PKI International Scan

———

January 31, 2004

PKI International Scan

International PKI Scan

Introduction

This report represents ongoing research conducted by the Government of Canada (GoC) PKI Secretariat to keep abreast of developments in secure electronic transactions and service delivery. The primary focus is on how federal governments are addressing the requirement to ensure a trusted environment to enable electronic delivery of services to the public. The document is compiled using information gathered from web sites, news reports, presentations from visiting delegations, and ongoing information exchanges with internal and external parties. Since most of the research has been compiled through secondary sources, the information in this document reflects how the profiled organizations present their situation, rather than a detailed and vetted analysis of actual progress. Also, due to the rapid pace of change in this area, new developments are happening all the time. The report should not be considered a final report, but rather an evolving source of compiled information for reference purposes.

Global/Multi-nation Activities

IDA and the EU's e-government Policy[1]

The European Union's (EU) e-government policy is part of the eEurope framework designed to harness the power of information and communication technologies (ICT) and provide a favourable environment for private investment, job creation and productivity growth. The EU aims to stimulate services, applications and content, covering both the modernisation of public services (e-government, e-learning, e-health) and the creation of a dynamic environment for enterprises (e-business). It also seeks to advance the underlying infrastructure towards broadband (wired and wireless) and addresses security matters. To deliver on these objectives, and in addition to Member States' initiatives, the EU uses a number of instruments and programmes such as; Information Society Technologies-IST, e-Trans European Networks-eTEN, Interchange of Data between Administrations-IDA, eContent.

Getting Europe Networked[2]

The European Commission has set out its latest proposals to improve the electronic delivery of information and services to citizens across the continent. The proposals set out seventeen recommendations for a pan-European interoperability framework to support the European Union's strategy of providing user centred e-services. The recommendations include: common definitions and identifiers to allow data to be shared are needed; the development of pan European services according to user demand should be among the governments' priorities; a "common security policy" should be agreed upon.

---

[1] http://europa.eu.int/ISPO/ida/jsps/dsp_showDocument.jsp?printerVersion=1&documentID=1920
[2] http://www.kablenet.com/kd.nsf/printview/1CD9C8CC79A891D580256E24004F994C?OpenDocument

EU – Data Protection Supervisor[3]

The European Parliament and the Council of the European Union have issued a decision appointing the EU's Data Protection Supervisor and Assistant Supervisor. They are Peter Hustinx, formerly the President of the Dutch Data Protection Authority and Joaquin Bayo Delgado, respectively.

Africa (Continent of)

Egypt – Gateway Unveiled[4]

Atif Ubayd, Prime Minister of Egypt, coincided the launch of Egypt's e-government portal with Microsoft chairman, Bill Gates', visit to the country. The Egyptian government is aiming to put services online by 2007 and Microsoft is one of its strategic partners in this initiative. Egypt's Gateway, influenced by the UK's Government Gateway, provides registration and authentication for e-government services offering users access with passwords. The Egyptian government also intends to provide access with digital certificates. Registration of vehicles, payment of parking fines, tax and customs are among the first services being offered.

Argentina

No new item to report.

Australia

Defence Smart Card Pilot Goes Solo[5]

Plans for the Australian Defence Force to conduct a smart card pilot in Canberra will take place towards the end of 2004 and run for about one year. Originally part of the $34M e-Defence project, the pilot of 5,000 smart cards is proceeding despite the fact that the rest of the e-Defence project is being re-examined. Other elements of the e-Defence project would include the deployment of a secure PKI gateway product to enable military messaging interoperability with allied forces. It would replace the existing Defence Integrated Secure Communication Network.

Digital Wills Concept Tested in Australia[6]

Australian technology lawyer, Jeremy Malcolm, is putting the validity of digital wills in Australia to the test. In doing so, he has placed his will, featuring encrypted digital signatures from himself and two witnesses, on a DUGI watch that includes a 128MB USB memory key. The will's validity relies on section 34 of the *Western Australian Wills Act*, which suggests that a will is valid, even if not executed properly, if it can be proven that it was intended as a will.

---

[3] Baker & McKenzie E-law Alert, 2004-01-25; http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_012/l_01220040117en00470047.pdf

[4] http://www.kablenet.com/kd.nsf/Frontpage/1F57F8F94BE7911880256E2700481450?OpenDocument; CIOB News 2004-01-26

[5] http://australianit.news.com.au/articles/0,7204,8500695%5E15321%5E%5Enbv%5E15306,00.html; CIOB News 2004-01-27

[6] http://www.zdnet.com.au/news/hardware/0,2000061702,39115755,00.htm

Belgium

No new item to report.

Bermuda

No new item to report.

Bosnia-Herzegovina

No new item to report.

Brazil

No new item to report.

Bulgaria

E-Government at Bulgarians' Disposal from 2005[7]

The first online administrative services were officially launched September 2003 as the first step for Bulgaria towards fulfilling its national strategy for building efficient e-government system. For 2004, the priority tasks are completing the administrative reforms and launching the e-government into operation, in compliance with EU standards. Thus, by the end of 2005, a total of 20 online administrative services including firms and vehicles registration will be available.

Canada

Feds Lay Groundwork for Inter-department e-Marketplace[8]

The first electronic supply chain that works across departments within the Government of Canada has been launched. Using this service, the government expects to save 10 per cent on the cost of goods and services and 50 per cent on administrative process costs associated with purchasing. Initially, the program will be piloted with Public Works and Government Services Canada, the RCMP, Transport Canada and the Transportation Safety Board of Canada. Initially, it will involve 1,300 users and could reach up 10,000 if expanded to other government departments.

---

[7] CIOB News 2004-01-22 http://www.novinite.com/newsletter/print.php?id=30153

[8] http://www.itbusiness.ca/print.asp?sid=54595

Contentious Laws Will Mould Technology[9]

2004 promises to be the most exciting yet in technology law. Three issues lead the concerns: privacy, internet marketing, and copyright. While businesses and consumers adjust to life with privacy legislation, several provinces may also become more active in the privacy arena by enacting their own provincial privacy laws. For internet marketing, following the United States', European, and Australian initiatives, the federal government shifted away from its previous position that opposed anti-spam legislation last year by initiating a consultation on the possibility of a Canadian anti-spam statute. Fall 2004 will be the expected date to see how the federal government will deal with the copyright issue.

Canada Health Infoway CEO [10]

Canada Health Infoway, mandated to transform Canada's health-care system through the development of pan-Canadian electronic health records (EHR), predicts that 2004 will be a breakthrough year in its revolutionary initiative. Infoway recently received unanimous endorsement of its business plan by its board of directors and its members; federal, provincial and territorial deputy ministers of health from across the country. This represents an inter-jurisdictional accord rarely witnessed in Canadian health care management.

Voice ID Sets The Tone For Security[11]

Voice authentication has been used for a few specialized purposes for several years but is now moving into more widespread commercial use. Starting in April in Ontario and in September in Quebec, Bell will enrol service technicians in its voice authentication system. This year in Canada, several implementations are expected, including at least one by a major bank. To reinforce the process, the system might combine voice authentication with knowledge by asking a question to which only the caller should know the answer.

Canada Plans Smart Card ID For Airport Workers[12]

The Canadian Air Transport Authority has launched the Restricted Area Identification Card (RAIC) program. It will provide a smart card ID for some 130,000 workers at 29 major airports. The chip card will carry two kinds of biometric data, fingerprint and iris, to identify the workers as they access restricted areas.

Consumer Ministers Advance Initiatives to Protect Consumers in a Marketplace Without Borders[13]

In response to consumer protection issues associated with a rapidly changing and increasingly open marketplace, the Federal, Provincial and Territorial consumer ministers endorsed the *Canadian Code of Practice for Consumer Protection in Electronic Commerce*. The code, developed cooperatively with business, consumer groups and governments, sets out good business practices for merchants conducting online commercial activities. The next step is to develop implementation mechanisms that will

---

[9] CIOB News – 2004-01-05
http://www.torontostar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call_pageid=971358637177&c=Article&cid=1073258103829
[10] CIOB News – 2004-01-06 http://www.newswire.ca/en/releases/archive/January2004/06/c7804.html
[11] CIOB News – 2004-01-08
http://www.globeandmail.com/servlet/ArticleNews/TPStory/LAC/20040108/TWVOIC08//?query=Voice+ID
[12] CIOB News 2004-01-13; http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040109CTDN019.xml
[13] CIOB News 2004-01-21;
http://www.ic.gc.ca/cmb/welcomeic.nsf/261ce500dfcd7259852564820068dc6d/85256a5d006b972085256e1d00739b27!OpenDocument

both engage merchants to use it and enable consumers to recognize merchants who respect its provisions. The new challenge facing the officials who have been asked to consult with the credit card industry is to determine the most effective way to achieve these objectives and to report back to the consumer ministers in six months regarding progress.

The *Code of Practice* is available at: http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/EcommPrinciples2003_e.pdf/$FILE/EcommPrinciples2003_e.pdf

Data Protection – Helping Organisations Get it Right[14]

Canada's Information Commissioner announced a package of measures in response to calls for greater guidance on interpreting the *Data Protection Act 1998* (DPA). The ICO already works closely with a range of businesses and representative bodies to develop appropriate guidance where required however, guidance for every eventuality is not expected. Therefore organisations will still be expected to seek their own legal advice, check existing ICO guidance and make their own decisions.

Federal Privacy Law Takes Full Effect[15]

 The third and final phase of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) took effect January 1, 2004. The legislation, which previously applied to federally regulated entities and interprovincial data transfers, now extends to all private sector businesses and organizations in Canada except within provinces that have adopted substantially similar legislation. To date, Quebec, Alberta and British Columbia have adopted privacy legislation, but only Quebec's has been found substantially similar.

Alberta – Personal Information Further Protected Under New Law[16]

In Alberta, the *Personal Information Protection Act* – PIPA takes the place of the federal *Personal Information Protection and Electronic Documents Act*. Consultation on PIPA began in November 2002 and passed on December 4, 2003. Therefore, as of January 1, 2004, businesses need to ask Albertans for consent when collecting their personal information and limit the information they collect to only what is needed for specific transactions with customers and employees. The legislation will not affect non-profit or charitable organizations unless they are carrying on commercial activities, such as the sale of donor, membership or other lists.

Manitoba – Cost Kills Manitoba Biometric Licence Plan[17]

The NDP government asked businesses last September to provide information on using technology to enhance its drivers licence system, with biometrics specifically mentioned as an area to explore. The idea is off the table and a decision has been made to weigh how effective it is in light of other security features that might not be as costly. Civil liberties organizations are glad, but remain worried it may be revived if the technology becomes less expensive.

Ontario – Security of Health Data Prompts Legislation

Ontario's *Health Information Protection Act* (Bill 31) is the province's response to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Bill 31

---

[14] CIOB News 2004-01-15
[15] Baker & McKenzie E-Law Alert 2004-01-12
[16] http://www.gov.ab.ca/home/index.cfm?page=675
[17] CIOB News 2004-01-13;   http://intranet/tbnews/stories/2004/20040113c0510.htm

requires all companies and organizations that deal with personal health information to ensure they obtain consent from all patients to use their information in non-medical cases, such as marketing. The bill also requires companies to verify the software protects the security of all files. Under Bill 31, health information custodians (including health care practitioners, pharmacies, ambulance services) would have to notify patients if their personal information is stolen, lost or accessed by unauthorized persons.

The draft bill is available at:
http://www.ontla.on.ca/documents/Bills/38_Parliament/Session1/index.htm#P190_15320

Quebec – Challenge to Federal Privacy Jurisdiction[18]

 The Quebec Court of Appeal granted the Quebec Government leave to challenge the constitutional jurisdiction of the federal government to implement PIPEDA. The federal law will not apply within Quebec, whose privacy legislation was found substantially similar to PIPEDA. However, a challenge could affect the implementation of PIPEDA in other Canadian provinces.

Quebec – Sur la voie de la continuité[19]

Le gouvernement du Québec a pour objectif d'être un exemple de gouvernement en ligne au Canada. Pour se faire, il compte entreprendre la migration d'une portion très significative des services et de l'information fournis aux citoyens et aux entreprises sur Internet. Le Gouvernement mise sur l'établissement de partenariats privé-public. Le défi serait de deux niveaux, le recherche d'une alternative à la carte à puce, impopulaire auprès des citoyens et la non option pour la création de maxi-fichier sur les citoyens par le secteur privé.

Quebec – Bientôt "entrepreneur.com" – guichet unique pour ceux qui veulent démarrer une entreprise [20]

Parmi les objectifs ciblés par la ré ingénierie du Gouvernement se trouve l'allégement réglementaire. Par conséquent, Québec se donne d'ici la fin de l'été pour lancer un guichet unique virtuel qui pourrait se nommer "entrepreneur.com" dont la mission serait de permettre la création d'entreprise par ordinateur. Les décideurs misent sur cette initiative pour doubler d'ici trois ans, le nombre de création d'entreprise qui se situe actuellement entre 1500 à 2000 entreprises annuellement.

Chile

No new item to report.

China

No new item to report.

---

[18] Baker & McKenzie E-Law Alert 2004-01-12
[19] http://www.directioninformatique.com/index.asp?theaction=61&lid=1&sid=51788

[20] CIOB News 2004-01-13; http://intranet/tbnews/stories/2004/20040113c0449.htm

Denmark

No new item to report.

Finland

E-Government in Finland: An Assessment[21]

The OECD has published an assessment of e-government policies, implementation and impact within Finland's central administration. The OECD's Policy Brief summarises the key finding of the OECD Report *E-Government in Finland*. It focuses on the drivers of e-government, the barriers impeding its development and implementation, and future directions for e-government in Finland. The Policy Brief is available at: http://www.oecd.org/dataoecd/20/50/13314420.pdf

France

No new item to report.

Germany

German Court Inaugurates Central e-payment Platform[22]

The German Federal Administrative Court became the first institution to adopt the central e-payment platform developed within the BundOnline 2005 framework. From now on citizens will have the possibility of purchasing copies of decisions of the Federal Administrative Court through an online shop, with payment being processed online via the e-payment platform. Purchased copies are delivered either by e-mail or regular mail.

Hungary

No new item to report.

India

World Bank to Discuss India E-Governance[23]

A World Bank team will discuss "e-governance" initiatives with Indian officials next week to develop more online services which would include such things as using Internet connections to apply for government documents like passports. With a population of

---

[21] http://www.oecd.org/dataoecd/20/50/13314420.pdf
[22] http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=1993&parent=chapter&preChapterID=0-140-194

[23] CIOB News 2004-01-15;
http://customwire.ap.org/dynamic/stories/A/AS_TEC_INDIA_WORLD_BANK?SITE=NYROM&SECTION=HOME&TEMPLATE=DEFAULT

more than 1 billion, India expects to have only 12 million computers by March 2004. There are only 4 million internet connections, 35,000 of them broadband.

Ireland

No new item to report.

Israel

No new item to report.

Italy

A Digital Revolution: the "IT Protocol" comes into force in Italy[24]

By 2006, all communications within and between Italian public administrations will be carried out exclusively electronically. This is the key point of the Italian directive on administrative transparency and management of document flows, known as the "IT Protocol" which came into force on 1st January 2004. From now on, according to the IT Protocol, management and storage of all government documents should be handled electronically. Forms submitted to government offices will also be transformed into digital documents.

Japan

No new item to report.

Kenya

No new item to report.

Korea

No new item to report.

Malaysia

E-filing of Tax Returns[25]

Malaysia's Inland Revenue Board (IRB) has announced that taxpayers will soon be able to file tax returns and have their documents stamped online using Mykad (the Malaysian Government's smartcard for citizens) to access the IRB website. Additional services such as e-stamping for legal documents such as the sale and purchase of properties are

---

[24] http://europa.eu.int/ISPO/ida/jsps/dsp_showDocument.jsp?printerVersion=1&documentID=1957
[25] http://www.thestar.com.my/news/story.asp?file=/2004/1/29/nation/7199016&sec=nation; CIOB News 2004-01-29

to be rolled out soon. Both the e-filing and e-stamping systems use PKI and were developed by the IRB with the collaboration of Mimos.

Mexico

Mexico Introduces E-Signatures For Tax Purposes[26]

The Mexican Senate has published a decree that amends several provisions of the Fiscal Code of the Federation and that allows for the use of advanced e-signatures and e-invoices by using the PKI of Mexico's Central Banking Authority. The Spanish language version of the Decree of January 5, 2004 is available at: http://dof.terra.com.mx/

Netherlands (the)

Dutch Government to Test Biometric Passports and ID Cards[27]

The Dutch government is about to launch pilot tests of high-tech passports and ID cards that will feature facial and fingerprint digital scans as biometric indicators. The pilots will test the adequacy of the prototype documents with the standard adopted in May 2003 by the International Civil Aviation Organization (ICAO) for using facial recognition technology to identify and screen people in airports. The new passport should be brought into use before the deadline of 26 October 2004 set by the US authorities for requesting nationals of countries taking part in their visa waiver (exemption) program to present machine-readable passports containing biometric information.

New Zealand

No new item to report.

Norway

No new item to report.

Pakistan

No new item to report.

Poland

No new item to report.

Russia

No new item to report.

---

[26] http://dof.terra.com.mx/

[27] http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=1977&parent=chapter&preChapterID=0-140-194

Singapore

No new item to report.

Slovak Republic

No new item to report.

Slovenia (Republic of)

No new item to report.

Spain

New Spanish Electronic Signatures Act[28]

An attempt to simplify and encourage the use of electronic signatures, the new Spanish Electronic Signature Act (Law 59/2003) will come into force on March 20 2004. The new Act adapts the current Spanish legislation and will replace the current Spanish Electronic Signature Act (Royal Decree-Law 14/1999). The most relevant developments are the regulation of the Spanish "national electronic identification document" and the possibility of electronic certificates for companies. This Act also modifies and adds some rules to the Spanish E-Commerce Act (Law 34/2002) and the Spanish Civil Procedure Act (Law 1/2000).

Sweden

No new item to report.

Switzerland

Electronic Signatures Gain Legal Status[29]

As the Swiss government is keen to see Switzerland among the top countries in the world in terms of daily use of the Internet and e-government services, Switzerland has recognised e-signatures. Under the law, the parties to an electronic contract would be clearly identified with a set of digital codes and would be cleared of responsibility for the misuse of their signatures, if they could show that they had taken adequate precautions to prevent this. However, certain official documents, such as wills or deeds of sale for buildings, will still have to be signed with pen and paper.

---

[28] Baker & McKenzie E-Law Alert, 2004-01-12
[29] CIOB News 2004-01-12 http://www.swissinfo.org/sen/swissinfo.html?siteSect=105&sid=4509386

Thailand

No new item to report.

United Kingdom

First UK Guide On E-Government Legal Issues Unveiled[30]

The UK Government's goal is to be fully online by 2005. As the workload for government offices continues to increase, e-government departments are tasked to maintain high standards of quality and responsiveness and consider the legal issues surrounding personal information, confidentiality and privacy. For this reason, 'E-Government: A Practical Guide to the Legal Issues' has been launched. Its purpose is to help Central Government and Local Authorities deliver on some of the promise of e-government by clarifying the laws and issues that need to be managed when implementing e-government.

Facing a Biometric Future[31]

British passports renewed as of 2007/8 will carry a photograph and microchip that holds biometric data. The photo and the chip will have the digital signature of the UK Passport Service (UKPS), in an attempt to protect against possible fraud. One other biometric identifier, iris pattern or fingerprints, will also eventually be stored on the chip and trials are underway in the UK to decide which one will be used.

Increased Use of Biometrics to Tackle Asylum Abuse [32]

As of March 2004, fingerprint data will be required from visitors to the UK from Djibouti, Eritrea, Ethiopea, Tanzania and Uganda and those travelling on refugee documents issued by other countries before entering the UK. Home Office Minister, Beverly Hughes, has said that the UK government is increasingly turning to biometric technology to help tackle the abuse of the UK's asylum and immigration system. This complements the UK's initiative to issue passports – capable of storing the holder's digital signature and key biometric data – to its own citizens.

Official Feasibility Study Backs UK Population Register Plan[33]

A feasibility study into developing a UK population register, dubbed "Citizen Information Project", was released on 6 January 2004. The UK-wide register, which could pave the way for the planned UK ID cards, would also be instrumental for the creation of more sophisticated, personalised e-government services. According to the study, building a UK population register should not be an impossible mission. However, as more research still needs to be done on this project, the Registrar General has announced that a dedicated

---

[30] http://www.managinginformation.com/news/content_show_full.php?id=2329

[31] CIOB News 2004-01-13 http://news.bbc.co.uk/1/hi/technology/3389209.stm
[32] http://www.homeoffice.gov.uk/n_story.asp?item_id=776

[33]
http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=1982&parent=chapter&preChapterID=0-140-194

team based within his office will carry out specific development work, mainly on data privacy issues. At the end of this period, the UK Government should be able to decide whether or not to create the register.

United States

Agencies on the Path to P3P[34]

One piece of the E-Government Act of 2002 aims to make Web site policies easier for users to understand. The next step is to develop privacy policies that can be understood by Web browsers. Section 208 of the E-Gov Act requires US Federal agency Web sites to include privacy policies in a machine-readable format that allows coding all the common elements of the privacy policies. This is intended to allow users to easily understand how their personal information is used, stored and shared.

Federal PKI Slow to Take Off, GAO says[35]

The General Accounting Office (GAO) was requested to provide a study on PKI implementation process. The conclusion was that progress in PKI has been slow over the last three years. The most commonly cited problems are funding and expense, the lack of government wide policy and guidance, the interoperability problems with existing systems, and the training and administration burdens. Most of the programs are in the planning, design or development phases; just 35 are operational; and six have been terminated. PKI implementation continues to face challenges: only twenty agencies have undertaken 89 PKI projects at a cost of about $1 billion.

The full GAO report is available at: http://www.gao.gov/new.items/d04157.pdf

Biometric Border Control System Launched in US Airports and Seaports[36]

The US-VISIT (United States Visitor and Immigrant Status Indicator Technology) programme officially kicked off on 5 January 2004 in 115 international airports and 14 major seaports across the country. By the end of 2004, a total of 179 land broder crossings will have a similar system. Foreigners entering the United States on visas must have their two index fingers scanned and digital photographs taken as they arrive to the US. Data collected is stored in a massive immigration tracking system for identification purposes and for matching against terrorist lists and criminal records. The programme has attracted some criticisms. Within the US, the criticisms are more likely related to the governance and lack of transparency in the way to conduct and publish a privacy impact assessment (PIA) for the technologies being used. The 28 European and Asian countries that participate in the visa waiver (exemption) programme have until October10th, 2004 to provide their citizens with a computer-readable passports containing biometric information. Several of the 28 concerned countries have said they would not be able to comply with the deadline.

---

[34] CIOB News 2004-01-22 http://www.fcw.com/fcw/articles/2004/0119/web-machine-01-21-04.asp
[35] CIOB News 2004-01-06 http://gcn.com/vol1_no1/daily-updates/24644-1.html
[36] http://europa.eu.int/ISPO/ida/jsps/dsp_showDocument.jsp?printerVersion=1&documentID=1958

Congress Questions US-VISIT[37]

Some Representatives of the US Congress have expressed skepticism with regards to the effectiveness of the US-VISIT system that is not checking visitors against all available watch lists, and lacks a process to track visitors' exits. Department of Homeland Security (DHS) contingency plans for the rollout of US-VISIT have not convinced Representatives that the system is on solid footing. DHS has countered that the contingency plans were available in case it had encountered difficulties during the roll-out. In effect, the roll-out was successful and did not require the use of those plans.

Passport Authorities Ask for the Finger[38]

As concerns have been raised over the security and accuracy of the biometrics, the US government is tight-lipped over how long the data will be retained. The US government has said that the data will be held and destroyed in accordance with applicable legal and regulatory requirements but have not specified which statutes will actually apply. While the government has acknowledged there will be a 0.1 per cent rate of false positives, it appears that other flaws in the technology could disrupt fingerprint and face scans.

Pentagon Stands by Internet Voting System[39]

The Pentagon is standing by an internet voting system it developed for US citizens overseas despite an independent analysis that said it was so vulnerable to attacks that it should be scrapped. Four computer security experts said the Secure Electronic Registration and Voting Experiment (SERVE), could be penetrated by hackers, criminals, terrorists or foreign governments. But, the Pentagon was confident that the system, which could get its first test February 3, 2004 in South Carolina's primary election, was secure. Another concern was that because of the automated nature of the system, it might be vulnerable to vote buying, selling or swapping in large numbers.

California's New Privacy Laws[40]

California recently passed two privacy laws that apply to online businesses. SB 27 requires companies to tell customers the kinds of information they collect and share with third parties about them, as well as the names of those third parties. The business must otherwise provide the customer a free opportunity to opt out. AB 68 dictates that online services that collect personal information on California residents must post a privacy policy and comply with it.

Grants.gov Takes Applications Online[41]

Using e-forms technology from Victoria, BC-based PureEdge, grant applicants can fill out forms and submit them through the Grants.gov website with authentication. Applicants can also digitally sign documents. Grants.gov is an integrated service of the US Federal government at which organizations can find, apply for and manage federal grants. It serves over 900 grant programs offered by 26 federal grant-making agencies awarding over $360B worth of grants. It is expected that 15,000 users will take advantage of the

---

[37] http://www.fcw.com/fcw/articles/2004/0126/web-usvisit-01-29-04.asp

[38] http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39117633,00.htm

[39] CIOB News 2004-01-22
http://customwire.ap.org/dynamic/stories/P/PENTAGON_INTERNET_VOTING?SITE=NYROM&SECTION=HOME&TEMPLATE=DEFAULT

[40] Baker & McKenzie E-Law Alert 2004-01-12

[41] http://www.transformmag.com/techselections/showArticle.jhtml?articleID=17501178; CIOB News 2004-01-27

portal during the first year of operation. Grants.gov is one of 24 federal cross-agency initiatives for improving access to services online.

NIST Recommendation for Electronic Authentication[42]

The National Institute of Standards and Technology (NIST) has published the draft *NIST Special Publication 800-63 Recommendation for Electronic Authentication.* The recommendation provides technical guidance for the implementation of electronic authentication to allow an individual to remotely authenticate his/her identity to a US Federal IT system. This publication supplements Office of Management and Budget guidance founds in *E-Authentication Guidance for Federal Agencies*.

The NIST's full report is available at: http://csrc.nist.gov/publications/drafts/draft-sp800-63.pdf

Data Storage Regulations[43]

Four key pieces of legislation pertain to the security and privacy of variety of information in the health care sector, financial institutions, accounting firms and other private sector enterprises. The *Health Insurance Portability and Accountability Act* (HIPAA) of 1996 stipulates requirements for data security for covered information as required or addressable. Required safeguards must be implemented. For addressable safeguards (such as the implementation of encryption and encryption specifications) a health insurance provider must document why the implementation is not appropriate to its circumstances and implement an equivalent measure. HIPAA's compliance deadline is April 2005, while small health plans have an extension until April 2006. The *Financial Services Modernization Act* or *Gramm-Leach-Bliley Act* (GLBA) of 1999 applies to financial institutions and stipulates the actions required for protecting the security and confidentiality of customers' non-public personal information. Its compliance date was July 1, 2002. The *Sarbanes-Oxley Act* of 2002 addresses aspects of security and controls of accounting and auditing processes for private companies. These include the development of policies and practices for the use of data integrity and confidentiality in handling complaints. The compliance deadline for most public companies is June 15, 2004, while smaller US business and foreign companies must comply by April 2005. Finally, California's *Security Breach Information Act* came into effect July 1, 2003. It requires business to inform customers when their electronic data is compromised.

Venezuela

No new item to report.

Viet Nam

No new item to report.

---

[42] CIOB News 2004-01-30
[43] http://searchstorage.techtarget.com/tip/0,289483,sid5_gci944159,00.html

Miscellaneous

Biometrics Enters Third Dimension[44]

DuPont Authentication Systems and A4Vision, a company that sells facial-imaging products, have developed a biometric security device that generates in-depth, three-dimensional facial portraits similar to holograms and secure enough to be embedded in documents. People can have their 3-D facial image embedded in a film and registered as digital data in a database in less than 10 seconds.

Biometric Technologies Come to e-Government[45]

Biometric technologies have made rapid progress in recent years, and the idea of using them for identifying individuals and enhancing security in society has gained momentum. However, four issues have emerged and must be understood and addressed to secure social acceptance. (1) In terms of accuracy and security, only iris scanning was found to be more reliable than both fingerprinting and face recognition. (2) Standardisation: the adoption of different biometric technologies may lead to confusion and make worldwide travel and trade considerably more difficult. (3) Finance: deploying biometric technologies on the scales currently envisaged would cost a lot of money. (4) Social acceptance: the use of biometrics data for daily-life applications and their protection are a novelty for Western societies, which is likely to face fierce resistance.

E-Privacy Year In Review[46]

The Electronic Privacy Information Centre (EPIC) published its 2003 Year in Review, noting the Can-Spam Act becoming law, schools installing biometrics technology to detect sex offenders, the Supreme Court allowing Internet filters in libraries, and the legal battle involving the Do-Not-Call registry. The 2003 Year in Review is available at: http://www.epic.org

What Keeps Information Security Professionals Up at Night?[47]

According to a recent study commissioned by Unisys, the biggest threats in information security systems and businesses are employee negligence or abuse of data warehouses or systems (97%), and insufficient resources to get the job done right (90%). The information security practices believed to be key for complex business organizations are as follows. (1) Integrate information security management. (2) Periodic and direct report to senior management. (3) Large enough budget to do the job well. (4) Decentralized IT infrastructure. (5) Introduce enabling technologies that help prevent common threats to data security and privacy. (6) Create the best possible training program. (7) Conduct vigorous internal monitoring of information security process and controls.

---

[44] http://www.wired.com/news/technology/0,1282,61969,00.html?tw=wn_tophead_5

[45] http://europa.eu.int/ISPO/ida/jsps/dsp_showDocument.jsp?printerVersion=1&documentID=1915
[46] Baker & McKenzie E-Law Alert 2004-01-12
[47] http://searchsecurity.techtarget.com/?track=NL-358&Offer=swp.

SSL To Be One of 2004's Bright Spots[48]

A key trend of 2004 seems so far to be the adoption of virtual private networks (VPNs) based on the browser-based secure sockets layer (SSL) technology. SSL allows for secure access to corporate networks from virtually any browser, providing flexible work options for roaming workers with laptops or smartphones. Along with the increased popularity of SSL, a key challenge is to strengthen the security features of SSL itself, especially with regards to authentication, which is still weaker than using internet protocol security (IPSec) VPNs. In this connection, Nokia has developed the Secure Access System, which exchanges digital certificates with the machine in use and performs client integrity scans to check for any weaknesses and adjust user privileges accordingly.

The primary source for the information contained in this document is the Internet – most articles are footnoted with links to source documents on various web sites. The reader is reminded that much of the information on Internet news sites is transitory and may only exist on a site for a short period of time. Readers wishing to maintain copies of the source information are encouraged to capture the text in a word processing application. Where possible, the date that an article appeared on a web site is provided following the link. Please do not report "broken links".

---

[48] http://www.theregister.co.uk/content/55/35075.html