Record and encode promises and representations made (in natural language) at time of collection
  - Need to translate natural language to formal language for enforcement and compliance auditing
- Purpose-based authorisation architecture
  - Use formal authorisation language to record and enforce purpose restrictions
    - XACML and EPAL are example languages that have been applied to privacy enforcement



Society, Law and Economics

Large-scale analysis of NL and FL privacy policies

Survey and Coding of Privacy-Related Law

Enterprise Side

Algorithms and Tools

Convert NL policies to FL policies

Authoring NL and FL policies, generate NL from FL

Policy compliance checking between top and middle tier

Policy authoring and analysis in middle tier

Generating bottom tier policies from middle tier

Language and Models

Top Tier

Privacy policies in natural languages (NL)

Privacy policies in a formal language (FL)

Middle Tier

AC and Audit policies

Data model

User

Choices and Consent

Privacy-protecting Information flow control

Bottom Tier

Fine-grained AC language (e.g., VPD) Databases

Fine-grained AC language for XML Store

Policies in Legacy Systems

User Side

Policy processing and User interaction, incl. policy presentation

User preferences in a formal language

User-level paradigms for preferences

Preference Specification tools

Human Factors-Based Design and Usability Study

Image source: Antón, A. I., Bertino, E., Li, N., and Yu, T. 2007. A roadmap for comprehensive online privacy policy management. Commun. ACM 50, 7 (Jul. 2007), 109-116. DOI= http://doi.acm.org/10.1145/1272516.1272522

Privacy GIS and Geocoding

- GIS offers a powerful way to search, analyse and represent diverse info:
  - Any object, entity, or concept that has a link to a physical location
  - Not just land use or geography!
- **Trend** - Governments are Geocoding databases:
  - Adding spatial coordinates to records that contain addresses
  - Addresses are a link that can be used to identify people
  - Spatial analysis can indirectly disclose or ‘create’ personal information

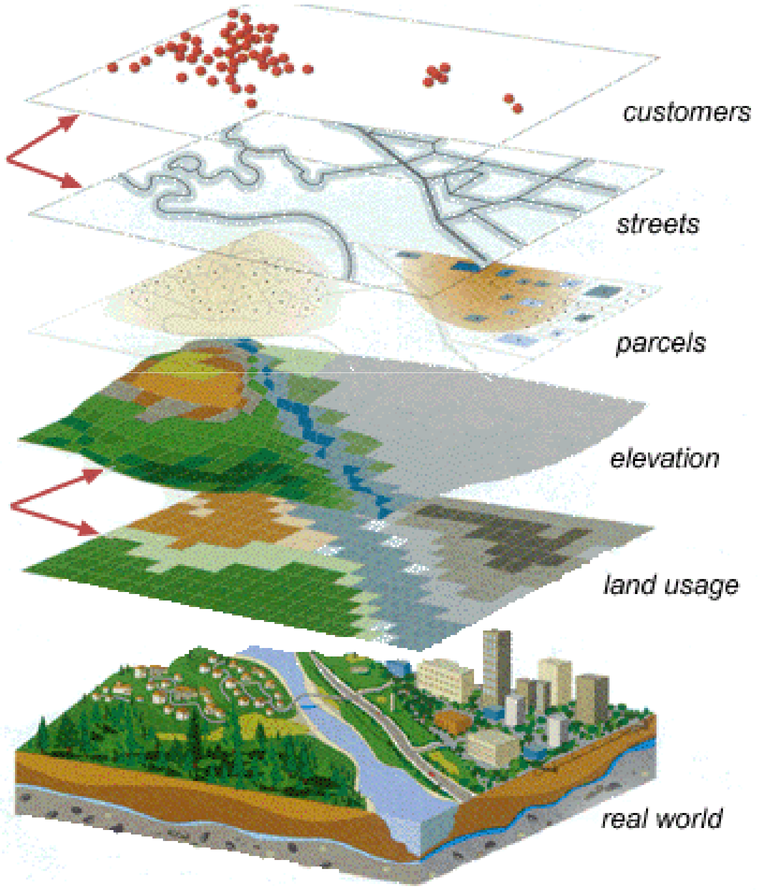


Image Credits: http://cier.uchicago.edu/gis/gis.htm

Privacy implications

- GIS + Data mining = Very difficult to effectively de-identify personal information while retaining its usefulness:
  - because correlations with other data reveal identity
  - Statistical techniques that introduce inaccuracy to hide individual data items have legal problems - publishing inaccurate data can lead to legal liability
  - It will be very difficult to secure the benefits of interconnected government and comply with privacy laws
- This will be a MAJOR CHALLENGE

Authentication & Identity Management

Authentication and Identity Management

- The issue of identity management is critical for connected-up E-Government
- Citizens and representatives of business entities need to be authenticated
- Government employees and contractors need to be authenticated
- Authorisation needs to be performed on the basis of authenticated attributes (Role, entitlement status, age, etc.)
- This is complicated in the setting of connected-up government - with its multiple cooperating entities

Current Models for Federated Identity Management

- Isolated
  - Agency with absolute authority
  - Tight control and simple but high load for management
- Centralised
  - Circle of trust with a single ID provider
  - Tight control with reasonable management effort
  - Suitable for large organisations under same authority
  - Easy for user
- Distributed
  - Common agreement and standards
  - Authentication & authorisation is distributed
  - Better flexibility, availability, manageability
  - Problems with cross recognition and complexity issues

Current Models for Federated Identity Management (Cont.)

Characteristic	Isolated Model	Centralised Model	Distributed Model
Flexibility	Low	Medium	High
Complexity	Low. Easy to implement as each service provider has its own security framework.	Medium due to the difficulty to achieve the common agreement between service providers.	High due to the high trust requirements, and difficulties in technical and legal issues.
Usability	High but only well suited for users with small number of identities	High. Well suited for service providers under single managements	High as the ability, in theory, to incorporate any large number of service providers
Management Cost for Service Provider	Low	Medium	High due to the management issues in cross-recognition of user identity and attribute, risk profile and security policy as well as efforts in maintaining consistency
Management Cost for User	High when user must manage a large number of identities.	Low	Low

Current Models for Federated Identity Management (Cont.)

- The main problem with the distributed model as shown above is the complexity issue.
- Further investigation is warranted with the aim of designing a less complex system while maintaining its benefits of flexibility, usability and low management costs.
- There are deployed two particular security models, namely Shibboleth and Liberty Alliance which each hold promise of either providing a full solution or a partial solution to the issue of managing identities across a federated system.

Shibboleth

- As a secure framework to enable single sign-on, attribute exchange and extended privacy protection mechanism, Shibboleth provides:
  - Federated Administration: A trust relationship is established between the Identity Providers and Service Providers. The Service Provider can rely on the credentials issued by the Identity Provider to make access control decision.
  - Access Control Based On Attributes: Access control decision are based on attributes of user’s identity rather than the actual identity

Shibboleth (Cont.)

- Active Management of Privacy: User has total control over which information user wants to release to the Service Provider as only necessary attributes are required for authorisation.
- Standards Based: By basing on SAML, Shibboleth is designed to be extensible and interoperable with other architectures such as Liberty Alliance.
- A Framework for Multiple, Scaleable Trust and Policy Sets (Federations): Shibboleth defines a common set of policies for a set of parties which has common agreement. This mechanism provides flexibility when federated activities require different sets of policies.

Liberty Alliance

- Liberty Alliance is a user-centric system as it allows users to actively decide whether they want to access a specified service provider without re-authentication.

Liberty Alliance (Cont.)

- The Liberty Alliance project defines 3 basic specifications which can be implemented together or independently:
  - Identity Federation Framework (ID-FF): provides the framework for single sign-on and account linking between member systems within a federation.
  - Identity Web Services Framework (ID-WSF): provides the framework to enable groups of trusted systems to link to other groups. More importantly, this framework allows users control over how their information is shared.
  - Identity Services Interface Specifications (ID-SIS): provides the framework to enable interoperable services on top of the ID-WSF.

Access Control in Shibboleth and Liberty Alliance

- Authentication and Identity Management:
  - each service provider, as member of the federation, maintains its own authentication mechanism and be responsible for the local identity management.
  - Shibboleth's identity is centrally stored and managed; only user attributes are exchanged between service providers for authorisation with alias management mechanism.
  - Liberty Alliance allows identity to be distributed.
  - The Liberty ID-FF domain discovery and Shibboleth WAYF mechanism are very similar in many aspects.

Access Control in Shibboleth and Liberty Alliance

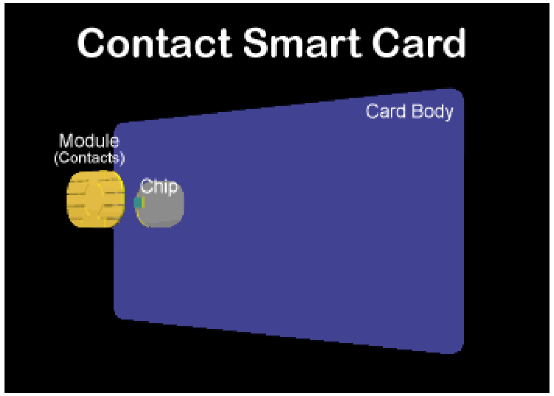
- Authorisation:
  - In general, in both approaches, each service provider controls its own authorisation mechanism.
  - In Shibboleth, the authorisation decision is made based on user attributes via Attribute Release Policies (ARP).
  - Liberty Alliance also supports this feature with the ID-WSF framework.
  - Account linkage is not supported in Shibboleth so user may only have one account on its home system which will be its identity provider.

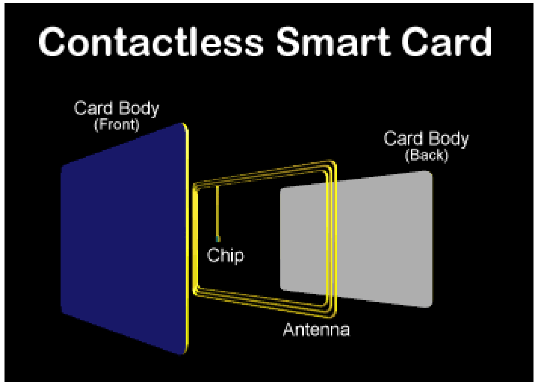
Shibboleth and Liberty Alliance

Feature	Shibboleth	Liberty Alliance
Targeted Environment	Education and Research Domain	General with focus on Business and Commercial Domain
Federation Strategy	Partner based Federation	Partners based Federation and Account Linkage Federation
Authentication and Identity Management	Identity information is centrally stored and managed. SSO is supported.	Identity information may be distributed. Alias management and SSO are supported.
Authorisation	Attribute information will be exchanged for authorisation. Account linkage is not supported	Attributed based authorisation is supported via ID-WSF.
User Information Privacy	Designed to enhance user privacy. However, user has little or no control over the attribute exchange process.	Designed to enhance user privacy. User has the flexibility to choose the identity providers and service providers. However, user has little or no control over the attribute exchange process.
Web Service Support	Not fully supported. Mainly, support SSO via web browser	Designed to support web service and web browser SSO.
Single Sign-Out	Not supported	Supported

Smart Cards and E-Government

What is a Smart Card?





Images courtesy of Gemplus

- Credit Card with embedded computer chip
- Contact or contactless designs
  - **Contact** cards inserted into a reader. Requires direct physical contact with the chip's plate
  - **Contactless** cards must pass within varying degrees of proximity to a smart card reader
  - Also hybrid

Smart Card Applications

- Identification
  - Passport / citizen Card
  - Driver’s Licence
  - Staff Card
- Health Care
  - Emergency info – allergies, blood type
  - Entitlement info
- Telecommunications
  - Mobile phone Subscriber Identity Module (SIM) card
  - Phone Cards
- Finance
  - Smart credit card
  - Stored value card
- Transport
  - Public transport ticket
  - Road Toll collection

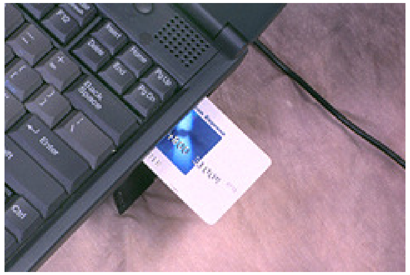
Why are Smart Cards Useful?

- Security
  - Secure storage
    - Cryptographic keys, PIN etc
    - Value – electronic cash, phone cards
    - Sensitive information – health data
  - Secure Processing
    - Crypto keys generated on card - stay on card
    - Decrement-only value registers
- Can be made difficult to counterfeit
  - Useful for ID

Smart Cards and Privacy Protection

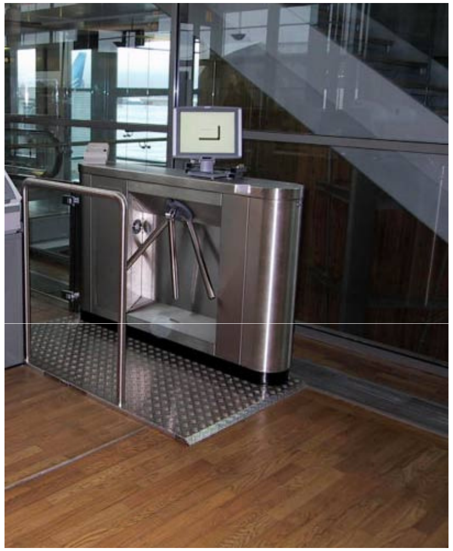
- **Enforce authenticated and authorized information access**
  - Protection of cardholder’s personal information through an intelligent interaction with the reader and verification system
    - Can verify the authority of the information requestor
    - Can provide *only* the information required by the transaction to an authorized requestor
- **Strong security**
  - Tamper-resistant
  - Unique ability to use active security methods that require on-card computations or interactions with the reader (e.g., symmetric and public key cryptography)
  - Contrast magnetic stripe - no computational capability

Smart Cards -Personal ID Systems



- Combine physical and digital identification and authentication
  - *Physical identification*: Visual printed information and security printing technologies
  - *Physical authentication*: cardholder biometric template stored on the card
  - *Digital identification*: Cardholder identity information stored on the card
  - *Digital authentication*: Cryptographic keys and digital certificates stored on the card

Why Smart Cards are Relevant to Privacy



- Decrease cost of data capture
  - Contrast:
    - Public phone and Mobile phone
    - Cash and stored value cards/credit cards
  - Increased data intensity - dataveillance
- Increase opportunity to collect data
  - Smart card ticketing and toll collection
    - tag on/tag off – time, date, where
    - Longitudinal data – cards are reloadable – collect data over longer time
    - Cards are identified – for auto-reload, concession, theft and loss protection
- Increased opportunity to cross link data
  - E.g. airline passenger risk assessment

Multi-application Cards and Privacy

- Business case often requires multiple uses for the same card e.g. Malaysian Multiapplication MyKad
  - Government applications:
    - national identity card (finger print biometric)
    - driving licence
    - passport information
    - national health application
  - Non-government applications:
    - e-purse 'MEPS Cash'
    - ATM application
    - digital signature application based on PKI
    - Loyalty Scheme
    - More to come……

Multi-application Cards – Issues

- Are the multiple uses compatible
  - Banking and health?
  - Drivers licence and loyalty scheme?
- Is data shared among application providers?
  - E.g. Change of address (convenience vs. segregation)
- Commercial applications not defined up front – can be added later
  - Function creep as a design feature

Multi-application Cards – Issues

- Commercial motivation and pressure to realize the value of transaction data
  - Users offered financial incentives to consent to secondary commercial use of their information
  - Price differences can remove effective choice
- Are extra applications really opt-in?
  - Preloaded and ready to (auto) activate
  - Pressure to use them because they're there

System Design and Privacy

- Privacy impact determined by the design of the system as a whole – not just the smart card
- Operational efficiency and cost often dictates design
  - Ease of issuing cards
  - Ease of replacing cards
- Privacy advantages are possible
  - Only store data on card – not in backend system
    - E.g. health data, biometric data
  - Doesn’t happen so much in practice
    - Management disadvantages – e.g. replace lost card particularly for multi-app card with many different organisations
    - Secure update of info more difficult

Privacy Positive Aspects

- Smart cards can support other cryptographic privacy enhancing technologies
  - E.g. Attribute authentication without identification (subscription status, concession entitlement, age)
- Anonymous electronic cash
  - Technically possible but hasn’t really taken off
  - Security risks favour fully accounted schemes

Privacy Trade-offs

- In the real world privacy must compete with other (valid) interests. Common Trade-offs
  - User convenience
  - Security (but for who?)
  - Decreased cost (implementation, management)
  - Access to information (risk mangement, profiling)

PKI Privacy – Issues

- PKI requires the ability to revoke certificates where the private key has been compromised
- Need to check that a certificate is still valid before relying on a signature
- Common way to do this is an online check to a certificate validity service – has this certificate been revoked?
  - History of validity enquiries allow profiling of behaviour/activities

Summary

- Smart Cards are a powerful technology
- An important element in an E-Government identity management solution
- If not correctly managed, they have the potential to increase the negative consequences of dataveillance
- Multi-application cards raise important, though subtle privacy issues
- The impact is largely determined by design and operational procedure – this is good news!

QUT isi
Information Security Institute

Biometrics

Harnessing the benefits whilst avoiding the dangers

Biometrics

- Seen as an attractive solution to many different problems:
  - Authentication (“Is this person who they claim to be?”)
  - Large scale identification (“Is this person in the database?”)
  - Screening (“Is this a wanted person?”)
- Role in locating terrorists and criminals, and combating fraud (welfare and identity)
- Accuracy problems in the past but technology is improving
  - fusion of multiple biometrics looks particularly promising

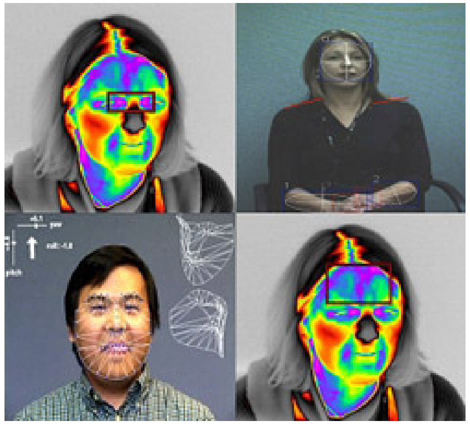
Biometrics

Image courtesy of Gemplus

- Individual-unique biometric information
  - Fingerprints
  - Hand geometry
  - Retinal or iris patterns
  - Facial characteristics
  - Voice prints
  - Gait
- Biometrics used with card technologies
  - Biometric template stored on the card
  - Can be matched on card

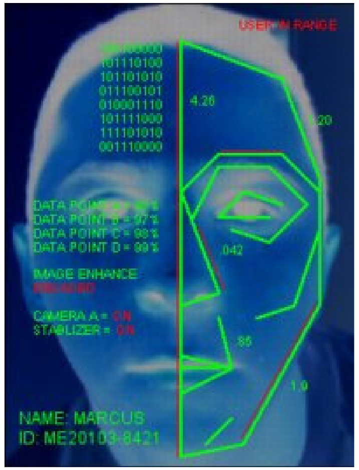
Biometrics in 10 years

- Trends:
  - Facial and voice recognition algorithms keep improving
  - Growth in processing power (computational grids) and cheaper storage
  - Increasing deployment of sensors (cameras and microphones) in public and private places
    - Retail shops, work place, public transport, private vehicles etc



What might happen?

- A company like Google pays private organisations to receive a feed from their cameras
- Facial and voice recognition algorithms used to identify persons (these don't require cooperation of subject)
- Enables physical movement and activity tracking - Google knows what you're doing, who you're with
- Combine with electronic data trail to improve profiling
- 'Minority Report' scenario may not be too far off.



Surveillance Implications

“Digital surveillance means there is no barrier to storing all footage indefinitely and ever-improving means of image-searching, in tandem with developments in face and gait-recognition technologies, allows footage to be searched for individual people. This will one day make it possible to `Google spacetime’, to find the location of an individual at some particular time and date.”

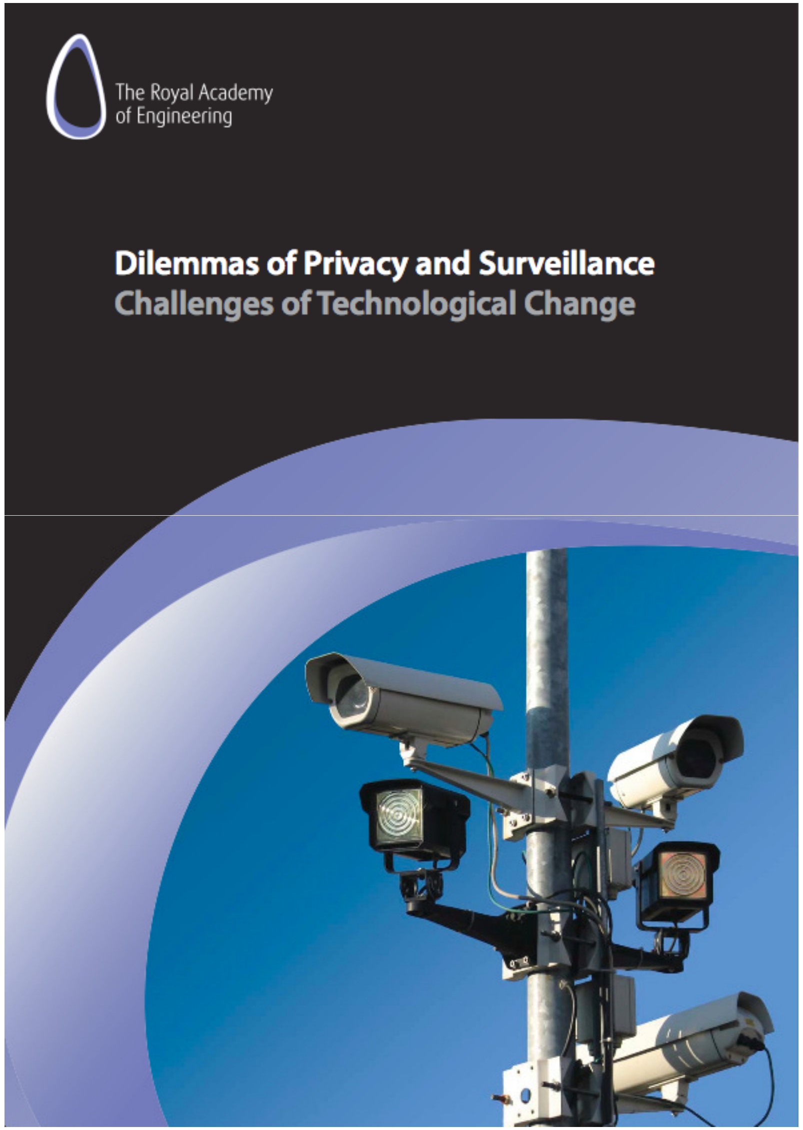
Dilemmas of Privacy and Technology, The Royal Academy of Engineering, 2007

Emerging Challenges

- We need to develop a legal, policy and governance framework:
  - Consistent with the principles of democratic society
  - Perceived need to be ‘doing something’ about terrorism, fraud and violent crime currently outweighs valid concerns with the long-term consequences of biometric adoption - a dangerous trend
- Biometric Cryptosystems
  - Cryptographic keys protected by what is ostensibly public information
  - Integration of biometrics with cryptographic protocols is an area of active research

Surveillance

- Tensions between benefits and privacy
- Development of technology should be monitored and managed so that its potential effects are understood and controlled
- Involves regulators, policy makers, businesses and individuals



The Royal Academy of Engineering

Dilemmas of Privacy and Surveillance

Challenges of Technological Change

Legal and Risk Issues in E-Government

Legal & Risk Issues

- The risk issues that can arise are:
  - Inter-operability between disparate information repositories that do not align;
  - Human Factors/Cultural issues;
  - Business Continuity Planning;
  - Information compromise: failure in the integrity of the system
  - Unauthorised disclosure of sensitive information
- As government commercialisation models mature so will the increased usage/dependency of the information held by governments. That is, commercial business decisions will be made on the basis that the information held by governments is both correct and commercially available.

Legal Issues (cont)

- Legal Liability
  - Non-availability of service.
    - This is a difficult issue because the aggregated information is dependent upon multiple sources. That is, if the information originates from multiple repositories then in order to get a true and accurate piece of information all of a repositories need to be available at the same time. Otherwise the lack of a component piece of information could distort the true situation which could create an unwanted legal liability.

Legal Issues (cont)

- Legal Liability
  - Incorrect information:
    - The publication of incorrect information which is later relied upon by some third party could also create a liability either in the common law doctrine of negligent misstatement or via some statutory liability like misleading or deceptive conduct on the part of the publisher.
    - It is not uncommon in many jurisdictions for the statutory obligation to be a strict liability: ie. intention is not an element. The mere publication of incorrect information is sufficient to warrant the liability.

Legal Issues (cont)

- Legal Liability
  - Compliance
    - Compliance issues also arise in situations where government agencies are obliged by legislation or regulation to act in a specific way. For example, the public good emanating from accurate recordkeeping by governmental organizations is recognized by the statutory obligations placed on agencies to record, maintain and destroy records within certain guidelines.

Legal Issues (cont)

- Legal Liability
  - Data Custodian Issues
    - A data custodian can be defined as a public official who has physical and legal custody of data and records on behalf of a corporate entity or government agency.
    - Data management responsibilities are concentrated in data custodians but data is held on behalf of organisations for the benefit of the public. As such, data custodians are essentially information trustees. This can create specific issues regarding:
      - **Archiving/information retention issues**
      - **Information classification issues (misclassifying)**
      - **Evidential responsibility (integrity & availability)**

Digital Archiving

- This is a non-trivial problem:
  - Issues:
    - What has to be archived:
      - Is it just the subject matter
      - Does it include the application that operates on the subject matter
      - What about hardware – does it affect the archiving issue
      - How do you maintain the long term integrity of the subject matter.

Information Classification

- In a federated system there needs to be a uniform information classification scheme that is applied uniformly across the federated system
- Alternatively – translation services may overcome non uniform classification schemes
- As the federation grows new participants need to be aware of the classification scheme.

Case Study: Security Frameworks for Electronic Tendering

Professor Ed Dawson

Dr Ernest Foo

Professor Sharon Christensen

Introduction

- Project Background
- Overview of Generic E-Tendering Process
- Generic E-Tendering System Design
- Security Issues
- Legal Issues
- Summary

Motivation

- Queensland government departments conduct tenders and contracts for over $600 million annually
- The use of Information and communication technology (ICT) has become commonplace within construction organisations
- The economic benefits that flow from the use of ICT, lead to a need for e-contracting guidelines
- The security and legal issues relating to the shift from a paper based tendering system to an electronic system need to be defined

Project Background

- Information in this presentation is based on the CRC for Construction Innovation Research Project on “E-tendering – Security and Legal Issues”
- Research was carried out by the QUT, with the assistance of
  - Department of Public Works
  - Department of Main Roads
  - Brisbane City Council
  - Crown Law
  - University of Newcastle

Research Outcomes

- An explanation of the government tendering process
- A review of current standards and e-tendering systems
- A summary of legal requirements impacting upon e-tendering
- An analysis of the threats and requirements for any generic electronic tendering system

Research Outcomes

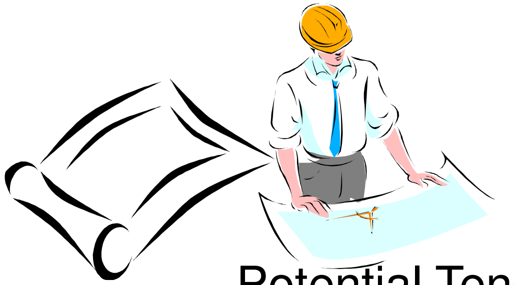
- The identification of outstanding security and legal issues
- An evaluation of possible electronic tendering implementation architectures
- Recommendations for developing electronic tendering systems

Introduction to e-Tendering

- Electronic Tendering follows normal tendering procedures, except documents are electronic and communications are via the Internet
- Electronic Tendering consists of the following steps
  - Pre-qualification and Registration
  - Public Invitation
  - Tender Submission
  - Close of Tender
  - Tender Evaluation
  - Award Tender

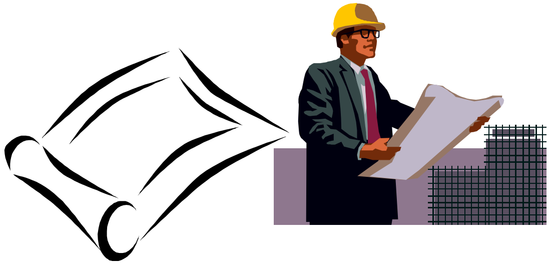
Pre-qualification and Registration

Potential Tenderers
Register with
the Principal



Potential Tenderer

Principal

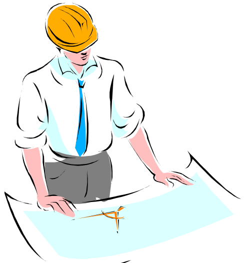


Potential Tenderer

Potential Tenderer

Public Invitation

Principal advertises
Tender to qualified Tenderers



Qualified Tenderer

Principal

Qualified Tenderer

Qualified Tenderer

Tender Submission

Tenderers submit tender documents

Qualified Tenderer

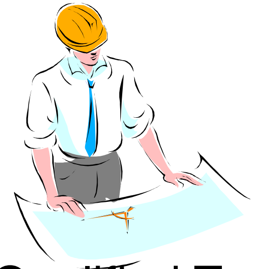
Principal

Qualified Tenderer

Qualified Tenderer

Close of Tender

The Tender Box does not allow Tenderers to submit documents and submitted documents are now available to the Principal



Qualified Tenderer

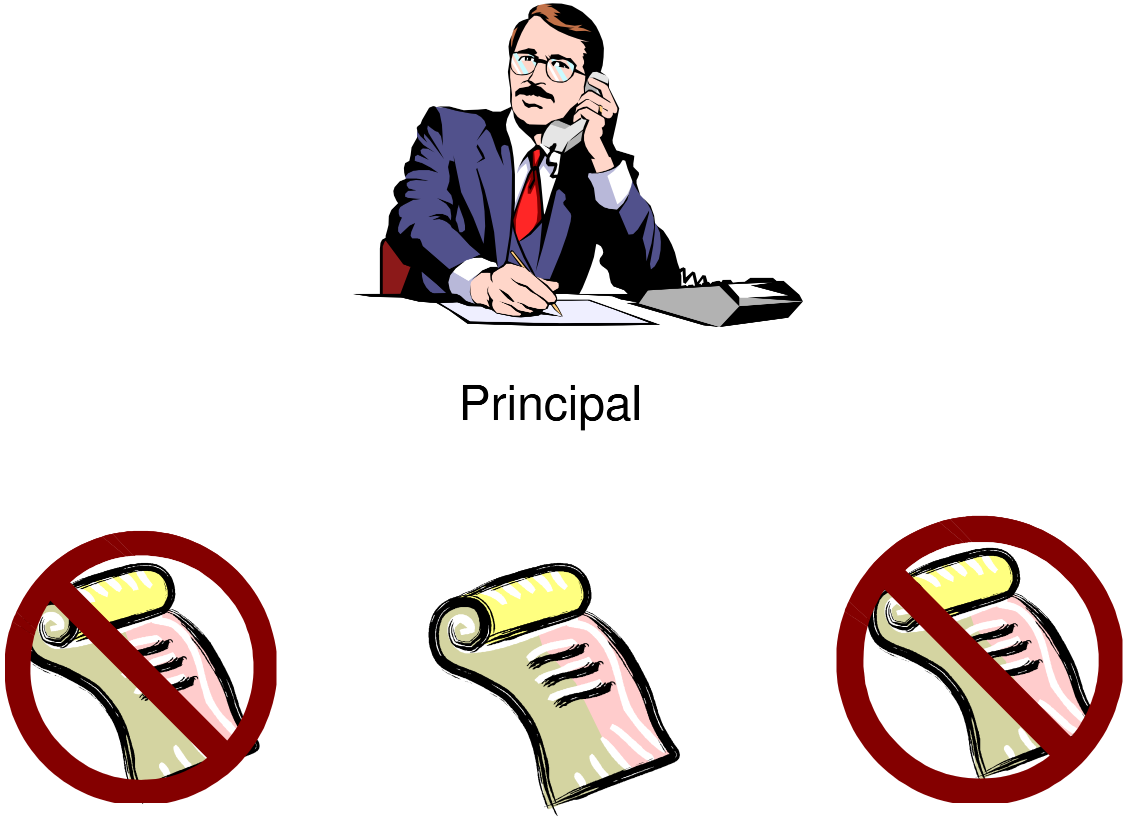
Principal

Qualified Tenderer

Qualified Tenderer

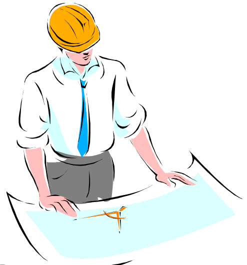
Tender Evaluation

The Principal evaluates the tender documents



Award Tender

Winning Tenderer is notified that they have won the tender



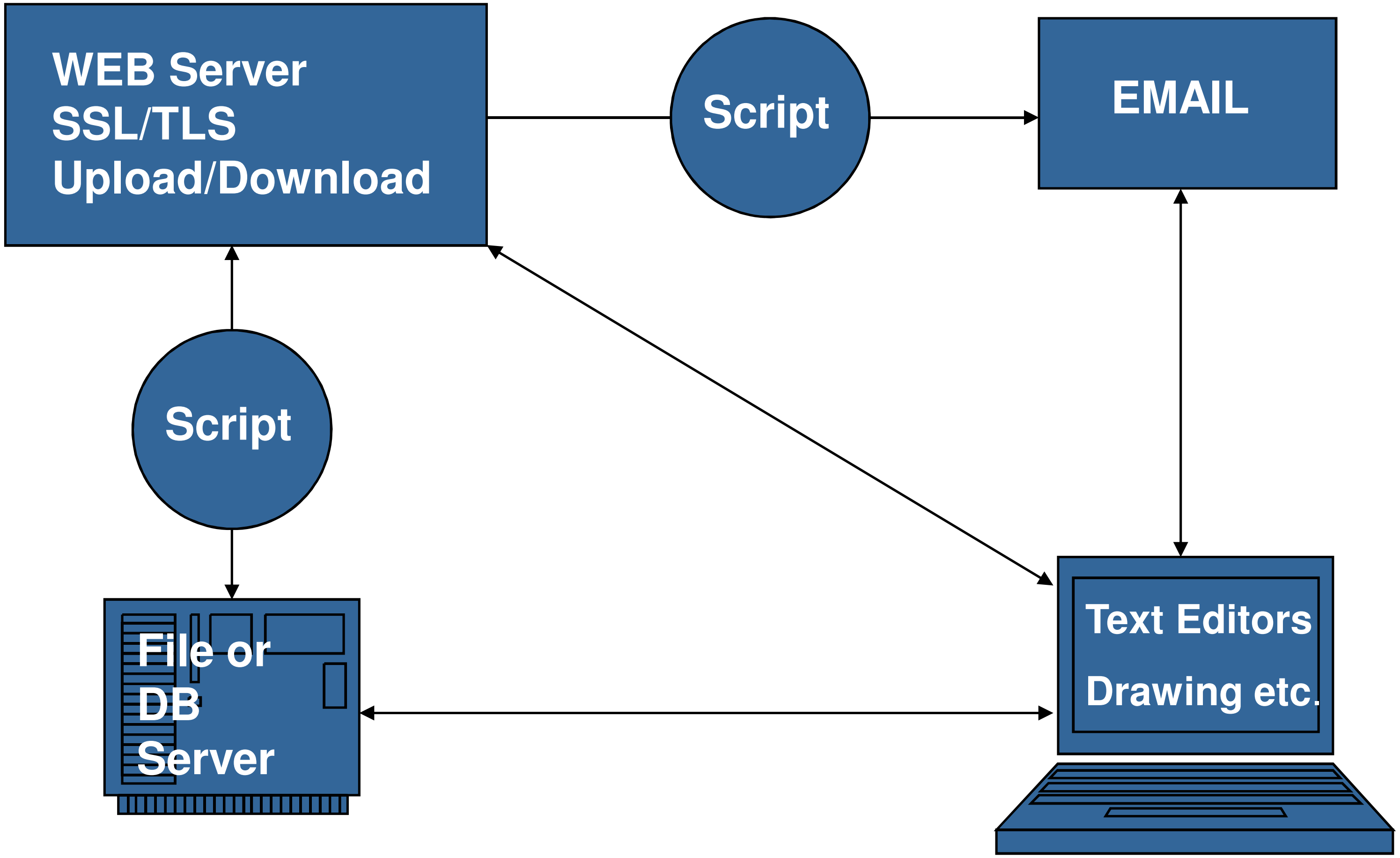
Qualified Tenderer

Principal

Qualified Tenderer

Qualified Tenderer

Generic System Design



QUT isi Information Security Institute

Security Issues

- **Basic security issues**
  - Confidentiality
  - Integrity
  - Authentication
- **Advanced security issues**
  - Compliance eg. legal, business
  - Threats to the business model
  - Evidence

Security Issues

How to integrate electronic tools to realize an e-tendering business process with security assurance

- Legal compliance, eg. tender closing time
- Ability to reduce tender collusion due to use social engineering, eg. the confidentiality of a submitted tender is unprotected before tender opening time
- Ability to generate reliable digital evidence to prove that the system provide assurance
- Whether suggested electronic tools or softwares provide the security mechanism we need

Security Issues Related to Electronic Communication

Intensive use of electronic communication

- email, web eg. browse business opportunity, request for information / negotiation

Problem

- No visual or voice identification
- Identify message originator, protect message integrity, protect confidentiality

Threats

- Masquerade, impersonate, repudiation, integrity violation, eavesdropping, unauthorized information access

Security Issues Related to Electronic Communication

SSL/TLS

- Provide confidentiality during transmission

Problems

- Submitted tender through web will be viewable when it reaches to the other end
- Can not identify message originator
- There is no integrity checking

Threats

- Basically any communication through web can be denied due to lack of message authenticity checking

Security Issues Related to Electronic Communication

Email

- – distribute user name password, addendums or request information

Problem

- – email server operate in plain text protocol
- – send email to distribute fake addendum to every other tenderers

Security Issues Related to Document Creation

Software

- Word, text editor, drawings

Problems

- Easy to update,
- Hard to maintain document integrity

Current industry practices

- turn digital data to paper based or PDF format document

Threats

- Integrity violation, repudiation

Security Issues Related to Document Creation

Once the digital document is stored, it poses threats to the integrity of print out

- Unless the print out document is signed and witnessed on every page, the print out does not provide any more integrity assurance than the digital one
- People can print out a changed copy to replace the previous print out
- PDF file can also be changed unless digital signature is performed in a proper way
- Without integrity assurance, documents can not be reliable evidence

Security Issues Related to Document Handling

Software and activities

- web, email, file server eg. file upload and download, distribute addendum, tendering submission, store and retrieve documents

Problems

- Tender submission issues such as time synchronisation and tender deadlines
- easy to change documents, integrity issues
- hard to control access (internal) eg. controlled viewing, printing

Threats

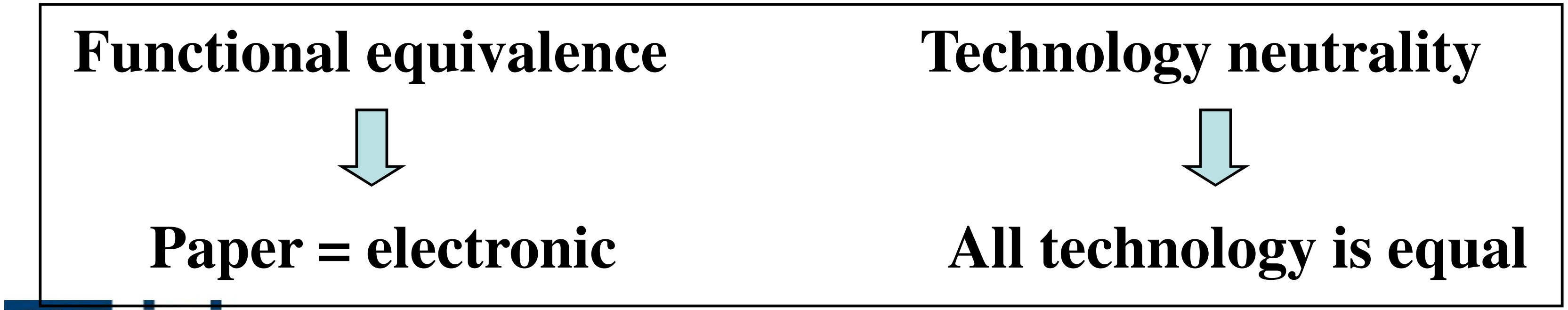
- Integrity violation, compromise confidentiality, collusion, disclose tender price or design

Electronic Transactions (Queensland) Act 2001

- Framed in substantially the same terms as Cth ETA with similar objectives
- Commenced 3 April 2001
- Applies to the law of the State
  - Applies to legislation and common law

Objectives of ETA

- Recognition of information economy
- facilitate use of electronic transactions
- promote confidence in electronic transactions
- enable use of electronic communication with government*



Functional equivalence ⇩ Paper = electronic

Technology neutrality ⇩ All technology is equal

Applications

- Requirements which can be met electronically:
  - Give information in writing
  - Provide a signature
  - Produce a document
  - Record information
  - Keep a document

Case Study 1

Issue: When is an electronic communication received?

Common Law

- When is an offer effective at common law?
  - Generally receipt
  - Can depend on terms of tender

ETA

- When is an electronic communication received under ETA?
  - S 24 time of receipt
    - When does a communication enter an information system?
    - How is an information system designated?
    - What is an information system?

Case Study 2

Issue - When is a contract created?

Common law

- General rule – at time of communication of acceptance
- Relevance of postal acceptance rule to email

ETA

- Does not alter CL rules only regulates receipt

Issue of time of creation of a contract by email or other electronic communication is unresolved.

Issue – When is revocation of an offer effective?

Common law

- At the time it is communicated
- Usually communicated through the same medium as the offer
- Only effective if given prior to acceptance

ETA

- Does not alter common law rules

Issue – When is acceptance effective?

Common law

- If general rule when communicated to offeror

ETA

- Is communication equivalent to receipt in s 24?
- If s 24 apply is it receipt when it enters the network of the principal or at time downloaded to computer of relevant officer?

Case Study 3

- **Issues**
  - – Can a corporation challenge a contract for lack of authority of an officer?
  - – Can an individual challenge a contract for lack of authority of an agent?

Common law

- Open question
  - – If principal is not put on notice about misuse of private key and acted in good faith – tenderer probably bound
  - – If execution is akin to forgery the result may be different

ETA

- S 26
  - Bound to a communication (unless otherwise agreed) only if sent:
    - By originator; or
    - with authority of originator (actual or ostensible)
- When is a communication ‘sent by the originator’?
- Will PKI assist with identification and prevent repudiation?
- Does prequalification assist?

Case Study 4

Issues:

- How can the contents of an e-document be proven?
- How can the integrity (ie no amendments) of an e-document be proven?
- How should the principal archive/store documents?
- How should e-documents be produced in court?

Summary

- Off-the-shelf products are not going to address all security issues in an e-tendering system
- The e-tendering system security assurance can only come from
  - understanding your system requirements eg. business, legal
  - full assessment of softwares chosen
  - understanding threats imposed on using e-tools and on business model
  - be prepared to integrate new technology

High Assurance ICT for E-Government

High Assurance ICT

- Some E-Government functions deal with highly sensitive information:
  - Planning for new transport corridors requiring land resumption
  - Criminal justice matters
  - Health care

Persistent access control - motivation

- Traditional access control enforcement architectures are inadequate for a highly sensitive information
  - they fail to provide ongoing control over information once it is transferred to the client platform of an authorised user (e.g. possible to email controlled document after downloading)
- Sensitive information requires persistent ongoing control over usage and dissemination
  - Regardless of where information resides
  - Robust control over local save, print, email etc.
- Persistent access control is a form of Digital Rights Management
  - Also known as Enterprise Rights Management (ERM) when applied to documents
  - Implementing robust ERM remains a serious technical challenge

Persistent Access Control (ERM) Functionality

- Uses industry standard encryption of the information – access control enforced by controlling distribution of cryptographic keys
- Provides usage protection, such as controlling copy & paste, preventing screen shots and printing
- Offline use allowing for users to create/access ERM sealed documents without needing network access for certain periods of time
- Full auditing of both access to documents as well as changes to the rights/policy by users

Persistent Access Control - Background

- Cryptography can protect digital information when it is stored or transmitted
- Information ‘bits’ must be *in the clear* to be rendered in a perceptible manner on the user’s computing platform
- Persistent access control assumes that these plaintext bits can be protected from access by the rendering platform owner/administrator
  - This is an access control problem
  - A difficult problem to solve for open computing platforms (PC) where the owner/administrator has control over the local platform software environment

Persistent Access Control - 2

- Persistent access control assumes complete trust in the environment that manipulates plaintext or keys
  - The remote system authority must be able to trust:
    - The “Editor/Viewer” client application (it directly enforces the access policy e.g. whether a document can be printed)
    - The local Operating System which supports the client application (because an application cannot be more secure that the operating system which provides and controls its resources)
  - This is a difficult problem on an open computing platform that can run arbitrary software: it requires requires robust domain separation
  - Mainstream, commercial operating systems do not provide robust domain separation, e.g. a kernel debugger or malicious device driver can access application memory hence plaintext

Persistent Access Control -3

- Persistent access control on open devices requires a reliable way of reporting the current software configuration
- If the system authority trusts this configuration, keys to decrypt protected information ‘bits’ can be released by trusted hardware
- Requires trusted OS + trusted hardware (TPM)

OS Weaknesses Undermine Persistent Access Control

- Client applications running on current commodity operating system architectures cannot reliably enforce persistent access control policies
- Commercial operating systems including Unix, Linux and Microsoft Windows implement a protection model known as identity based discretionary access control (DAC).
  - A process executes with all of the privileges of its associated principal (user)
  - A user cannot control what their programs can do with their documents and files
  - This makes malware very effective and dangerous

Threats to Persistent Access Control

- Threats against client platforms connecting to E-Government networks are the most difficult to deal with:
  - A malicious program **accesses authentication secrets** of a user - enables impersonation of the user at a later time.
  - A malicious program running on a user machine **accesses information** stored on the network while a valid user session is active and stores it locally or sends it over the network to another machine.
  - A malicious program running on a user machine **modifies information** stored on the network while a valid user session is active.

Need for a Trusted Platform

- Client platforms that connect to the E-Government network will need to be able to deal with these threats
- Client platforms based on current commodity operating system architectures cannot adequately defend against these threats
- Nodes that deal with sensitive information should be based on higher assurance operating system architectures that can be trusted to enforce the required policies at all times
- Configuration of the platform must be measured and attested before network connection is established
- Protected information must be stored and transferred in encrypted form
  - only decrypted in a known trusted environment which enforces usage controls.
- Requires use of Trusted Computing Technologies

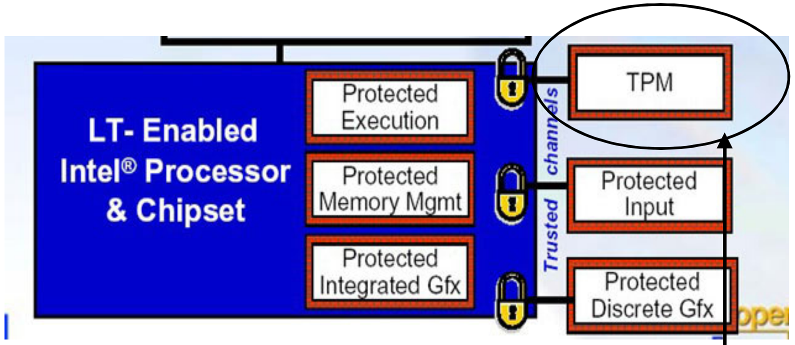
QUT isi
Information Security Institute

Trusted Computing Technologies : A vital ingredient for Sensitive E-Government Services

3 Key Trusted Computing Technologies

1. Trusted Computing Group (TCG) specification (2002) for Trusted Platform Module (TPM) and interfaces
   - Hardware module attached to computing platform
   - Uses public key crypto for platform and software authentication
2. Security Focused Operating Systems
   - Implement a *mandatory* protection architecture - less susceptible to malware and Trojan horses
3. Intel and AMD: new CPU instructions to support Hardware Virtualisation
   - Allows multiple operating systems to share the same CPU
   - provides hardware enforced protected execution environment

Technology 1: TPM



TPM security services

1. Protected Storage
   - HW storage for cryptographic keys
2. Sealed Storage
   - Release authentication or decryption key only if platform state is OK
3. Remote Attestation
   - Report current software environment to remote challenger
   - Aims to address problem of platform owner config control – can change but platform must report new config honestly
   - Challenger can decide if platform is configured to enforce security policy

TPM requires tight integration with platform chipset for services to work securely

TPM – Relevance

- Supports authentication of computing platform to sensitive E-Government networks
  - Physical device authentication – imposter devices can’t connect
  - Authentication of *approved* software stack including OS and client application used to access sensitive network and services
    - Network connection can be refused if authentication fails
    - Protects against connection by malware infected client
  - Hardware-protected storage for cryptographic keys used to encrypt sensitive information
    - Supports confidentiality, integrity and non-repudiation requirements
- BUT …. TPM cannot fix mainstream OS security problems (which are a consequence of the DAC protection architecture)
  - This requires a secure OS with a different protection architecture…

Technology 2: Security Focused OS

- Provides Mandatory Access Control:
  - confinement of information based on confidentiality and integrity requirements
  - confine user programs and system processes to the minimum amount of privilege they require to do their jobs (i.e., not based on DAC: no concept of a "root" super-user)
  - Provides a higher level of protection against malicious software including Trojan horse software

Security Focused OS – Relevance

- Can be used for both server and client platforms
- Less susceptible to software based attacks
- Can be difficult to configure and manage as a general purpose OS - Not necessarily a big problem though:
  - – Client platform: by using virtualisation, OS and client application can be tightly integrated and distributed together – a *software appliance* – very little configuration required
  - – Server platform: inconvenience is worth it for extra security

Security Focused OS - Examples

- Sun Microsystems – Trusted Solaris
- NSA-developed SELinux
- Aesec Inc’s GEMSOS general purpose security kernel
- XTS-400 (Using STOP OS) by BAE Systems

Technology 3: Virtualisation

- New CPUs from Intel and AMD – now widely available
- Intel Virtualisation Technology (VT) and Trusted Execution Technology (Formerly known as Intel LaGrande):
  - consists of hardware extensions (new cpu instructions) to allow for the creation of “multiple separated execution environments”
- AMD processors have equivalent capability
  - AMD-V extensions (formerly known as ‘Pacifica’)

Hardware Virtualisation

- Run multiple operating systems on a single CPU concurrently
- Virtual Machine Monitor (hypervisor) ensures each virtual machine is isolated from others
- Hypervisor controls access to actual hardware using special CPU instructions

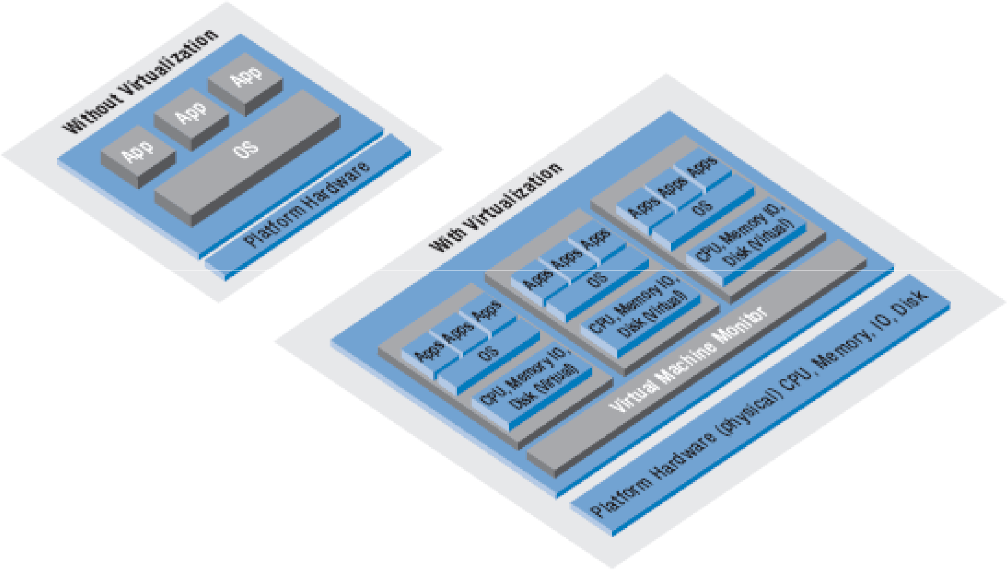
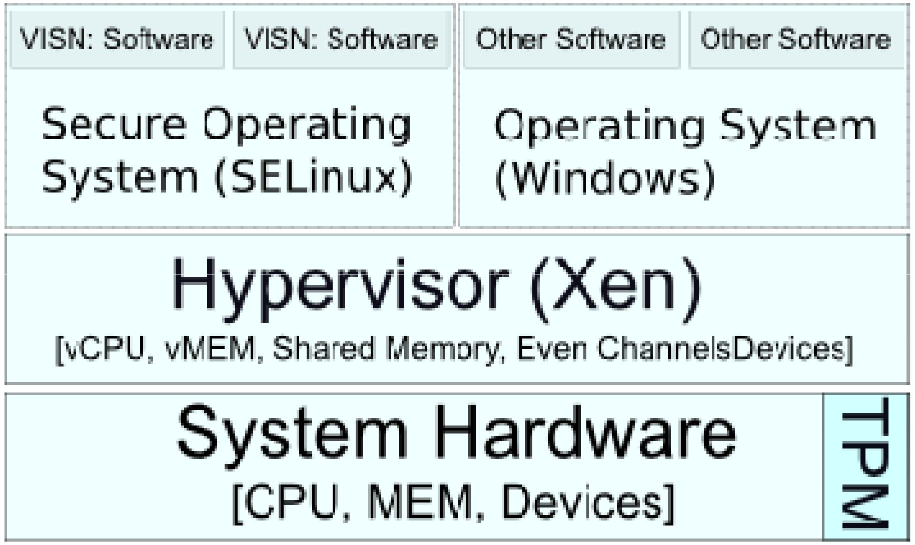

Without Virtualization
App
App
App
OS
Platform Hardware
With Virtualization
Apps Apps Apps
OS
CPU, Memory IO, Disk (Virtual)
Apps Apps Apps
OS
CPU, Memory IO, Disk (Virtual)
Apps Apps Apps
OS
CPU, Memory IO, Disk (Virtual)
Virtual Machine Monitor
Platform Hardware (physical) CPU, Memory, IO, Disk

Image credits: Intel available at
http://www.intel.com/technology/magazine/computing/platform-2015-0305.htm

Virtualisation: Relevance

- Run sensitive client application on a standard desktop/laptop computer alongside existing (Windows?) OS and applications
- Client has its own dedicated secure OS in its own isolated execution space
- Use TPM to authenticate (attest) hypervisor + Secure OS + client software before allowing connection to network
- Hypervisor provides hardware enforced domain isolation


VISN: Software

VISN: Software

Other Software

Other Software

Secure Operating System (SELinux)

Operating System (Windows)

Hypervisor (Xen)

[vCPU, vMEM, Shared Memory, Even ChannelsDevices]

System Hardware

[CPU, MEM, Devices]

TPM

Opportunity: Packaging Sensitive applicaiton software + Secure OS as an integrated *Software Appliance* makes remote attestation using TPM more feasible

Examples of Hypervisors

- Xen (Open source hypervisor)
- Microsoft's Hyper-V (released in June 2008)
- Citrix XenServer
- VMware's ESX Server

Some Commercially Available Information Sharing Products

Secure Information Sharing Architecture (SISA)

- SISA is an alliance of major ICT vendors specifically focusing on cross organization information sharing architecture.
- The architecture is based on off the shelf products from Cisco, Microsoft, EMC, SwanIsland, TITUS, Liquid Machines and others
- Principally concerned with the needs of government, military coalitions and emergency response communities, called *communities of interest*.
- It focuses on connecting existing computing infrastructure with the support of legacy applications.

Secure Information Sharing Architecture (SISA)

- SISA pursues a defence in depth strategy, relying on well-understood technologies such as VPNs, firewalls and VLANS to secure lower layers of the communications stack.
- However it has some short comings :
  - Not a lot of technical information available – *Whitepaper Analysis*
  - Doesn’t appear to be taking full advantage of trusted computing technologies
  - SISA doesn’t adequately address client platform security issues
    - Operating system vulnerabilities remain so malware is still a major problem
    - Relies on Host-based intrusion prevention – highly susceptibility to false positives
  - Most of the Commercial products used in SISA target Microsoft Applications (windows, office)

Liquid Machines: Overview

- Provides the ERM capability in the SISA architecture
- Provides a suite of applications to enable document protection in shared environments
- Based on Windows Rights Management Services (RMS)
- Their applications are integrated to Microsoft products (e.g., Windows, Office), some of Adobe products and CAD
- They assume clients are “trusted”. So they don't address the platform threats mentioned earlier

Liquid Machines: Features

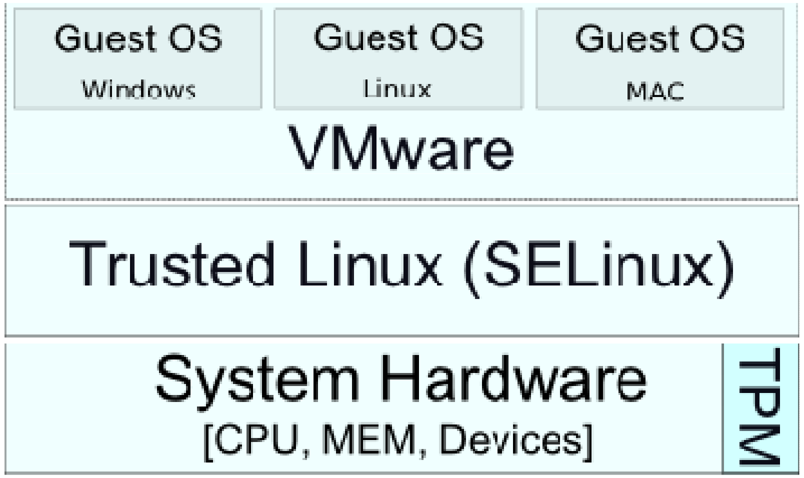
- Document Control: specify policies that control who can read, edit and print sensitive documents
  - Policy specification interface
- Dynamic policy control:
  - Rights can be revoked and content can be expired – even to remote users.
- Offline support: policies are enforced while documents are accessed offline.
- Detailed logs and audit trails of document content access and usage

Other SISA ERM Focused Companies and Products

- EMC
  - – Access Management
  - – Federated Identity
  - – Digital Certificate Solutions
- TITUS Labs
  - – Document/Email classification services
- SwanIsland
  - – TIES: Web 2.0 information sharing services

Virtualisation Architectures: NetTop

- Originally developed by NSA
- Hewlett Packard licensed NetTop from NSA in 2003
  - HP Develops and sells NetTop as a commercial product
- Main focus: Defense MLS environments
  - NetTop users can access networks at different sensitivity levels from a single workstation (by using different VMs)



Case Study

Information Sharing for Critical Infrastructure Protection

ARC Funded Research Project

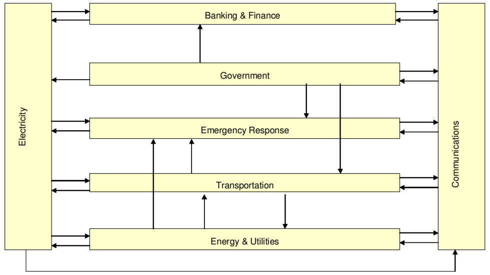
Australian Government
Australian Research Council

- Project Title: Technical and Legal Models for Virtual Info-Sharing Networks (VISN) for Critical Infrastructure Protection (CIP)
- Three year project 2007-2010
- Research team includes:
  - Legal specialists (Competition, FOI, Privacy)
  - Technical infosec specialists (Network security, trusted computing, access control etc.)

Case Study Overview

- Background: Critical Infrastructure Protection
- CIP information sharing in Australia
- CIP information sharing in US
- CIP information sharing in Israel
- Summary

CIP Introduction



- Modern societies are increasingly vulnerable
  - Technologically/economically
  - Because of reliance on infrastructures
    - telecommunications, energy, transportation, etc
    - critical to advanced societies
    - infrastructure exhibits vulnerabilities (including interdependence)
    - threats from malicious actors, accidents/errors/faults, natural disaster etc.
  - Potential for consequences that have national security implications
  - Protecting national security is the most basic responsibility of a nation’s government

QUT isi Information Security Institute

CIP Challenges

- Majority of critical infrastructure is owned, operated and supplied by private interests
  - In Australia as much as 90% of CI is privately owned
  - Consequence: Government does not directly, unilaterally discharge its national security responsibility
  - Why? - Businesses are responsible for securing their assets and managing risk

CIP - a Cooperative Effort?

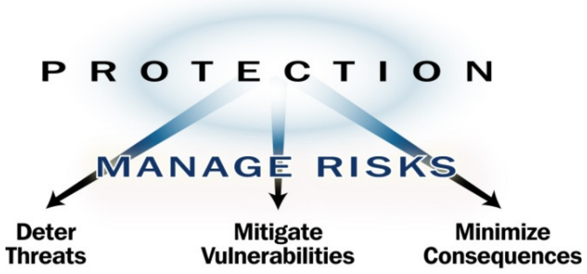
- Two competing CIP perspectives:
  1. National security perspective (government is responsible - safety is paramount)
  2. Business continuity perspective (business and 'the market' responsible - economic efficiency, shareholder value paramount)
- Each perspective is important and valid
- Each perspective has a different view of risk (particularly high consequence - low probability risks)
- Reconciling these perspectives is a challenge!
- Pragmatic reality: effective infrastructure protection requires
  – sharing information and coordinating responses to threats among various stakeholders: owners and operators, regulators, industry associations, professional bodies
- Information sharing model and arrangements will reflect the balance that is struck between the two perspectives

CIP in Australia

Highlights

- CIP involves a public/private partnership with voluntary private sector participation
- Business continuity perspective on CIP dominates
- Australia takes an all-hazards approach to CIP - not focused around counter-terrorism
  - Natural disasters seen to present an equal or greater threat
- Australia does not have a centralised department (like US DHS) concerned with security and CIP
  - Functions are spread across a range of departments and agencies

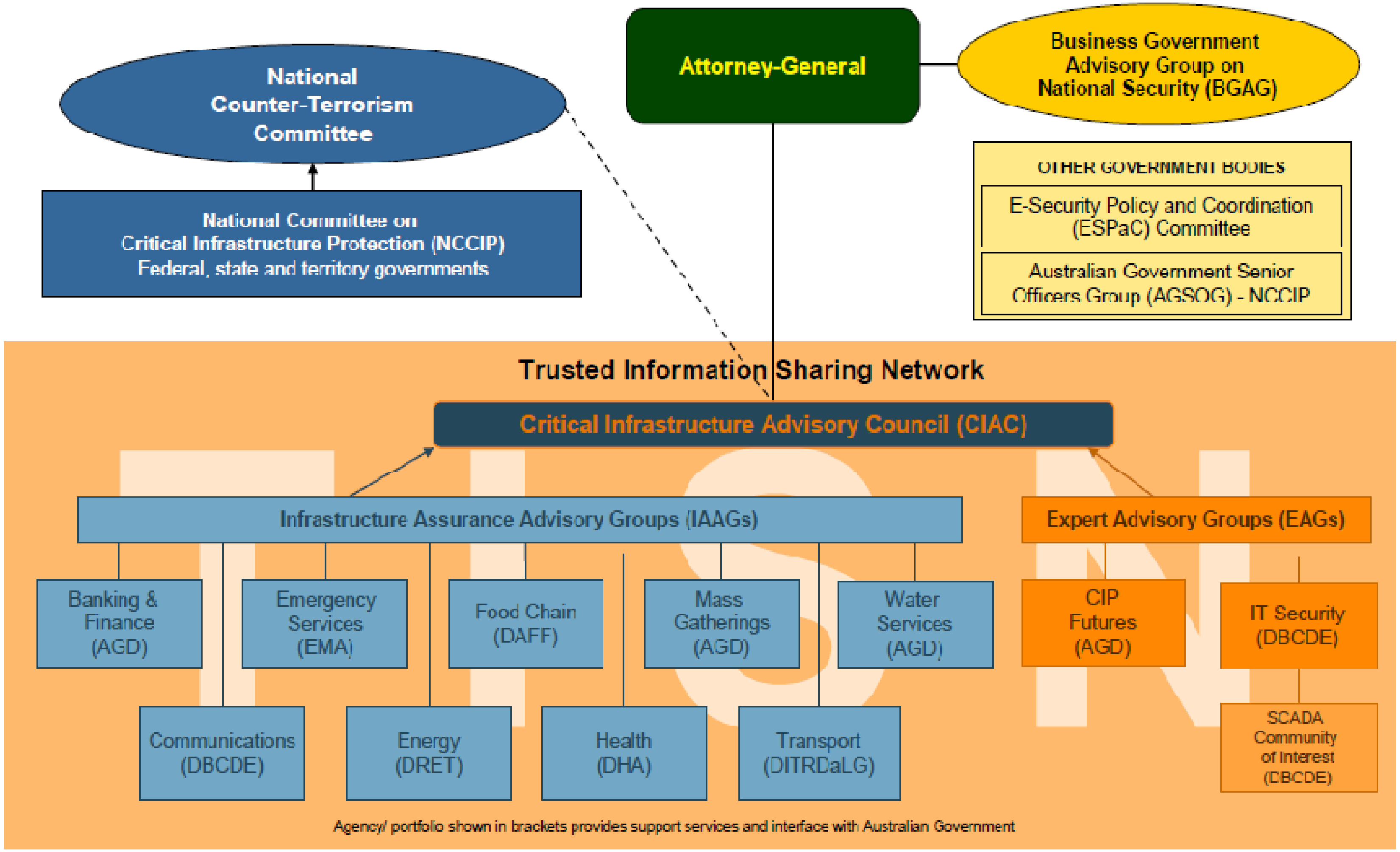
TISN



- Trusted Information Sharing Network formed in 2003
- Purpose: Allow CI stakeholders to share information on:
  - Information system attacks and vulnerabilities
  - E-crime
  - Business continuity
  - Consequence management
  - Protection of key sites from attacks and sabotage
  - Chemical, biological and radiological threats to water and food supplies
- Sharing of threat and vulnerability information assists stakeholders in managing risk
- TISN Strategy – building trust through personal relationships and face-to-face meetings

Trusted Information
Sharing Network
for Critical Infrastructure Protection

TISN Structure



National Counter-Terrorism Committee

National Committee on Critical Infrastructure Protection (NCCIP)
Federal, state and territory governments

Attorney-General

Business Government Advisory Group on National Security (BGAG)

OTHER GOVERNMENT BODIES

E-Security Policy and Coordination (ESPaC) Committee

Australian Government Senior Officers Group (AGSOG) - NCCIP

Trusted Information Sharing Network

Critical Infrastructure Advisory Council (CIAC)

Infrastructure Assurance Advisory Groups (IAAGs)

Banking & Finance (AGD)

Emergency Services (EMA)

Food Chain (DAFF)

Mass Gatherings (AGD)

Water Services (AGD)

Communications (DBCDE)

Energy (DRET)

Health (DHA)

Transport (DITRDaLG)

Expert Advisory Groups (EAGs)

CIP Futures (AGD)

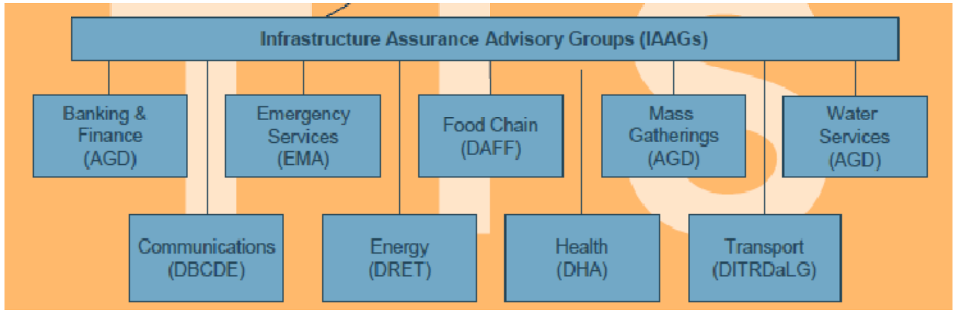
IT Security (DBCDE)

SCADA Community of Interest (DBCDE)

Agency/ portfolio shown in brackets provides support services and interface with Australian Government

TISN: Infrastructure Assurance Advisory Groups

- IAAGS are the principal vehicle for private sector participation
- Relevant Govt. Dept. also participates in each IAAG
- Businesses share information with each other
- Government shares information with business sector
- 9 IAAGs based on business/industry sectors
  - Banking and Finance
  - Communications
  - Emergency Services
  - Energy
  - Food Chain
  - Health
  - Mass Gatherings
  - Transport
  - Water Services
- IAAG participants attend regular face-to-face meetings



TISN Regulatory Arrangements

- TISN membership is voluntary
- Formation of TISN did not require enabling legislation
- No specific legislation passed to protect sensitive information or limit liability through participation
  - Australian Government position is that existing exemptions are sufficient
  - Contrast with US approach: *Homeland Security Act (2002)* explicitly protects voluntarily shared critical infrastructure information
    - FOI exemption
    - Prevents government and 3rd party use of info in civil actions against the information provider
- “Regulation may be considered however if the business-government partnership fails to adequately protect critical infrastructure”

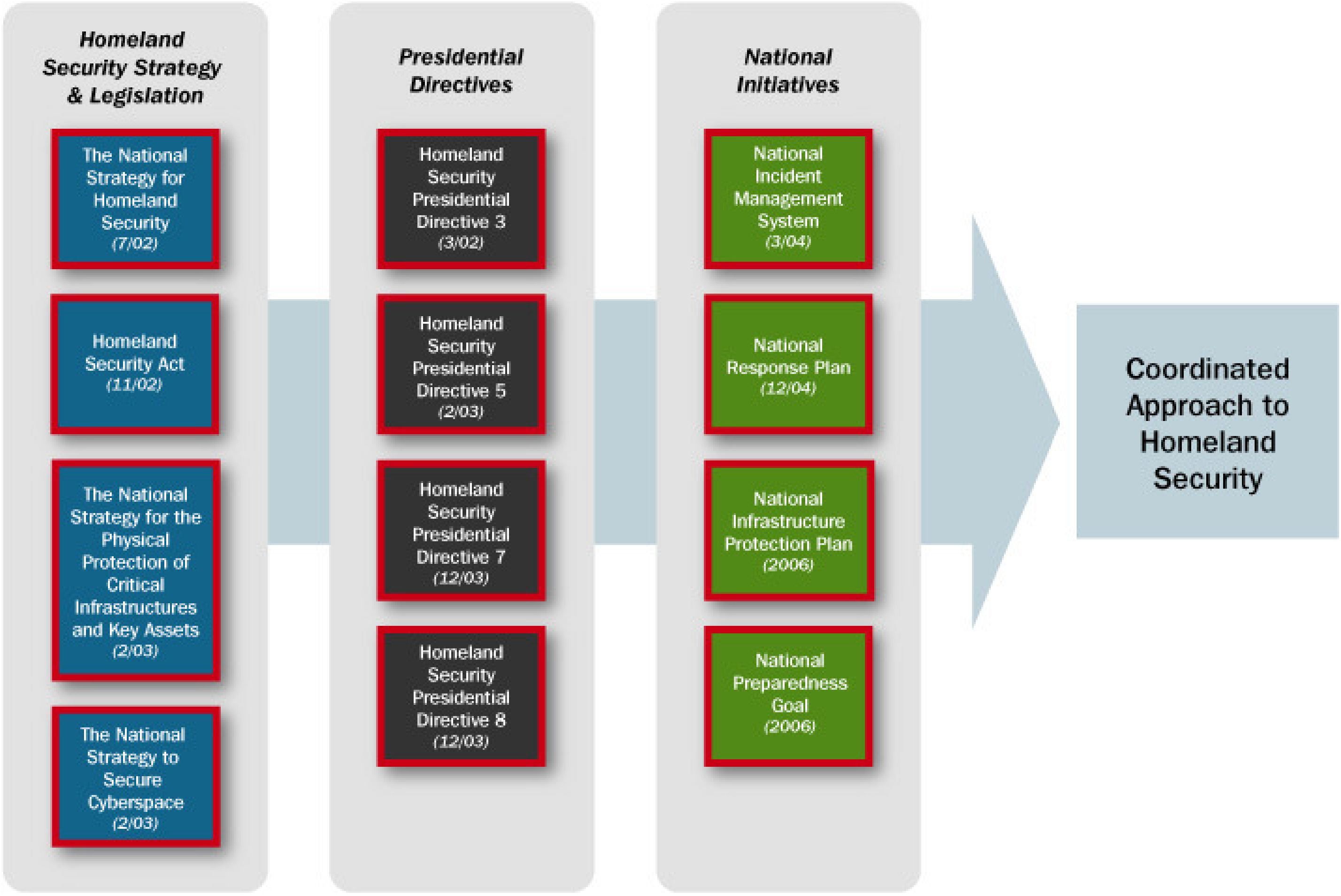
TISN - Critical Infrastructure Protection National Strategy Version 2.1, 12 March 2004
http://ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~National+CIP+Strategy+2.1+final.PDF/$file/National+CIP+Strategy+2.1+final.PDF

CIP in US

Highlights

- CIP policy heavily influenced by terrorist attacks - 9/11
- Counterterrorism concerns dominated restructuring of US Federal Government to form DHS - has overarching authority for CIP
- Specific regulation enacted to facilitate information sharing and CIP
- Some direct regulation of CI operators - but voluntary self regulation preferred
- ICT used extensively to support sharing (e.g. HSIN)
- Public/private sector partnership for information sharing through sector-based ISACs and SCCs

Legislative & Policy Framework



Homeland Security Strategy & Legislation

- The National Strategy for Homeland Security (7/02)
- Homeland Security Act (11/02)
- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2/03)
- The National Strategy to Secure Cyberspace (2/03)

Presidential Directives

- Homeland Security Presidential Directive 3 (3/02)
- Homeland Security Presidential Directive 5 (2/03)
- Homeland Security Presidential Directive 7 (12/03)
- Homeland Security Presidential Directive 8 (12/03)

National Initiatives

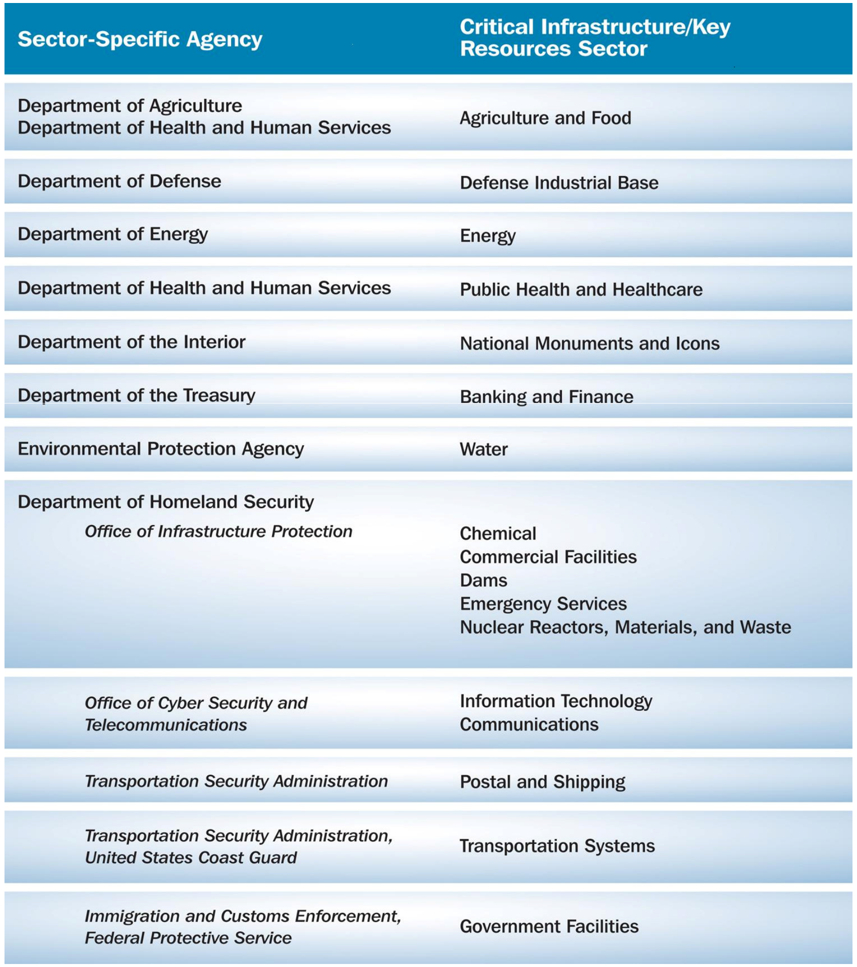
- National Incident Management System (3/04)
- National Response Plan (12/04)
- National Infrastructure Protection Plan (2006)
- National Preparedness Goal (2006)

Coordinated Approach to Homeland Security

Graphic credits: Presentation - R J Caverly, “Critical infrastructure protection overview” available at www.helsinki.fi/aleksanteri/civpro/events/cip_Caverly.ppt

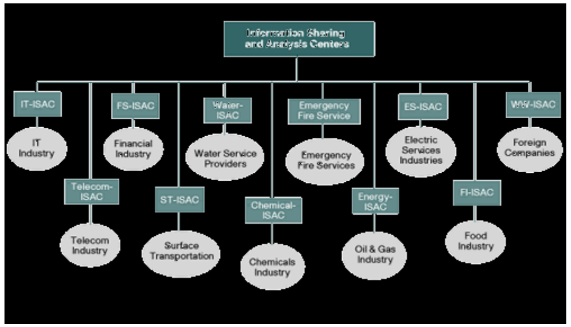
DHS

- Formed in 2002/03 combining 22 agencies
- CIP Role: Manage the broad CI protection framework and oversee the development and implementation of the National Infrastructure Protection Plan (NIPP)
- Establish and maintain multi-tiered, dynamic information-sharing network (See National Strategy for Information Sharing 2007)
- Promote public/private partnership



Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard	Transportation Systems
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

ISACs



Information Sharing and Analysis Centers

IT-ISAC
IT Industry

Telecom-ISAC
Telecom Industry

FS-ISAC
Financial Industry

ST-ISAC
Surface Transportation

Water-ISAC
Water Service Providers

Chemical-ISAC
Chemicals Industry

Emergency Fire Service
Emergency Fire Services

Energy-ISAC
Oil & Gas Industry

ES-ISAC
Electric Services Industries

FI-ISAC
Food Industry

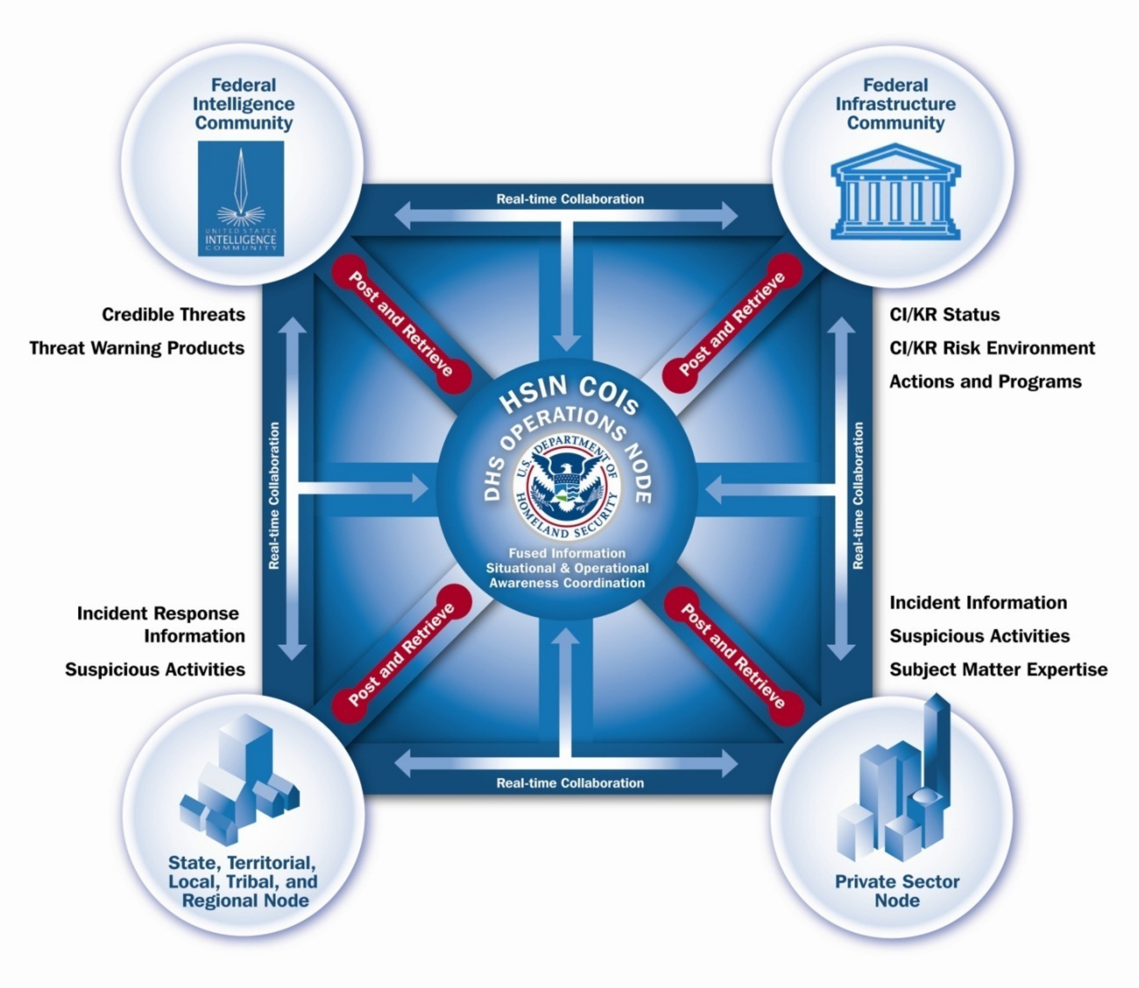
WW-ISAC
Foreign Companies

- Information Sharing and Analysis Centers (ISACs):
  - – Sector-based membership organizations managed by the private sector
  - – Established pursuant to Presidential Decision Directive-63 (1998)
  - – share and analyse security incident and response information among ISAC members and with other ISACs
  - – facilitate information exchange between the government and the private sector

CIP/information sharing regulation

- Homeland Security Act (2002) explicitly protects voluntarily shared critical infrastructure information
  - FOI exemption
  - Prevents government and 3rd party use of info in civil actions against the information provider
- Chemical Sector Regulation - *Homeland Security Appropriations Act* (2007) Section 550 establishes federal security standards for high risk chemical facilities (includes information security management standards)
- Energy Sector - enforced self regulation - *Energy Policy Act* (2005) authorised Federal Energy Regulatory Commission (FERC) to approve industry developed standards (includes information security management standards)

ICT support for info sharing



Graphic credits: Presentation - R J Caverly, “Critical infrastructure protection overview” available at www.helsinki.fi/aleksanteri/civpro/events/cip_Caverly.ppt

CIP in Israel

Highlights

- Radically different approach to regulation!
- National security perspective dominates despite privatisation of critical infrastructure
- Direct mandatory operational government control and oversight of critical infrastructure operators

GSS-NISA controls CIIP

- 2002 Government resolution assigned responsibility for Critical Information Infrastructure Protection (CIIP) to the General Security Service (GSS) - Israel’s internal security organisation
- National Information Security Authority (NISA) within GSS has the power to determine that a company or sector (public or private) is critical and subject to NISA’s executive authority

NISA’s Powers

- Appoint an officer responsible for securing the information systems of an organisation/sector
- Instruct the officer regarding required actions to secure the infrastructure
- Inspect and audit infrastructure within a regulated entity - any time - any system
- Regulated entities must comply - very limited discretion - includes private sector entities

Case Study Summary

- Australian approach to CIP information sharing based on voluntary public/private partnership
  - Starting in 2003, Australia has implemented a Trusted Information Sharing Network (TISN) to support critical infrastructure protection
  - Business continuity focus - all hazards approach
  - Australia has not enacted any new laws to protect shared information or limit member's liability through participation
- US information sharing approach is similar but more mature
  - Also based on public/private partnership model established in 1998
  - Some regulation but a preference for voluntary self regulation
  - Counterterrorism view still dominates
  - Extensive use of ICT through HSIN
- Israel is an example of an alternate, centralised regulatory approach
  - Privatised infrastructure however,
  - Information sharing mandated by law
  - Direct control and reporting through National Internal Security Agency

International Security Issues

- Different laws including FOI and privacy
- Digital divide within/between countries
- How to prosecute criminals across international boundaries?
- How to govern and control a global structure such as the Internet in the absence of a global governance?
- The Internet is moving towards an unsustainable system due to failure of governance standards for
  - Accuracy of information
  - Integrity and accountability of reporting systems
  - controlling prevalence of spam

Research Challenges for E-Government

Legal & Policy Challenges

- Cyber vs. physical criminal behaviour
- Balance between national, commercial and individual interests
- Mechanisms for organisations to identify and/or develop appropriate information security standards and policies and to ensure they are implemented
- Legal status of electronic evidence

Establishing and maintaining Confidence in ICT

- User friendly security mechanisms
- Protection of digital identity
- Methods for users to trust computing devices

Security and Privacy in Mobile Networks

- Lightweight cryptographic protocols for highly resource-constrained devices
- Trusted computing for embedded systems
- Distributed filtering and intrusion detection for ad-hoc and wireless networks
- Usability of pervasive security and privacy mechanisms

Enhanced Security Mechanisms

- Security tools to detect, respond and recover from security attacks
- Tools to better understand emergent behaviour in complex software systems
- Continued development of risk assessment and management practice, theory and tools
- Simulation and modeling of information infrastructure especially for information security issues

Identifying and Removing Impediments to Deployment of Secure Technologies

- Closer collaboration with business
- Design of appropriate government regulations
- International collaboration

Questions?