

PKI International Scan

February 28, 2005

PKI International Scan

INTRODUCTION 6

GLOBAL/MULTI-NATION ACTIVITIES..... 6

 LEGAL ISSUES IN BIOMETRICS (*BIOMETRIC / PRIVACY*) 6

 EU CONSULTS ON BLUEPRINT FOR FUTURE INFRASTRUCTURE OF EUROPEAN E-GOVERNMENT (*E-GOVERNMENT*) 6

 E-GOVERNMENT AND COMPETITIVENESS: IDENTIFYING THE CONNECTION (*E-GOVERNMENT*) 6

 E-GOVERNMENT BRINGS REAL BENEFITS TO EU CITIZENS AND BUSINESSES, FINDS NEW SURVEY (*E-GOVERNMENT*) 7

 EU CONSULTS ON RFID TECHNOLOGY (*PRIVACY*)..... 7

AFRICA (CONTINENT OF) 7

SOUTH AFRICA 7

SOUTH AFRICA 7

ARGENTINA 7

AUSTRIA 8

 AUSTRIAN CITIZEN CARD NOW INTEGRATED IN BANK CARDS (*PKI / DIGITAL SIGNATURE / E-COMMERCE / E-SERVICES*) 8

AUSTRALIA 8

 FEDERAL E-GOVERNMENT FLOUNDERS (*E-GOVERNMENT*) 8

 FEDS LOOK AT E-PAYMENTS (*E-COMMERCE*) 8

BELGIUM..... 8

 MSN BELGIUM TO USE EID CARDS FOR ONLINE CHECKING (*AUTHENTICATION*)..... 8

BERMUDA 9

BOSNIA-HERZEGOVINA 9

BRAZIL 9

BRUNEI..... 9

 E-GOVERNMENT SETS ROAD TO DIVERSIFICATION SAYS CANADIAN PROFESSOR (*E-GOVERNMENT*) 9

BULGARIA 9

CANADA..... 9

 NET BANKING ENTERS 'MATURE' STAGE (*ONLINE TRANSACTIONS / E-COMMERCE*)..... 9

 GOVERNMENT OF CANADA ANNOUNCES CYBER SECURITY INITIATIVES (*E-GOVERNMENT*) 9

 SECURITY ON HER MIND: INTERVIEW WITH JULIE SPALLIN, MANAGER CCIRC (*E-GOVERNMENT / INTEROPERABILITY*) 10

 USERS BENEFIT FROM NEW ON-LINE PAYMENT SERVICE AT CITIZENSHIP AND IMMIGRATION CANADA (*E-GOVERNMENT, PKI, ONLINE TRANSACTIONS*) 10

 MINISTRY OF TRANSPORTATION CAUTIONS PUBLIC OF INTERNET E-MAIL FRAUD (*PIPEDA*) (I AM NOT SURE IF IS IT RELEVANT?)..... 10

 SO WHO'S STOLEN YOU? (*PIPEDA*)..... 10

 GOOD REASONS FOR CANADIANS TO NETFILE (*E-GOVERNMENT / ONLINE TRANSACTIONS*) 11

 BLACKBERRY MAKER GETS NIST NOD (*CRYPTOGRAPHY*)..... 11

 CANADA HELPS NORWAY FIND ITS ONLINE FEET (*E-GOVERNMENT*) 11

 REVISE PRIVACY LAW TO PROTECT PUBLIC, NOT OFFENDERS (*PIPEDA*) 11

 SECURITY LAPSES OPEN PUBLIC DATA TO HACKERS (*E-GOVERNMENT / AUTHENTICATION*)..... 12

 FEDS RESPOND TO AUDITOR GENERAL'S IT SECURITY CRITIQUE (*E-GOVERNMENT / AUTHENTICATION*)..... 12

 BELL CONSOLIDE SON OFFRE DE SERVICES EN SÉCURITÉ (*AUTHENTICATION / BIOMETRICS*) 12

 PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT CANADA EVIDENCE ACT (*DIGITAL SIGNATURE*)..... 12

 BRITISH COLUMBIA: CANADIANS FIGHT FOR PRIVACY (*PRIVACY / PIPEDA*) 13

BRITISH COLUMBIA: GOVERNMENT TO EASE ONLINE ACCESS: SINGLE WEB IDENTITY WILL OPEN DOORS TO ALL DEPARTMENTS (E-GOVERNMENT / AUTHENTICATION)	13
NEW BRUNSWICK: SERVICE NB SEEKS MERGER WITH FEDERAL COUNTERPART; FEDERAL SERVICES COULD BE PROVIDED IN TANDEM AT SERVICE NB OUTLETS (E-GOVERNMENT / E-SERVICES)	13
NEW BRUNSWICK: SNB WINS THREE NATIONAL AWARDS FOR E-GOVERNMENT SERVICE (E-GOVERNMENT)	13
NEW BRUNSWICK: NB POWER BILLS NOW AVAILABLE ONLINE THROUGH E-POST (E-COMMERCE / E-SERVICES)	14
NUNAVUT: SET TO GO HIGH-SPEED WITH LAUNCH OF BROADBAND INTERNET; FOR NUNAVUT IT'S A LONG-AWAITED LIFELINE TO BANKING AND OTHER SERVICES (E-SERVICES) ..	14
ONTARIO: SSHA RAMPS UP SECURITY FOR BACKUP STORAGE (PRIVACY / CRYPTOGRAPHY) ...	14
ONTARIO: MCGUINTY GOVERNMENT HELPS BUSINESS PREVENT IDENTITY THEFT (AUTHENTICATION / E-SERVICES).....	14
QUÉBEC: LA CAI S'INQUIÈTE DU DOSSIER MÉDICAL; VOS INFORMATIONS DE SANTÉ POURRAIENT CIRCULER DANS LE CYBERESPACE SANS VOTRE CONSENTEMENT (E-GOVERNMENT / PRIVACY)	15
QUÉBEC: FORTE HAUSSE DE L'UTILISATION D'INTERNET AU QUÉBEC (ONLINE TRANSACTIONS) ..	15
QUÉBEC: REVENU QUÉBEC ET LA RÉGIE DES RENTES DU QUÉBEC S'ASSOCIENT POUR RENDRE LEURS SERVICES ÉLECTRONIQUES PLUS ACCESSIBLES (E-GOVERNMENT / AUTHENTICATION / E-SERVICES)	15
QUÉBEC: CITY OF LAVAL ADDS 311 AS PART OF IT OVERHAUL (E-GOVERNMENT)	15
CHILE	16
CHINA	16
DENMARK	16
EDAY2 MARKS NEW E-GOVERNMENT MILESTONE IN DENMARK (E-GOVERNMENT / DIGITAL SIGNATURES / PKI / AUTHENTICATION).....	16
DUBAI	16
ESTONIA	16
FINLAND	16
FRANCE	16
FRANCE LAUNCHES NATIONAL E-ID CARD DEBATE (SMART CARDS / BIOMETRICS / PRIVACY).....	16
FRENCH GOVERNMENT TO LAUNCH BIOMETRIC VISA TRIAL (BIOMETRICS)	17
GERMANY	17
HONG KONG	17
MIGRATING CITIZENS TO E-GOVERNMENT CHANNELS IN HONG KONG (E-GOVERNMENT)	17
HONG KONG SETS OUT NEW ELECTRONIC SERVICE DELIVERY STRATEGY (E-GOVERNMENT) .	17
HUNGARY	18
INDIA	18
IRELAND	18
ISRAEL	18
ITALY	18
JAPAN	18
KENYA	18
KOREA	18
LITHUANIA	18
LUXEMBURG	18
MALAYSIA	18
MALTA	18
MEXICO	19
NETHERLANDS (THE)	19

NEW ZEALAND	19
BUILDING NEW ZEALAND'S E-GOVERNMENT ECOSYSTEM (<i>E-GOVERNMENT</i>)	19
NORWAY	19
PAKISTAN	19
POLAND	19
PORTUGAL	19
RUSSIA	19
SINGAPORE	20
SLOVAK REPUBLIC	20
SLOVAKIA STEPS UP E-GOVERNMENT EFFORTS (<i>E-GOVERNMENT</i>)	20
SLOVENIA (REPUBLIC OF)	20
SOUTH KOREA	20
SPAIN	20
SWEDEN	20
SWITZERLAND	20
TAIWAN	20
TANZANIA	21
THAILAND	21
TURKISH	21
UNITED KINGDOM	21
ACCREDITATION SCHEMES TO HELP REDUCE IT RISKS IN THE UK PUBLIC SECTOR (<i>INTEROPERABILITY / DIGITAL SIGNATURE</i>).....	21
ID CARD BILL 'IS A THREAT TO HUMAN RIGHTS' (<i>BIOMETRICS / SMART CARDS</i>).....	21
ID CARDS 'CONTRARY TO BRITISH VALUES' (<i>SMART CARDS / BIOMETRICS</i>).....	21
UK'S ID CARDS BILL WINS PARLIAMENTARY VOTE DESPITE HUMAN RIGHTS CONCERNS (<i>SMART CARDS / BIOMETRICS / PRIVACY</i>).....	22
FINGERPRINTS, IRIS RECOGNITION AND TAGGING 'TO CUT IMMIGRATION' (<i>BIOMETRICS</i>).....	22
DOTP - DELIVERING ON THE PROMISE (<i>E-GOVERNMENT</i>)	22
TOOLKIT FOR SMART CARDS RELEASED BY E-GOVERNMENT NATIONAL PROJECT (<i>SMART CARDS</i>)	22
UK.GOV LAUNCHES VIRUS ADVICE SITE (<i>E-SERVICES</i>).....	23
SCHEMES TO BOOST E-GOVERNMENT (<i>E-GOVERNMENT</i>).....	23
UNITED STATES	23
PERSONAL IDENTITY VERIFICATION STANDARD (<i>BIOMETRICS / SMART CARDS</i>).....	23
US TECHNOLOGY FIRMS ENDORSE HEALTH DATA PLAN (<i>E-GOVERNMENT / PRIVACY</i>)	23
ID THEFT SURGE HITS US CONSUMERS (<i>AUTHENTICATION</i>)	23
BUSH HIGHLIGHTS IT HEALTH ARCHITECTURE, US VISIT IN STATE OF UNION (<i>E-GOVERNMENT / SMART CARDS</i>).....	24
DOD CERTIFIES XML PRODUCT FOR PKI USE (<i>INTEROPERABILITY / PKI / CRYPTOGRAPHY</i>)	24
NIST URGES CAUTION FOR SWITCH TO VOICE OVER IP (<i>INTEROPERABILITY</i>)	24
OMB CONSIDERING CYBERSECURITY STANDARDIZATION (<i>E-GOVERNMENT</i>)	24
TECH EXECs ASK BUSH FOR CYBERSECURITY COMMISSION (<i>AUTHENTICATION / PKI</i>).....	25
PARENTS PROTEST STUDENT COMPUTER ID TAGS (<i>PRIVACY / CRYPTOGRAPHY</i>)	25
NASCIO LOOKS AT PRIVACY IMPLICATIONS OF SPAM, PHISHING AND SPYWARE (<i>PRIVACY</i>)	25
DEFENSE PICKS TWO FOR PKI (<i>PKI / SMART CARDS</i>).....	25
NEW BOOK MAKES CASE FOR DIGITAL REVOLUTION IN GOVERNMENT (<i>E-GOVERNMENT</i>)	25
THE FIGHT OVER CYBER OVERSIGHT (<i>E-GOVERNMENT</i>).....	26
COVIELLO: EMBRACE AUTHENTICATION (<i>AUTHENTICATION</i>).....	26
NIST SETS ID SCHEDULE (<i>PKI / AUTHENTICATION</i>)	26
FINGERPRINT STANDARD STILL ELUSIVE (<i>BIOMETRICS / INTEROPERABILITY</i>)	26
NO ENCRYPTION FOR E-PASSPORTS (<i>CRYPTOGRAPHY</i>)	27
DHS NAMES PRIVACY COMMITTEE (<i>PRIVACY</i>).....	27

GAO WANTS BETTER US-VISIT OVERSIGHT (*BIOMETRICS*)..... 27

SCREENING METRICS NEED WORK, GAO SAYS (*AUTHENTICATION*)..... 27

GSA WORKS ON ID GUIDE (*SMART CARDS / BIOMETRICS*)..... 28

MAKING IT HARDER TO GET A DRIVER'S LICENSE (*SMART CARDS / BIOMETRICS / AUTHENTICATION*)28

VENEZUELA..... **28**

VIET NAM..... **28**

MISCELLANEOUS **29**

GOVTS TO GET EARLY MS WARNINGS (*E-GOVERNMENT*) 29

OASIS CONSORTIUM MEMBERS APPROVE UDDI VERSION 3 AS AN OASIS STANDARD
(*INTEROPERABILITY*) 29

IDENTITY THEFT, LOSS OF PRIVACY FACE PEOPLE IN A WIRED WORLD (*PIPEDA*) 29

SHARED-SERVICES IN GOVERNMENT (*E-GOVERNMENT*) 29

MOVE OVER, PASSWORDS, AND MAKE ROOM FOR TOKENS (*AUTHENTICATION / PKI / SMART
CARDS*) 30

HOW TO STOP JUNK E-MAIL: CHARGE FOR THE STAMP (*DIGITAL SIGNATURES / CRYPTOGRAPHY*). 30

AUTHENTICATION AND DIGITAL SIGNATURES IN E-LAW AND SECURITY (A GUIDE FOR
LEGISLATORS AND MANAGERS) (*AUTHENTICATION / PKI / DIGITAL SIGNATURES*)..... 30

NEARLY HALF OF CONFIDENTIAL DATA STAYS ON THE PC WHEN THE PC LEAVES (*PRIVACY*)
..... 30

INFORMATION SECURITY FORUM ANNOUNCES NEW STANDARD OF GOOD PRACTICE 30

International PKI Scan

Introduction

This report represents ongoing research conducted by the Government of Canada (GoC) 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

Legal Issues In Biometrics ¹ (*Biometric / Privacy*)

One of the key drivers behind the push to take up biometric technologies is that governments are beginning to mandate that biometric identifiers such as facial images and fingerprints be used in official documents, including passports. In so doing, biometrics is seen as essential for the provision of e-Government services to citizens to ensure accurate authentication to prevent fraud. But legal challenges remain to the use of biometric technologies by both public institutions and businesses. In Europe, the most pressing legal challenges are in the area of conforming to privacy and data protection requirements. As part of its remit, the European BioSec consortium is working to develop a legal framework for the use of biometric technologies that ensures full compliance with European regulations in the area of data protection.

EU Consults On Blueprint For Future Infrastructure Of European e-Government ² (*e-Government*)

A blueprint for the future technical infrastructure of European e-Government has been published by the Interoperable Delivery of European e-Government Services to Public Administrations, Business and Citizens (IDABC) programme. The e-Government plan sets out several scenarios for the three dimensions of information exchange that are technical, semantic, and organizational.

e-Government And Competitiveness: Identifying The Connection ³ (*e-Government*)

A research report published by the e-Government Observatory outlines ways to leverage e-Government as a key factor to make European economies more competitive. It says that to boost competitiveness, governments need to become 'competitive' themselves, which means acquiring the capacity to steadily improve government quality, and to always strive to serve the public more efficiently and effectively. However, the correlation between the digitization of public services and a more competitive economy, leading to higher growth, better jobs and rising living standards,

¹ <http://www.it-director.com/article.php?articleid=12556&SESSID=e982f9505102f48b45281da14439e17b> CIOB News 2005-02-08

² <http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=2445> CIOB News 2005-02-15

³ <http://europa.eu.int/idabc/en/document/3863/194>

remains complex and elusive. To access the e-Government Observatory report, click on the following link: [The impact of e-government on competitiveness, growth and jobs](#)

e-Government Brings Real Benefits To EU Citizens And Businesses, Finds New Survey ⁴ (e-Government)

Published on January 14th, 2005, the 2004 edition of the 'Top of the Web' survey, which assesses progress made under the eEurope 2005 Action Plan, confirms that e-Government services yield real benefits for European Union (EU) citizens and businesses; namely in terms of saving time and gaining flexibility. The survey focused on six specific services: reporting personal income tax returns, reporting business VAT returns, registering a new business, submitting a proposal for a public tender, searching a public library catalogue, and enrolling in higher education. According to the survey results, 90% of users appreciate the quality of the available online services and over 60% are very satisfied with them.

EU Consults On RFID Technology ⁵ (Privacy)

The European Union (EU) is developing privacy guidelines for the use of Radio Frequency Identification (RFID) technology. But critics say the technology could threaten civil liberties, and the issue becomes even more acute with plans to put RFID tags into identity cards. The EU says that the privacy implications of RFID chips go beyond cases where unique serial numbers are linked to an identity. "Even if the individual is not immediately and directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him." Unwanted individual tracking, without a link to the identity of the data subject, also falls within the scope of the Data Protection Directive.

Africa (Continent of)

No new item to report.

South Africa

No new item to report.

South Africa

No new item to report.

Argentina

No new item to report.

⁴ http://europa.eu.int/idabc/isps/documents/dsp_showPrinterDocument.jsp?docID=3791&lg=en

⁵ http://www.theregister.co.uk/2005/02/23/eu_rfid_consultation/

Austria

Austrian Citizen Card Now Integrated In Bank Cards ⁶ (PKI / Digital Signature / e-Commerce / e-Services)

Starting January 31st, 2005, Maestro bank cards issued in Austria can contain a 'citizen card' function. An optional function, digital signature stored in the bankcard's microchip, allows users to use their Maestro card to identify themselves online. This new functionality, which is aimed at increasing the uptake of e-services provided by the Austrian public sector, could ultimately be extended to the 6.7 million bank cards currently in circulation in the country. According to Alfred Finz, undersecretary of state at the Ministry of Finance, Austria is the first country in the world to offer citizens the possibility to integrate an electronic signature in a bankcard.

Australia

Federal e-Government Flounders ⁷ (e-Government)

An audit conducted by The Australian National Audit Office (ANAO) found that Federal government agencies were unable to report any efficiency savings derived from their use of the Internet because they had not evaluated services. ANAO concluded that agencies' methods were inadequate to assess whether their internet-delivered services and programs were efficient and effective. The audit also found that agencies had paid widely varying amounts of money to set up websites, with no explanation for those varying costs. ANAO recommends agencies use cost-benefit analyses to support proposals for online services, evaluate websites, and integrate the measurement of website performance with the measurement of service delivery.

Feds Look At e-Payments ⁸ (e-Commerce)

The federal government is planning to fund research intending to explore the structure and operation of the electronic transactions marketplace and its role as a key component of the information economy. To this regard, the Department of Communications, Information Technology and the Arts (DCITA) said, "Australia was experiencing a major shift away from paper-based payment instruments to a more electronic environment. Yet associated issues such as security, privacy, identity and fraud-minimization still need to be addressed in order to promote and retain trust in these economic systems."

Belgium

MSN Belgium To Use eID Cards For Online Checking ⁹ (Authentication)

Belgian State Secretary for e-Government, Peter Vanvelthoven, and Microsoft's Bill Gates announced that Microsoft will integrate the Belgian eID Card with MSN Messenger. On this subject, Bill Gates said, "we're working to ensure that our technologies support eID, to help make online transactions and communications more secure." The card that contains an electronic chip will gradually replace the existing ID card, and by end-2005, over 3 million eID cards will be distributed in the country. Microsoft believes that combined with the eID Card MSN Messenger chat rooms will be much safer since users would have a trustworthy way of identifying themselves online.

⁶ <http://europa.eu.int/idabc/en/document/3857/194>

⁷ <http://australianit.news.com.au/articles/0,7204,12208977%5E15306%5E%5Enbv%5E.00.html>

⁸ <http://www.zdnet.com.au/news/business/0,39023166,39181954,00.html> CIOB News 2005-02-23

⁹ <http://www.securityfocus.com/news/10392> CIOB News 2005-02-02

Bermuda

No new item to report.

Bosnia-Herzegovina

No new item to report.

Brazil

No new item to report.

Brunei

E-Government Sets Road To Diversification Says Canadian Professor ¹⁰ (e-Government)

Brunei's initiative to develop its e-Government has attracted the attention of Professor Jim Tam from a leading Canadian University, who said he is confident the e-Government project will set the Sultanate on the road to economic diversification. Professor Tam of Ryerson University in Toronto who is also a former Information and Communication Technology (ICT) manager added, "achieving e-Government success requires active partnerships between government, citizens and enterprises. And to ensure its success, Brunei could benefit from the insights learned from e-Government implementation in other countries."

Bulgaria

No new item to report.

Canada

Net Banking Enters 'Mature' Stage ¹¹ (Online Transactions / e-Commerce)

Marketing research firm TSN Canadian Facts conducted their annual study, How Canadians Bank, in the fall of 2004. The study pointed out that the number of Canadians who do their banking on-line has reached a plateau. According to the study 30 per cent of Canadians reported using an on-line banking service in the month prior to the survey. This is the first time in eight years that the figure has not increased over the previous year's levels, and is similar to the results from the 2003 study. In addition, fewer non-users now say they have an interest in banking over the Internet. Only 6 per cent of those who have not yet signed up for Internet banking are likely to do so in the next six months. The study concluded that it may translate into continued stability in the future.

Government of Canada Announces Cyber Security Initiatives ¹² (e-Government)

Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness, Anne McLellan, announced two cyber security initiatives. First, the Government of Canada is the first signatory to an agreement to participate in Microsoft's Security Cooperation Program (SCP).

¹⁰ <http://www.brudirect.com/DailyInfo/News/Archive/Feb05/030205/nite07.html>

¹¹ <http://www.globetechnology.com/servlet/story/RTGAM.20050131.gtbank0131/BNStory/Technology/>

¹² <http://www.newswire.ca/en/releases/archive/February2005/02/c9595.html> CIOB News 2005-02-02

Second, the establishment of the Canadian Cyber Incident Response Centre (CCIRC), which will serve as Canada's focal point for dealing with cyber threats to Canada's critical infrastructure. "In a global environment where we are increasingly reliant on information technology, we have a responsibility to do everything we can to reduce the risk of cyber threats that could have an impact on our shared critical infrastructure," said Minister McLellan. The main objective of this public-private collaboration is to respond to computer security incidents proactively, and therefore to reduce the impact of cyber attacks.

Security On Her Mind: Interview With Julie Spallin, Manager CCIRC ¹³ (e-Government / Interoperability)

As manager of the recently launched Canadian Cyber Incident Response Centre (CCIRC), Julie Spallin and her team have been tasked with monitoring the cyber threat environment in Canada and coordinating appropriate responses. Two key CCIRC focus areas are: creating the right information exchange mechanisms, and fostering close, ongoing collaboration between the private and public sectors. Answering to why was CCIRC established? Spallin said "there are a number of things in the Government of Canada's National Security Policy (released in April 2004) that support what we are doing here. One is the priority of cyber security outlined in the National Policy and another is a more integrated approach to national security as a whole."

Users Benefit From New On-Line Payment Service at Citizenship and Immigration Canada ¹⁴ (e-Government / PKI / Online Transactions)

Citizenship and Immigration Canada (CIC) announced the launch of a service that allows clients to use the Internet to pay their fees for applications for citizenship or immigration services made through a case-processing centre in Canada. Rather than conducting transactions during banking hours, clients who choose this form of fee payment can access the Internet 24 hours a day, seven days a week, using their credit card as a means of payment. This is the fourth on-line service developed for the Department's clients in support of the Government of Canada's Government On-Line initiative. Since December 2000, CIC clients have been using the change-of-address feature to advise the Department when they move. And by April 2002, they have been able to view the status of their citizenship or immigration applications on-line; and application kits have also been available on-line for some time. More clients will be able to use the service when it is expanded to include clients in foreign countries.

Ministry of Transportation Cautions Public of Internet E-mail Fraud ¹⁵ (PIPEDA / e-Government)

The Ministry of Transportation has learned that a fraudulent e-mail was recently sent to members of the public. The e-mail stated that the ministry is updating its license database system and requested that the recipient confirm personal information such as name, address and driver's license number. The e-mail was disguised to look like an official communication from the ministry and it contained a link to a web page similar to the Ministry of Transportation's website.

So Who's Stolen You? ¹⁶ (PIPEDA)

McMaster University professor Milena Head is part of a team of researchers from four Canadian universities that are trying to create a library of information on identity theft that aims to make people more aware so they can protect themselves. McMaster is looking to take the lead on the

¹³ <http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-4076050f-2ade-4e50-9fc4-f6ee52c8e3fa&News=Daily%20ITwire> CIOB News 2005-02-04

¹⁴ http://publiservice.gc.ca/newsdesk/cnw/2005/2005020313_e.html CIOB News 2005-02-04

¹⁵ http://ogov.newswire.ca/ontario/GPOE/2005/02/04/c1030.html?!match=&lang=_e.html CIOB News 2005-02-05

¹⁶ CIOB News 2005-02-08

project that also involves Queen's, Carleton and Ottawa universities. Head said that in Canada the Royal Canadian Mounted Police (RCMP) has taken a lead in this fast-expanding crime, but the data is scattered, at best, and there's no centralized tracking system. "We don't even necessarily know in Canada to what scale the problem is," she said. Figures for 2003 released by Phonebusters, a national anti-fraud centre, suggest just over 13,000 Canadians were victims of identity theft that year, totaling nearly \$22 million. "I'm guessing that is grossly underestimated," Ms. Head added.

Good Reasons for Canadians to NETFILE ¹⁷ (e-Government / Online Transactions)

Last tax season, over 23,254,722 personal tax returns were filed with the Canada Revenue Agency (CRA). Of these, almost 50% or 11,056,214 were filed electronically. This represents an increase of over 11% in electronic filings over the previous year. Following this trend, by the year 2007, CRA projects 70% of tax returns will be filed electronically. Will 5 million more Canadians start filing electronically over the next 3 years? The chances are they will, and there are a number of good reasons why Canadians will be taking advantage of IT. In fact, filing electronically means that (1) the assessment process is fully automated, and tax software catches some errors instantly, (2) a faster refund, in less than 10 days, (3) when filing electronically, there is no need to sort, staple and mail all tax slips along with tax return, and (4) there is no need to mail anything.

BlackBerry Maker Gets NIST Nod ¹⁸ (Cryptography)

National Institute of Standards and Technology (NIST) officials issued the 500th certificate to Research in Motion, the Canadian maker of the wireless BlackBerry for its BlackBerry cryptographic kernel, firmware that performs all basic cryptographic functions. Federal agencies are required to use only validated cryptographic modules, and in this context, certification means that the module conforms to Federal Information Processing Standard 140-2. NIST officials operate the Cryptographic Module Validation Program in conjunction with the Canadian government, and have already accredited nine laboratories in the United States, Canada and the United Kingdom.

Canada Helps Norway Find Its Online Feet ¹⁹ (e-Government)

Norway's first minister in charge of public sector IT co-ordination was in Ottawa and New Brunswick, meeting with officials to learn how Canadian e-Government works. The delegation discussed cooperation between the different levels of government such as how to get common standards in the public sector and how to build common architecture that gives the opportunity to exchange information between departments at different levels. In the agenda were also questions concerning privacy and security, as well as how to get all departments involved in giving better IT service to the citizens.

Revise Privacy Law To Protect Public, Not Offenders ²⁰ (PIPEDA)

In the coming months, Industry Minister David Emerson will lead the federal government on a review of Canada's national privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Critics are likely to call for tougher enforcement measures, better reporting of decisions, and an end to the Federal Privacy Commissioner's policy that shields organizations that are the target of successful complaints. The law now on the books has

¹⁷ <http://www.newswire.ca/en/releases/archive/February2005/09/c1763.html> CIOB News 2005-02-09

¹⁸ <http://www.fcw.com/fcw/articles/2005/0207/web-nistberry-02-10-05.asp>

¹⁹ <http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=58097>

²⁰ http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call_pageid=971358637177&c=Article&cid=1108336208261 CIOB News 2005-02-14

supporters who said that it has achieved its goals by providing Canadians with a mechanism to resolve privacy disputes while encouraging businesses to adopt privacy-friendly practices.

Security Lapses Open Public Data To Hackers ²¹ (*e-Government / Authentication*)

In her report released on February 15th, 2005, the Auditor General Sheila Fraser said that most federal departments are failing to meet their own minimum standards for computer and network security, leaving Canadians' personal information vulnerable to hackers. Ms. Fraser said, "I am disappointed that the government still does not meet its own minimum standards for IT security, even though most of the standards have been well known for more than a decade." Vulnerability assessments conducted by external consultants and the Defence Department's Communications Security Establishment (CSE) also revealed weaknesses that had already been exploited, but gone undetected. In addition, the Canada Computer Emergency Response Team (CanCERT), a private tracking company, detected more than 400,000 attacks against government and commercial networks in 2004, compared with less than 50,000 two years earlier. More information are available at the link below: <http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20050201ce.html>

Feds Respond To Auditor General's IT Security Critique ²² (*e-Government / Authentication*)

Canadian federal departments say they are already taking steps to address the concerns raised in the Auditor General Sheila Fraser's report to improve IT security systems. The report released on February 15th, 2005 follows up on a review of the public sector's IT security policies and practices from 2002. Paul Rummell, a former CIO with the Treasury Board said the government will continue to be challenged by IT security until a central authority is established. "You need a single agency that's accountable for policy and operations," he said. "Right now it's divided across Treasury Board (TB), Royal Canadian Mounted Police (RCMP) and the Canadian Security Establishment (CSE)."

Bell consolide son offre de services en sécurité ²³ (*Authentication / Biometrics*)

Bell Canada consolide son offre de services en créant la filiale Bell Solutions de sécurité (BSS), spécialisée en sécurité des réseaux. BSS offrira aux administrations publiques et aux grandes entreprises privées du Canada des services de sécurité intégrés, regroupés en trois catégories, soit, (1) les services professionnels sous forme de services-conseils et intégration de solution, (2) les services de sécurité gérés 24/24, pour la protection des réseaux et le contrôle des identités et des accès, et (3) fourniture de produits matériels et logiciels de sécurité. La filiale dont le siège social se trouve à Ottawa compte recourir lors de la conception de ses solutions aux technologies prédictives, aux technologies d'identification biométrique et aux étiquettes intelligentes, communément connues sous le nom de Radio Frequency Identification (RFID).

Personal Information Protection and Electronic Documents Act Canada Evidence Act ²⁴ (*Digital Signature*)

The Governor in Council has approved the secure electronic signature regulations. The regulations are derived from the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Part II of PIPEDA provides a framework by which federal statutes and regulations may be adjusted to accommodate electronic alternatives to paper-based means of communication. It requires a secure electronic signature, that is defined as an electronic signature that results from the application of a technology or process. However, secure electronic signature is trustworthy only

²¹ CIOB News 2005-02-16

²² <http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=58160>

²³ <http://www.directioninformatique.com/index.asp?theaction=61&sid=52539>

²⁴ <http://canadagazette.gc.ca/partII/2005/20050223/html/sor30-e.html> CIOB News 2005-02-25

if the digital signature certificate is issued by a reliable certification Authority. The regulations establish the process by which this reliability is determined.

British Columbia: Canadians Fight For Privacy ²⁵ *(Privacy / PIPEDA)*

British Columbians are fighting to halt an outsourcing contract recently signed by their government that would place millions of their health records in the hands of a private American company. Activists with the British Columbia Civil Liberties Association are concerned that the data could be susceptible to seizure by American law enforcement agencies if the data resides with a US based firm. Marc Rotenberg, executive director of the Electronic Privacy Information Centre said, "the level of protection in the US is inadequate for non US persons. And it's understandable that foreign governments would be concerned on behalf of their own citizens about what might occur."

British Columbia: Government To Ease Online Access: Single Web Identity Will Open Doors To All Departments ²⁶ *(e-Government / Authentication)*

Management Services Minister Joyce Murray announced that a single password and one central electronic identity check will soon allow British Columbians to do Internet business with all government departments. The results will be the elimination of the need for a variety of passwords and IDs when people are dealing with government. In the meantime, government is smoothing the way for genuine users, and escalating its war against spam, viruses and worms. "e-Government is an important part of the vision of serving people better and more cost-effectively, but for it to succeed, security is absolutely vital," Murray said.

New Brunswick: Service NB Seeks Merger With Federal Counterpart; Federal Services Could Be Provided In Tandem At Service NB Outlets ²⁷ *(e-Government / e-Services)*

New Brunswickers could soon be renewing their passports and driver's licenses at the same place. Service New Brunswick (SNB) is pushing for a deal with the federal government to deliver federal services alongside provincial services through its one-stop shopping storefronts. Intergovernmental Affairs Minister Percy Mockler and SNB president Jacques Dubé will be in Ottawa today, Tuesday 15th, February 2005 for meetings with Public Works Minister Scott Brison and Human Resources Minister Lucienne Robillard to discuss the issue. On the other side, the federal government is looking to consolidate its services under Service Canada, an agency that has been two years in the making, and according to M. Dubé, "Service Canada could be launched in New Brunswick very quickly if they identify two or three things we could easily deliver, and SNB is looking to partner with it." When asked by reporters about federal government plans with Service Canada, Treasury Board President Reg Alcock said, "there has been no decision at this point. We will await the decisions that the Finance Minister puts forward in the budget and we will see where we end up."

New Brunswick: SNB Wins Three National Awards For e-Government Service ²⁸ *(e-Government)*

Service New Brunswick (SNB) has been honoured with three national awards, including two gold medals and one silver medal, for e-Government service at the first annual Chief Information Officer (CIO) Government Review (CGR) e-Government Awards of Excellence. These awards are a welcome continuation of the recognition that SNB has been receiving over the last few years," said Intergovernmental and International Relations Minister Percy Mockler, Minister responsible for

²⁵ http://www.wired.com/news/privacy/0,1848,66497,00.html?tw=wn_tophead_1 CIOB News 2005-02-04

²⁶ CIOB News 2005-02-11

²⁷ CIOB News 2005-02-15

²⁸ <http://www.gnb.ca/cnb/news/snb/2005e0187sn.htm> CIOB News 2005-02-17

Service New Brunswick. "Our one stop, multi-channel approach to government service delivery is known the world over as the model for e-Government."

New Brunswick: NB Power Bills Now Available Online Through e-Post ²⁹ *(e-Commerce / e-Services)*

New Brunswick Power announced that it has partnered with epost, the service that delivers bills, statements and other documents online for Canada Post, providing consumers with the tools they need to efficiently receive, view, pay, print and store their mail online. The service is accessible through convenient online locations including <http://www.epost.ca> and national financial institution online banking services. There are more than 100 Canadian organizations sending over 200 distinct documents through the epost service, representing over 70 per cent of monthly bills received in Canada.

Nunavut: Set To Go High-Speed With Launch of Broadband Internet; For Nunavut It's A Long-Awaited Lifeline To Banking and Other Services ³⁰ *(e-Services)*

Beginning February 2005, the region is set to launch broadband Internet access. In this respect, Lorraine Thomas, project manager of Nunavut Broadband Development Corp., a non-profit organization said "the smallest communities need it the very most, so we make sure every single community gets connected." Unlike high-speed access in the rest of the country that streams through fiber links, Nunavut is using a satellite-based delivery. It wasn't feasible to install cables due to the lack of roads and other infrastructure, Ms. Thomas said. Consequently, costs are slightly higher for the average user at \$60 per month.

Ontario: SSHA Ramps Up Security For Backup Storage ³¹ *(Privacy / Cryptography)*

The Ontario Government agency Smart Systems for Health Agency (SSHA), has selected the Assurance SecureData solution from Mississauga, Ontario based solutions provider Kasten Chase to guarantee the security of its backup tapes. Michael Milligan, president and CEO of Kasten Chase, said many organizations are becoming aware of the security risks associated with the backup procedure and are moving toward encrypting backup data. "The most pressing is the tape application. In most cases when tapes are moved out of the data centre, they are taken to offsite storage, so organizations want those tapes to be encrypted before they leave the data centre," Milligan said.

Ontario: McGuinty Government Helps Business Prevent Identity Theft ³² *(Authentication / e-Services)*

Consumer and Business Services Minister Jim Watson launched the identity theft kit and checklist for business. Federal, provincial and territorial consumer ministries jointly developed the kit and checklist in consultation with banks, business associations, privacy commissioners, credit-reporting agencies, credit card companies, law enforcement officials and consumer groups. Canadian credit-reporting agencies receive more than 1,800 identity theft complaints each month. According to a US report, as much as 70 per cent of all identity theft begins with theft of personal information from a company by an employee.

²⁹ <http://www.gnb.ca/cnb/news/nbp/2005e0227nb.html>

³⁰ CIOB News 2005-02-05

³¹ <http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idqml-e73de5fa-1318-46c2-877d-54273e378fd2&News=Daily%20Wire> CIOB News 2005-02-21

³² <http://ogov.newswire.ca/ontario/GPOE/2005/02/28/c8998.html?lmatch=&lang= e.html> CIOB News 2005-02-28

Québec: La CAI s'inquiète du dossier médical; vos informations de santé pourraient circuler dans le cyberspace sans votre consentement ³³ (*e-Government / Privacy*)

Québec veut rendre accessible le dossier médical des citoyens au personnel des hôpitaux, aux médecins des cabinets, aux organismes communautaires, aux résidences privées, à l'employé d'une entreprise d'économie sociale; ce qui n'est pas sans soulever les inquiétudes de la Commission d'Accès à l'Information (CAI). C'est ainsi que dans un mémoire soumis à l'Assemblée Nationale pour le débat sur le projet de loi 83 qui lance le gros de la réforme du réseau de la santé du ministre Philippe Couillard, le CAI écrit, "l'utilisateur ne pourra pas intervenir dans la circulation des renseignements de santé qui le concernent. Non seulement il perdra son droit de consentir à leur communication, mais il ne sera pas informé des échanges de renseignements qui se feront à son sujet". De plus, la CAI souligne qu'en l'absence d'encadrement, le critère de nécessité pourrait être interprété différemment d'un intervenant à l'autre; alors que le caractère sensible des renseignements de santé n'est plus à démontrer".

Québec: Forte hausse de l'utilisation d'Internet au Québec ³⁴ (*Online Transactions*)

Le Centre Francophone d'Informatisation des Organisations (CEFRIO), conjointement avec Léger Marketing a publié une vaste enquête sur Internet nommée «NETendances 2004», de laquelle il ressort que le Québec fait partie des plus grands utilisateurs d'Internet au monde. Selon l'étude, si le Québec était un pays, avec 60 % de ses citoyens qui naviguent quotidiennement, il se classerait 11e parmi les 189 pays étudiés par la firme Internet World Stats. À titre de comparaison, la proportion d'utilisateurs réguliers dans l'Union européenne est de 45 %, mais elle est de 68 % aux États-Unis et de 64 % dans le reste du Canada, avec les taux les plus élevés en Ontario, en Alberta et en Colombie-Britannique.

Québec: Revenu Québec et la Régie des Rentes du Québec s'associent pour rendre leurs services électroniques plus accessibles ³⁵ (*e-Government / Authentication / e-Services*)

Revenu Québec et la Régie des rentes du Québec s'associent pour mettre en place un nouveau service d'authentification qui permettra aux internautes d'avoir accès aux services électroniques des deux organismes de manière simple, unique et sécuritaire. Ce sont les services électroniques Clic Revenu de Revenu Québec destinés aux particuliers qui serviront de porte d'entrée. A Revenu Québec, le nouveau service d'authentification destiné aux particuliers leur permettra de consulter leur avis de cotisation en ligne. Alors qu'à la Régie des rentes du Québec, le service donnera principalement accès aux services "Demande de rente de retraite" et "SimulRetraite".

Québec: City of Laval Adds 311 As Part of IT Overhaul ³⁶ (*e-Government*)

The 311 system, is what the City of Laval, Quebec is giving to its residents to enable them to call a single number for any city service. The number is expected to be available for use during the first half of 2006. This initiative is part of the city's two-pronged approach to overhauling its IT infrastructure. The first stage is on the front end, a citizen interaction centre, due this spring. On the back end is an Enterprise Resource Planning (ERP) system to eliminate silos and consolidate data in various departmental systems.

³³ CIOB News 2005-02-09

³⁴ CIOB News 2005-02-02

³⁵ <http://communiqués.gouv.qc.ca/gouvqc/communiqués/GPQF/Fevrier2005/09/c2355.html> CIOB News 2005-02-10

³⁶ <http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=58104&adBanner=eGovernment> CIOB News 2005-02-15

Chile

No new item to report.

China

No new item to report.

Czech Republic

No new item to report.

Denmark

eDay2 Marks New e-Government Milestone in Denmark ³⁷ (*e-Government / Digital Signatures / PKI / Authentication*)

As of February 1st, 2005, or 'eDay2', all Danish citizens have a legal right to communicate electronically with central government bodies. The authenticity of all messages will be certified by the use of digital signatures. Public authorities have prepared for eDay2 by establishing secure e-mail solutions and by re-arranging their working practices in order to comply with guidelines from the Danish Data Protection Agency. The first eDay took place on September 1st, 2003, when Denmark became the first country in the world to introduce a general right for public authorities to communicate electronically between themselves with the exception of sensitive documents and personal data. This exception is cancelled by eDay2.

Dubai

No new item to report.

Estonia

No new item to report.

Finland

No new item to report.

France

France Launches National e-ID Card Debate ³⁸ (*Smart Cards / Biometrics / Privacy*)

³⁷ <http://europa.eu.int/idabc/en/document/3835/194>

³⁸ <http://europa.eu.int/idabc/en/document/3839/194>

In cooperation with the Internet Rights Forum, the French Ministry of the Interior launched an online debate over the proposed national electronic ID card. The online debate is intended to allow citizens to make their opinions heard on a number of key issues such as: (1) replacing the current national ID card with an e-ID card containing biometric identifiers stored in a microchip, (2) defining the measures required for privacy protection, (3) accessing e-government and e-commerce services via the e-ID card, (4) delivering the card, including logistics and cost aspects. In addition to the online consultation, a number of public debates will be organized in several cities. The Internet Rights Forum will then prepare a report for the Ministry of the Interior in mid-2005.

French Government To Launch Biometric Visa Trial ³⁹ (*Biometrics*)

The e-visa trial, foreseen by the new French law on immigration adopted in November 2003, was authorised by a decree published in November 2004. In seven French consulates abroad, visa applicants will have their 10 fingerprints scanned and their face digitally photographed. The biometric data will be stored both in the visa document containing a chip, and in a central database designed to track and identify illegal immigrants. The French e-visa pilot is based on an architecture similar to that of the proposed Europe-wide Visa Information System (VIS).

Germany

No new item to report.

Hong Kong

Migrating Citizens To e-Government Channels In Hong Kong ⁴⁰ (*e-Government*)

In order to improve service delivery and rationalize the management of the government's IT projects, the Hong Kong government established the Office of the Government Chief Information Officer (OGCIO). Headed by a Government Chief Information Officer, the OGCIO was formed by merging the functions of the former Information Technology Services Department and the IT-related divisions of the Communications and Technology Branch of the Commerce, Industry and Technology Bureau. "We are moving along similar lines as the United States, the United Kingdom, Canada and Australia, all of which have established a Chief Information Office (CIO) or its equivalent who reports to the highest level of government," explains Betty Fung, Deputy CIO at OGCIO.

Hong Kong Sets Out New Electronic Service Delivery Strategy ⁴¹ (*e-Government*)

A new strategy for the future delivery of e-Government services, based on a service clustering and customer segmentation approach, was endorsed by the Digital 21 Strategy Advisory Committee. Under this new strategy, the Hong Kong government will group the related e-Government services into a number of service clusters with regard to the specific needs of the individual customer segments. The technology architecture supporting the new business strategy will be based on open and interoperable standards those enable easy and secure interfacing within Government and with the private sector.

³⁹ http://europa.eu.int/idabc/jsp/documents/dsp_showPrinterDocument.jsp?docID=3794&lg=en

⁴⁰ <http://www.pstm.net/article/index.php?articleid=511>

⁴¹ <http://www.pstm.net/article/index.php?articleid=515> CIOB News 2005-02-15

Hungary

No new item to report.

India

No new item to report.

Ireland

No new item to report.

Israel

No new item to report.

Italy

No new item to report.

Japan

No new item to report.

Kenya

No new item to report.

Korea

No new item to report.

Lithuania

No new item to report.

Luxemburg

No new item to report.

Malaysia

No new item to report.

Malta

No new item to report.

Mexico

No new item to report.

Netherlands (the)

No new item to report.

New Zealand

Building New Zealand's e-Government Ecosystem ⁴² *(e-Government)*

New Zealand has ambitious plans to establish a rich e-Government ecosystem that syndicates content and services through the national government portal, individual agency sites as well as the private sector. The good news seems to be coming through thick and fast for New Zealand's e-government planners. In November 2004, the United Nations praised New Zealand's e-government as an example of 'global best practice'! According to the UN's Global E-govt Readiness Report: "New Zealand has taken extra efforts to actively encourage and promote [e-government's] use to citizens, and does so ... across all ministries and sub-sites. This kind of integrated implementation and promotion puts [New Zealand] in an altogether different league, one shared by only a few other e-government innovators and leaders."

Norway

No new item to report.

Pakistan

No new item to report.

Poland

No new item to report.

Portugal

No new item to report.

Russia

No new item to report.

⁴² <http://www.pstm.net/article/index.php?articleid=522>

Singapore

No new item to report.

Slovak Republic

Slovakia Steps Up e-Government Efforts ⁴³ *(e-Government)*

A number of new e-Government services have been launched in Slovakia since early 2005. These new services and projects show a willingness of the Slovak authorities to accelerate the delivery of their e-government initiatives. However, e-government progress in Slovakia remains slowed down by the relatively low level of Internet penetration in the country, particularly in terms of broadband access. Increasing ICT deployment in Slovakia is one of the main priorities of the country's competitiveness strategy to 2010. Based on the strategy, an implementation project called 'Minerva' has been launched, and the action plan is due to be released in April 2005.

Slovenia (Republic of)

No new item to report.

South Korea

No new item to report.

Spain

No new item to report.

Sweden

No new item to report.

Switzerland

No new item to report.

Taiwan

No new item to report.

⁴³ http://europa.eu.int/idabc/jsp/documents/dsp_showPrinterDocument.jsp?docID=3852&lg=en

Tanzania

No new item to report.

Thailand

No new item to report.

Turkish

No new item to report.

United Kingdom

Accreditation Schemes To Help Reduce IT Risks In The UK Public Sector ⁴⁴ *(Interoperability / Digital Signature)*

On January 24th, 2005 the 'UK e-GIF Accreditation Authority' published the first list of 'e-GIF Accredited Organizations' a development that reflects the commitment of both the public and private sectors to the full implementation of the e-Government Interoperability Framework (e-GIF). The e-GIF sets out the technical policies and standards designed to ensure interoperability of systems used to deliver e-Government services. Complying with the e-GIF is mandated widely across the United Kingdom (UK) public sector because it helps build more sustainable and flexible IT systems, making for efficiency and effectiveness gains in the immediate and longer terms as systems are upgraded or replaced.

ID Card Bill 'Is A Threat To Human Rights' ⁴⁵ *(Biometrics / Smart Cards)*

The Joint Committee on Human Rights (JCHR) has published its report into the implications of the Identity Cards Bill, and said the legislation "raise[s] a number of serious questions" on human rights. The report considers how the Bill potentially infringes the European Convention on Human Rights, and queries the possibility for information on United Kingdom (UK) citizens to be held without their knowledge or consent. The Committee also believes that ID cards could become "effectively compulsory" for certain groups of people and the cards' introduction could see some government and private sector organizations withholding services unless ID cards are produced.

ID Cards 'Contrary To British Values' ⁴⁶ *(Smart Cards / Biometrics)*

Peter Lilley, Member of Parliament (MP), and former Secretary of State for Trade And Industry, was highly critical of Labour's plans to introduce identity cards, branding them unworkable, expensive and potentially dangerous. "The public sector's record in successful implementation is woeful, and this would be the biggest yet. It's not just the IT system that will be liable to failure: the biometric systems on which they intend to rely simply have not been tried on any scale. A Cabinet Office study said that biometric tests would wrongly conclude that between 10 and 15 per cent of those tested were not who they actually were." wrote Lilly. He also pointed out that no country based on common law has successfully introduced ID cards in peacetime.

⁴⁴ http://europa.eu.int/idabc/isps/documents/dsp_showPrinterDocument.jsp?docID=3838&lg=en

⁴⁵ <http://management.silicon.com/government/0.39024677.39127564.00.html>

⁴⁶ <http://www.vnunet.com/news/1161025> CIOB News 2005-0204

UK's ID Cards Bill Wins Parliamentary Vote Despite Human Rights Concerns ⁴⁷ (*Smart Cards / Biometrics / Privacy*)

On February 10th, 2005 the United Kingdom (UK) ID Cards Bill passed in the House of Commons, a week after a report published by the Parliament's Joint Committee on Human Rights questioned its compatibility with Human Rights. The government's determination to push the e-ID cards forward was confirmed by the Prime Minister Official Spokesman (PMOS) on February 2nd, 2005. Asked if it wasn't time to put plans for ID cards on hold given the concerns voiced by the Joint Committee on Human Rights, the PMOS said that the case for ID cards remained the same, that biometric ID cards and passports would help in the fight against terrorism and were therefore "the right thing to do."

Fingerprints, Iris Recognition and Tagging 'To Cut Immigration' ⁴⁸ (*Biometrics*)

Kingdom (UK) Home Secretary Charles Clarke announced that by 2008, all visa applicants will be fingerprinted once they arrive at UK ports of entry. In addition to the biometric rollout, the UK government will be putting in place the e-Borders system that captures, reviews and stores data about immigrants on travel routes, as well as collecting arrival and departure information. The procedure means that carriers will be obliged to submit information about their passengers to the UK authorities before the travellers' arrival. The e-Borders scheme, which begun its trial in December, 2004 on a selected few routes, will run for 39 months and will be replaced with a full implementation at the end of the trial.

DotP - Delivering On the Promise ⁴⁹ (*e-Government*)

The e-Government Unit is building a central infrastructure, known as Delivering on the Promise (DotP), designed to host multiple government websites. This Government Gateway will lead the delivery of a central common infrastructure providing economies of scale benefits to government departments through a modular 'build-once, use-many' architecture. Endorsing this approach, departments are required to prove that equivalent market solutions are better value than the DotP and Gateway offering, before funds will be released. The DotP platform deliver's benefit is decrease time to market economies of scale in compliance with government standards.

Toolkit For Smart Cards Released By e-Government National Project ⁵⁰ (*Smart Cards*)

The National Smartcard launched a smart toolkit offering local authorities the help needed to set up a multi-application smart card scheme. Produced by Bolton Metropolitan Borough Council, the toolkit provides a step-by-step guide for setting up a smart card scheme to enable councils to improve access to services for citizens. Richard Tyndall, National Smartcard project manager, said, "with all local authorities being required to meet priority outcome G12 to implement smart card schemes for access to leisure and libraries by 2006 the project's toolkit provides a useful guide to the process."

⁴⁷ http://europa.eu.int/idabc/jsp/documents/dsp_showPrinterDocument.jsp?docID=3861&lg=en

⁴⁸ <http://software.silicon.com/security/0,39024655,39127657,00.html> CIOB News 2005-02-09

⁴⁹ http://e-government.cabinetoffice.gov.uk/Responsibilities/ElectronicDelivery/EDTArticle/fs/en?CONTENT_ID=4000265&chk=0xvB%2B4 CIOB News 2005-02-16

⁵⁰ <http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=2482> CIOB News 2005-02-22

UK.gov Launches Virus Advice Site ⁵¹ (e-Services)

The United Kingdom (UK) government launched an official virus alert site [ITsafe](#) designed to help home users and small businesses use the net more safely through a combination of free advice and threat alerts about risks such as fast-spreading computer viruses. The service is funded by the Home Office and uses information provided by the National Infrastructure Security Co-ordination Centre (NISCC). Hazel Blears, the Home Office minister said: "The purpose of this new Government service is to ensure computer users are aware of the risks involved and how to deal with them easily and effectively without causing alarm."

Schemes To Boost e-Government ⁵² (e-Government)

The public sector IT managers' group Socitm and technology industry association Intellect launched separate initiatives in February to pinpoint gaps in government IT policy, and suggest how e-government could be improved. Socitm's e2Government programme is designed to promote efficient use of IT in local government. According to Socitm, current e-government initiatives focus too much on technology and improving access to services, while ignoring the need for back-office efficiencies. Glyn Evans, chair of Socitm's Information Age Government Group said, "every project should be approached with two things in mind: improving the service for the customers and making the service more efficient. e-Government is no different." Evans also called on IT chiefs in the public sector to break down the barriers between business staff and IT departments.

United States

Personal Identity Verification Standard ⁵³ (Biometrics / Smart Cards)

In response to Homeland Security Presidential Directive (HSPD-12), the National Institute of Standards and technology (NIST) Computer Security Division initiated a new project for Personal Identity Verification (PIV) of Federal employees and contractors. A set of Federal Information Processing Standards (FIPS) has been identified as being needed to: (1) properly protect the personal privacy of all subscribers of the PIV system, (2) authenticate identity source documents to obtain the correct legal name of the person applying for a PIV "card", (3) electronically obtain and store appropriate biometric data from the PIV system subscriber, (4) create a PIV "card" that is "personalized" with data needed by the PIV system to grant access to the subscriber to Federal facilities and information systems, (5) assure appropriate levels of security for all applicable Federal applications, and (6) provide interoperability among Federal organizations. FIPS 201 is scheduled for development and promulgation by February 28th, 2005.

US Technology Firms Endorse Health Data Plan ⁵⁴ (e-Government / Privacy)

Eight of the largest American technology companies, including IBM, Microsoft and Oracle agreed to embrace open non-proprietary technology standards as the software building blocks for a national health information network. The Bush administration has said that creating such network should be a national priority over the next several years. The goal is to improve care and reduce costs by abandoning paper and moving to a digital system for handling patient records, clinical research, claims and payments. Analysts said that such network, should save both lives and money.

ID Theft Surge Hits US Consumers ⁵⁵ (Authentication)

⁵¹ <http://www.theregister.co.uk/2005/02/24/itsafe/>

⁵² <http://www.vnunet.com/news/1161505> CIOB News 2005-02-25

⁵³ <http://csrc.nist.gov/piv-project/index.html#jan31> and <http://csrc.nist.gov/piv-project/index.html> CIOB News

2005-02-01

⁵⁴ <http://www.iht.com/articles/2005/01/26/business/health.html> CIOB News 2005-02-01

Almost a quarter of a million US consumers complained of being targeted for identity theft in 2004, official figures suggest. The Federal Trade Commission said two in five of the 635,173 reports it had from consumers' concerned ID fraud. Internet auctions were the second biggest source of fraud complaints, comprising 16% of the total. The total cost of fraud reported by consumers was \$546 million.

Bush Highlights IT Health Architecture, US Visit In State of Union⁵⁶ (e-Government / Smart Cards)

In his speech to the Congress, President Bush mentions two federal IT initiatives as part of his broad-reaching domestic agenda: (1) the federal health IT architecture, and (2) the government's entry-exit system. To give the first project higher profile, Bush named David Brailer as national health IT coordinator in May of last year. Most recently, Brailer's team at Health and Human Services Department (HHS) began reviewing responses to a request for information on how to build a medical Internet by 2007. For the second project, Homeland Security Department (HSD) has rolled out US Visit, its virtual border system, to the 50 busiest land crossings and plans to deploy the system to 115 additional land ports this year. More information is available at the following hyperlink: [GCN story](#).

DOD Certifies XML Product for PKI Use⁵⁷ (Interoperability / PKI / Cryptography)

The joint interoperability test command has certified that a security appliance for handling Extensible Markup Language (XML) messages can interoperate with other Defense Department public-key infrastructure equipment. The command OK'd the XS40 XML Security Gateway from DataPower Technology Inc. of Cambridge, Massachusetts, as interoperable with other approved PKI equipment. The gateway uses encryption, firewall filtering, XML schema validation and XML Access Control. Responding to the increased Defense use of PKI for access control and other security duties, the command created a team to work exclusively on PKI testing to certify the interoperability of hardware and software from different vendors.

NIST Urges Caution for Switch to Voice Over IP⁵⁸ (Interoperability)

Government agencies and other organizations that are considering switching their telephone systems to Voice Over Internet Protocol (VoIP) should carefully consider the security risks, says a recent report by the National Institute of Standards and Technology (NIST). VoIP is an important emerging technology that makes it possible to place telephone calls using a broadband Internet connection rather than traditional, circuit-based telephone lines. While it shows promise for lower cost and greater flexibility, VoIP has a different architecture than circuit-switched telephony. These differences, resulting from implementing security services such as firewalls or encryption, can cause poor voice quality and blocked calls if not done carefully and with the proper equipment.

OMB Considering Cybersecurity Standardization⁵⁹ (e-Government)

Office of Management and Budget (OMB) officials are considering standardizing the cybersecurity business processes of agencies in order to save money, increase security and help those with small information technology budgets. In this respect, a task force led by the Homeland Security Department (HSD) and OMB officials will meet in March, 2005 to consider whether the consolidation of common processes, services and technologies regarding security could improve performance while reducing costs. About \$4 billion is spent each year securing federal information technology; an OMB official speculated that 40 percent of that is spent on processes that are

⁵⁵ <http://news.bbc.co.uk/1/hi/business/4227293.stm> CIOB News 2005-02-02

⁵⁶ http://www.gcn.com/vol1_no1/daily-updates/34970-1.html

⁵⁷ http://www.gcn.com/vol1_no1/daily-updates/35028-1.html CIOB News 2005-02-08

⁵⁸ <http://www.govtech.net/news/news.php?id=92991> CIOB News 2005-02-09

⁵⁹ <http://www.govexec.com/dailyfed/0205/020805p1.html> CIOB News 2005-02-09

common among agencies. The task force would examine how much of the \$4 billion is spent on actual security improvements rather than duplicative administrative functions.

Tech Execs Ask Bush For Cybersecurity Commission ⁶⁰ (*Authentication / PKI*)

Technology executives from the largest US software companies called on President Bush to create a high-level commission to address cybercrime and identity theft. During a meeting with administration officials, chief technology officers from more than a dozen companies said the threat of malicious Internet incidents has become so great that a high-profile governmental response is necessary. "I think the reaction was very positive," said Chris Voice of Entrust.

Parents Protest Student Computer ID Tags ⁶¹ (*Privacy / Cryptography*)

On January 18th, 2005, at Brittan Elementary School, in a farming town northwest of Sacramento, California, students were asked to wear Radio Frequency Identification (RFI) badges that can track their every move. Some parents are outraged, in addition to the privacy concerns, they are worried that the information on and inside the badges could wind up in the wrong hands and endanger their children, and that radio frequency technology might carry health risks. School officials are dismissing each objection, arguing that the devices do not emit any cancer-causing radioactivity, and the 15-digit ID number that confirms attendance is encrypted, and not linked to other personal information such as an address or telephone number.

NASCIO Looks At Privacy Implications of Spam, Phishing and Spyware ⁶² (*Privacy*)

In response to the growing privacy concerns associated with Internet and email threats, National Association of State Chief Information Officers (NASCIO) released a study titled "Welcome to the Jungle: The State Privacy Implications of Spam, Phishing and Spyware." This trio of threats not only causes frustration and anxiety among computer users, but also can potentially compromise the privacy of citizen and government information through identity theft scams. The first portion of this research provides an overview of these potential privacy threats, including a discussion of their impact on state business processes, and concludes with a look at recent efforts to deal with them. For more information, see the hyperlink below:

<https://www.nascio.org/nascioCommittees/privacy/Spam%20Brief%20Welcome%20to%20the%20Jungle%20200805%20Final.pdf>

Defense Picks Two For PKI ⁶³ (*PKI / Smart Cards*)

Department of Defense (DOD) officials selected two companies: Tumbleweed Communications and CoreStreet as the two certificate validation providers for its Identity Protection and Management Program, which includes the Common Access Card smart card program for the department's public-key infrastructure (PKI). Some officials feel this decision could spur a faster move to paperless e-Government. DOD requires that all e-mail messages be digitally signed, which means PKI users must download a Certificate Revocation List (CRL).

New Book Makes Case For Digital Revolution In Government ⁶⁴ (*e-Government*)

⁶⁰ . http://news.zdnet.com/2100-1009_22-5571850.html CIOB News 2005-02-11

⁶¹ <http://www.globetechnology.com/servlet/story/RTGAM.20050210.gtfdfeb10/BNStory/Technology/> CIOB News 2005-02-14

⁶² <http://www.public-cio.com/newsStory.php?id=2005.02.15-93079> CIOB News 2005-02-15

⁶³ <http://www.fcw.com/fcw/articles/2005/0214/web-dodpki-02-15-05.asp>

⁶⁴ <http://www.govexec.com/dailyfed/0205/021505tdpm2.htm> CIOB News 2005-02-16

Before technology can transform the federal government, the government must become less hierarchical and agency-centered, an expert said. "I think that conventional wisdom is wrong," William Eggers, the author of the new book *Government 2.0*, said at a Cato Institute forum in Washington. Government must reshape its way of thinking about education and regulation, he said, and it must remake itself into a networked, citizen-centered and transparent structure. He envisions a network-centric government where information is shared across agencies in order to streamline processes, foster efficiency, improve services and ease access to information. He argues that under that model, private enterprises will find different ways to package government information.

The Fight Over Cyber Oversight ⁶⁵ (*e-Government*)

A recent security breach at data aggregator ChoicePoint was the topic of conversation as related to government regulation and corporate liability at the RSA Conference on security in San Francisco held on February 16th, 2005. Panelists discussing who should be responsible for company security breaches that result in identity theft or economic loss to customers were divided on whether government regulation would help improve security. The same experts said that companies will not get serious about securing their networks and protecting customer data until they are forced to do so by regulations that impose fines or other penalties for failing to secure their networks. Others argued that regulation would stifle innovation and wouldn't solve the problems since other regulated industries, like the energy and telecommunications industries, still have issues that regulation hasn't solved.

Coviello: Embrace Authentication ⁶⁶ (*Authentication*)

Software industry officials have blamed the slow expansion of e-Government and e-Commerce on a lack of trust in the Internet, but the problem can be overcome by treating electronic identities as digital assets, the head of RSA Security said this week. Electronic authentication must become commonplace across the Internet before public agencies and companies will be willing to open up their networks for business transactions, said Art Coviello, president and chief executive officer of RSA Security. How those agencies and corporations provide e-authentication is not as important as just doing it, "there is no single answer. Organizations will need to check devices for accurate configurations and patches before they allow them to connect to the network." Coviello said.

NIST Sets ID Schedule ⁶⁷ (*PKI / Authentication*)

National Institute of Standards and Technology (NIST) reported that federal officials laid out a deadline this week, February 14th, 2005 for federal agencies to comply with an executive order known as Homeland Security Presidential Directive (HSPD) 12. The executive order relates to issuing federal employees and contractors identity cards that conform to a new government wide standard, Federal Information Processing Standards (FIPS 201). Judith Spencer, chairwoman of the Federal Public Key Infrastructure Steering Committee said that by June 25, officials must tell Office of Management and Budget (OMB) officials how they plan to comply with the directive's requirements. The HSPD 12 implementation deadline for agencies is October 27th, 2005.

Fingerprint Standard Still Elusive ⁶⁸ (*Biometrics / Interoperability*)

According to a December 2004 Justice inspector general report, progress toward making all biometric fingerprint systems fully interoperable has stalled, partly because Department of Justice

⁶⁵ <http://www.wired.com/news/print/0,1294,66632,00.html> CIOB News 2005-02-17

⁶⁶ <http://www.fcw.com/fcw/articles/2005/0214/web-coviello-02-16-05.asp>

⁶⁷ <http://www.fcw.com/fcw/articles/2005/0214/web-nist-02-16-05.asp>

⁶⁸ <http://www.fcw.com/fcw/articles/2005/0214/web-fingers-02-18-05.asp>

(DOJ), the Homeland Security Department (HSD) and Department of States (DOS) had not agreed on a uniform fingerprint technology standard.

No Encryption For e-Passports⁶⁹ *(Cryptography)*

Despite widespread criticism from security experts that a proposed high-tech upgrade to Americans' passports actually introduces new security risks, the government is declining to encrypt data on new high-tech e-passports. In response to this criticism and some public questioning, the State Department delayed its rollout of the chip-equipped passports and hired additional companies to provide prototypes. Other countries are also wrangling with the issue, as the United States is requiring all 27 countries whose citizens do not need visas to visit America to begin issuing e-passports by October 2005. So far only Belgium has started production, and it is likely the deadline, which was originally October 2004, will be pushed back another year.

DHS Names Privacy Committee⁷⁰ *(Privacy)*

The Homeland Security Department (DHS) announced the appointments of 20 members to the Data Privacy and Integrity Advisory Committee that will advise the department's secretary and Chief Privacy Officer on issues that affect privacy, data integrity, and data interoperability. "This committee will provide the department with important recommendations on how to further the department's mission while protecting the privacy of personally identifiable information of citizens and visitors of the United States," Nuala O'Connor Kelly, DHS's Chief Privacy Officer, said in a press release. "The diversity of experience and perspectives represented by this committee will play an important role in advancing the national discourse on privacy and homeland security."

GAO Wants Better US-VISIT Oversight⁷¹ *(Biometrics)*

Government Accountability Office (GAO) officials released a report that calls for program management scrutiny and exit system reassessment for the US Visitor and Immigrant Status Indicator Technology (US-VISIT) program. The report focused on the implementation of US-VISIT's exit system, which records foreign visitors' departures. As of November 2005, the system was operational at only five of 15 ports of entry scheduled for evaluation of exit. Eight international airports and one seaport are conducting exit tests. For entry, Customs and Border Protection (CBP) officers use biometrics to determine if someone attempting to enter the United States matches the visa issued by the State Department.

Screening Metrics Need Work, GAO Says⁷² *(Authentication)*

Government Accountability Office (GAO) officials released a report on measures that the Homeland Security Department (HSD)'s Transportation Security Administration (TSA) has developed for determining whether commercial data can improve airline passenger pre-screening, and concluded that TSA's initial work is inadequate. More work has to be done to allow HSD and TSA officials to use the test results to develop policies in TSA's Secure Flight passenger prescreening program. The Secure Flight testing will occur in two phases. One tests how historical passenger data matches an expanded terrorist watch list. The other will determine if the use of personally identifiable commercial data can improve the prescreening process. According to the report, overall system testing will begin in early June 2005.

⁶⁹ <http://www.wired.com/news/print/0,1294,66686,00.html> CIOB News 2005-02-24

⁷⁰ <http://www.fcw.com/fcw/articles/2005/0221/web-dhsprivacy-02-23-05.asp>

⁷¹ <http://www.fcw.com/fcw/articles/2005/0221/web-usvisit-02-24-05.asp>

⁷² <http://www.fcw.com/fcw/articles/2005/0221/web-tsa-02-24-05.asp>

GSA Works On ID Guide ⁷³ (*Smart Cards / Biometrics*)

General Services Administration (GSA) officials are developing a guidebook to help federal agencies comply with the upcoming standards on issuing secure credentials to their employees and contractors. Judith Spencer, chairwoman of the GSA's Federal Identity Credentialing Committee, said the Identity Management Handbook for the Federal Information Processing Standard (FIPS) 201 will provide checklists, recommendations, best practices and other guidance to help officials complete their plans for implementation. The common credential is expected to improve security by providing a common way to authenticate identity for access into physical facilities and information systems. It will require officials to issue smart cards in some cases. Some cards will need biographic and possibly biometric data.

Making It Harder To Get A Driver's License ⁷⁴ (*Smart Cards / Biometrics / Authentication*)

The Senate will soon take up a House bill that seeks to establish uniform security standards for state-issued driver's licenses and identification cards. Part of the *Real ID Act*, which passed the House's vote this month, February 2005, would require states to incorporate minimum information and features into every license and ID card, including biographical data, digital photographs and physical security features to prevent fraud. The States would also be required to use a common machine-readable technology with defined minimum data elements. Under the bill, federal agencies would not have to accept for official purposes any state-issued driver's license or identification card that does not meet the proposed standards.

Venezuela

No new item to report.

Viet Nam

No new item to report.

⁷³ <http://www.fcw.com/fcw/articles/2005/0221/web-ficc-02-23-05.asp>

⁷⁴ <http://www.fcw.com/fcw/articles/2005/0221/pol-license-02-21-05.asp>

Miscellaneous

Govts To Get Early MS Warnings ⁷⁵ (e-Government)

Microsoft wants to work with governments to help prevent and mitigate the damage from hacker attacks. The announcement made by Microsoft chairman Bill Gates, coincides with a mounting threat to the company's global dominance from open source software alternatives such as the Linux operating system. Proponents say open-source software is cheaper to run and less vulnerable to security threats because the underlying code is freely shared. Government agencies and municipalities from China and Japan to Germany and France are embracing or investing in developing open source systems. Microsoft already provides the US government with early warnings. The new program is intended to complement Microsoft's existing Government Security Program

OASIS Consortium Members Approve UDDI Version 3 As An OASIS Standard ⁷⁶ (Interoperability)

Version 3 of the Universal Description, Discovery, and Integration (UDDI) specification, in development since mid-2002, has been ratified as an OASIS Standard. Based on a common set of industry standards, including HTTP, XML, XML Schema, and SOAP. UDDI provides an interoperable, foundational infrastructure for a Web services-based software environment for both publicly available services and services only exposed internally within an organization. The key objective in UDDI Version 3 is to support secure interaction of private and public implementations as major element of service-oriented infrastructure.

Identity Theft, Loss Of Privacy Face People In A Wired World ⁷⁷ (PIPEDA)

The New York Times reported that identity theft is one of the fastest growing white-collar crimes. There were almost 10 million identity theft victims in 2003, resulting in about \$48 billion in losses to businesses and \$5 billion in out-of-pocket expenses to individuals trying to regain their identities. In Canada, there is a legislation such as *the Personal Information Protection and Electronic Documents Act* (PIPEDA) that provides new powers to victims of identity theft that could use it and other laws as recourse against the business that indirectly facilitated the crime.

Shared-Services In Government ⁷⁸ (e-Government)

According to a study released recently by Accenture, the majority of government executives believe that shared services are important to helping them achieve their organizations' strategic goals. Accenture interviewed more than 140 senior executives at all levels of governments across 13 countries in Europe, North America, the Asia Pacific region and Africa. Eighty-five percent said they believe that shared services are playing or will play a role in supporting their organizations' strategic goals. In addition, two-thirds (66 percent) of the government executives reported that they had already implemented, or were in the process of implementing, shared services, while 6 percent of respondents said they would not even consider a shared services model. The most common processes found in government-shared services are related to information technology, finance and human resources.

⁷⁵ <http://australianit.news.com.au/articles/0,7204,12135030%5E15306%5E%5Enbv%5E,00.html> CIOB News 2005-02-03

⁷⁶ <http://xml.coverpages.org/ni2005-02-02-a.html> CIOB News 2005-02-03

⁷⁷ CIOB News 2004-02-05

⁷⁸ http://www.govtech.net/magazine/channel_story.php?channel=17&id=93082 CIOB News 2005-02-17

Move Over, Passwords, and Make Room For Tokens ⁷⁹ (Authentication / PKI / Smart Cards)

At the RSA Conference in San Francisco, two security vendors announced new tokens to gain access to computers through a Universal Serial Bus (USB). The first is RSA Security Inc. who announced the SecurID SID800 that can be used for "strong authentication" (two or more ways of identifying a user). RSA also unveiled the SecureID SID700, which is 35% smaller than SecurID authenticator. The second is VeriSign Inc. who announced that it will offer a one-time password token with a total cost of operation per user of less than \$10 a year. The USB authenticators can be used to store one-time passwords, PKI credentials, and provide functionality similar to that of smartcards.

How To Stop Junk e-Mail: Charge For the Stamp ⁸⁰ (Digital Signatures / Cryptography)

Internet service providers are starting to stamp outgoing messages with a digital signature of the customer's domain name, using strong cryptography so the signature cannot be altered or counterfeited. This is accomplished with software called DomainKeys, originally developed by Yahoo. It is now offered in open-source form and was recently adopted by EarthLink and some other major services.

Authentication and Digital Signatures In e-Law and Security (A Guide for Legislators and Managers) ⁸¹ (Authentication / PKI / Digital Signatures)

The problem of authentication in the online world goes to the heart of trust and therefore confidence-building for ecommerce and all of the benefits that this entails. This paper seeks to provide an understanding about the different ways of assuring authentication. These authentication rules and tools, including for example Public Key Infrastructure (PKI), are sometimes meant to set a legal and technological framework for trustworthy electronic transactions, promoting e-Procurement, e-Commerce, e-Business and e-Government.

Nearly Half of Confidential Data Stays On The PC When The PC Leaves ⁸² (Privacy)

University of Glamorgan, England research revealed that organizations are failing to follow security measures to erase confidential information from computers before machines are disposed of. Andy Blyth, who leads the research of the Information Security Research Group at the university said, "the research project was concerned with measuring the level at which personal and commercial data is being made available on the used computer market. In particular, the project wanted to examine the extent to which commercial data was available via computer hard disks. We are used to this kind of work as we have functioned as expert witnesses for both regional and national high tech crime units; however, the results were still surprising."

Information Security Forum Announces New Standard of Good Practice ⁸³ (e-Government / Privacy)

Information Security Forum (ISF) announced the latest version of its international industry benchmark, the Standard of Good Practice for Information Security. The ISF 2005 Standard of Good Practice pays particular attention to current hot issues such as secure instant messaging,

⁷⁹ <http://www.banktech.com/news/showArticle.jhtml?articleID=60401347> CIOB News 2005-02-17

⁸⁰ <http://www.nytimes.com/2005/02/13/business/yourmoney/13digi.html> Thanks to HD

⁸¹ <http://topics.developmentgateway.org/edevelopment/rc/filedownload.do~itemId=1027239> Thanks to HD

⁸² <http://www.usabilitynews.com/news/article2253.asp> CIOB News 2005-02-28

⁸³ http://www.managinginformation.com/news/content_show_full.php?id=3567 CIOB News 2005-02-28

web server security, patch management and virus protection as well as important and changing areas of information security including information risk management, outsourcing, privacy and the disappearance of the network boundary. Compiled by some of the world's leading independent experts in information security, the Standard is based on over 16 years and \$75 million of investment in practical research.