

To EURIM Members and Observers

From Philip Virgo, EURIM Secretary General
15 Chestnut Road, London SE27 9EZ
Tel:020 8761 5926; Fax:020 8670 4345
E-mail: virgo.philip@eurim.org

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



EURIM Newsletter May 2006

1) Delivering Transformation

Addressing Cobb's Paradox

“We know why projects fail, we know how to prevent their failure – so why do they still fail?” - Martin Cobb: Treasury Board of Canada Secretariat. The full responses to the Transformational Government consultation are on www.cio.gov.uk/transformational_government/responses/index.asp. They contain considerable food for thought but short-term expediency will continue to lead to long-term failure until it becomes the norm to build good practice into the initial policy formation rather than subsequently muzzle those who seek to point out the risks of being at the bleeding edge. That entails involving those with delivery experience in developing and reviewing proposals *before* they are put to ministers. Hence EURIM's firm commitment to supporting the ideas now emerging from the CIO Council.

The EURIM Council has given the Transformational Government group two core objectives:

- to convince industry and parliamentarians that e-Government really can achieve fundamental improvements in service delivery to the citizen, at affordable cost.
- to make sure that the citizen really is at the centre of the agenda, with shared services tailored for access/use by those who most use the services to be transformed

The initial task is to identify examples of shared services across authorities, departments and agencies and use these to demonstrate that organisations can co-operate successfully. The more difficult, longer term, task is to ensure that the Transformational Government and Social Inclusion action plans are integrated and do not operate as parallel streams.

On the afternoon of 8th May, in parallel with the break-out sessions of the Government IT Summit, Margaret Moran will chair a Group meeting to ratify the objectives, explore the issues, agree priorities and allocate responsibilities. Please email emma.fryer@eurim.org if you would like to attend or would like to be involved subsequently and receive outputs.

“Shared services cannot be forced”

On April 23rd the “latest news link” on www.cio.gov.uk was to a Computer Weekly story headlined “Shared services cannot be forced”. Some EURIM members have strongly welcomed the implication that these are *not* intended to be synonymous with a new generation of centrally planned, standardised, outsourcing contracts. But changing the ingrained habits of central government and its suppliers, let alone politicians of all colours, requires sustained effort. Moreover bottom-up sharing requires effective interoperability standards in order to gather momentum and deliver benefit.

Delivering Interoperability

The eGIF standards are central to achieving TG objectives, but the high levels of take-up in local government are in marked contrast to those achieved by central government departments. There are also concerns as to whether changes to the rules on government security (and to use of the government secure intranet) that would open the door to greater use of eGIF-compliant off-the-shelf software have been fully understood. EURIM is therefore organising a round table meeting on the morning of Thursday 18th May focussing on the UK issues of Interoperability with respect to the current and potential role of eGIF within the Transformational Government agenda (shared systems and services as well as data and identity); the issues that need to be resolved; and how EURIM can help. Contact Dave Wright (davywright2@ntlworld.com) if you would like to comment or attend the meeting.

2) **Demonstrating success**

Secure identity management is on the critical path

The TG Implementation Plan at <http://www.cio.gov.uk/documents/pdf/transgov/transgovt.pdf> is based on “an holistic approach to identity management based on a suite of identity management solutions” via a range of measures which “will converge towards biometric identity cards and the National Identity Register”, with appropriate physical and legal safeguards. Recent market research in the US and Canada indicates that on-line users respect the identity management systems of the banks rather more than those of government and considerably more than those of Internet or e-commerce service providers. There is now a plethora of would-be technology and service suppliers making grandiose claims as to what they can supply to government. It is therefore essential to brief parliamentarians and policy makers on the lessons learned by those who have been running shared identity management systems, some for a decade or more. The Personal Identity Group is looking at how best to achieve this. Please e-mail eurim@eurim.org if you would like to help organise this or attend workshops introduced by those with practical experience of developing and running such systems over time.

Showcases of public success in information sharing

It is good to read in the Implementation Plan that Government is 'working to clarify its strategy ... to see what more can be done to retain trust in services that involve sharing information', that 'data sharing is an integral part of designing new and improving established public services' and that the Information Commissioner will be involved in assessing the potential impact on individual privacy. We also need to build on the £billions already invested (some very successfully) in IT across the public sector, particularly in local government. On 22nd June, EURIM is organising a “showcase” in the Attlee Suite, Portcullis House, at which members and observers will display successful examples of information sharing across organisational boundaries. The aim is not only to give parliamentarians and policy advisors an opportunity to see what has already been delivered but to involve more MPs in helping publicise that which is already delivering benefit to voters in their own constituencies. For more information on this event, contact Dave Wright (davywright2@ntlworld.com).

3) **E-Crime: Moving the goalposts**

Co-operation in turning problems into opportunities

The reported losses from computer assisted crime may still be “in the noise level” but it is apparent that industry now spends at least as much on electronic security as it does on physical security while the public sector spends very much less. Much current spend is seen to be duplicated or wasted and there is a growing user view that well-targeted co-operation could remove many of the vulnerabilities and those who exploit them. Meanwhile the recent sharp increase in the volume of “malware” is having significant impact on the behaviour and attitudes of Internet users and commercial ISPs are responding to the changing priorities of those they wish to attract as paying customers, especially parents, small firms and the silver surfers who control most of the nation’s disposable wealth.

Police-Industry co-operation in reporting, intelligence and reduction

Public reaction to the withdrawal of the NHTCU website after the launch of SOCA has so far been muted but private reactions from those representing industry, both users and suppliers, has been sharp. The agenda for the meeting on 28th April was therefore expanded to include reviews of current UK reporting mechanisms, evidence on the cost of computer assisted crime and the need, if any, for rapid action to replace the NHTCU guidance for small firms and others whose confidence in e-commerce might have been shaken by recent developments.

The responses to a Google search on 18th April asking how to report a computer crime? included:

Australia: <http://www.netalert.net.au/01601-How-do-I-report-an-E-crime.asp>

NZ: <http://www.police.govt.nz/service/ecrime/netsafe.html>

USA: <http://www.usdoj.gov/criminal/cybercrime/reporting.htm>

UK: <http://www.met.police.uk/computercrime/>

The SOCA page that has replaced the NHTCU website leads to <http://www.police.uk/> and the minor incident reporting system. Apart from the IWF, other UK sites appear to be largely invisible to those who do not already know they exist.

Previous plans for e-crime prevention pilots had assumed use of the NHTCU website as a common, authoritative source, including to maintain links to the many sites providing guidance on self protection and what to do, short of reporting to law enforcement, in the event of becoming a victim.

The E-Crime group is now looking at the practicality of taking the relevant material and links from the NHTCU site and using these as the basis of a shared service, perhaps organised by a consortium of regional police forces and e-commerce (including banking and Internet Service Provider) security teams which will enable the websites of all participants to provide current guidance, including on self-protection and reporting. The meeting also discussed the need for much greater co-operation between those already running reporting and intelligence services and recommendations will be circulated for comment later this month.

From frightened and confused awareness to educated confidence

There are now National Occupational Standards for most of the skills needed and courses and qualifications for many, but much less progress has been made in ensuring that these are delivered to and obtained by those who need them. On the morning of 5th May we will review who is currently doing what with the objective of agreeing recommendations and action plans, beginning by identifying what is already available. There is also a need to publicise examples of current good practice, (e.g. training all staff/users in basic systems security). Is anyone else doing this? If not, is this an action that our members and observers would wish to organise via EURIM? Please e-mail eurim@eurim.org if this area is of direct interest to your organisation.

Leader or laggard in the confidence stakes

Finland has stated that Internet safety and security will be the main priority for its Presidency and is said to have made impressive progress in addressing the issues. How true is that? How much have we to learn from others? On the morning of 16th May the Group will review its current recommendations for UK action before going firm on those for inclusion in the policy papers for launch in June/July. These main recommendations can be summarised as:

- A well publicised e-crime reporting and prevention network, funded and resourced by law enforcement, industry and government (including government as target/victim).
- One or more, non-geographic Cyberhood policing units building on lessons from the British Transport Police and the Dedicated Cheque and Plastic Crime Unit.
- Basic Internet Safety and Systems Security to be mandatory on all publicly funded ICT courses and qualifications and for all public sector end-users, including contractor staff.
- Suppliers to be “encouraged”, including by public sector procurement, to provide, support and “police” more secure systems/services, with end-over-end filtering, authentication and track and trace facilities – using terms and conditions of service and contract/civil law.
- Adequate penalties for Computer Misuse and for unauthorised information access and sale, especially of information that might be used to aid identity theft or impersonation.
- Greatly enhanced police forensic skills and resources, because for some forces (e.g. MPS) the majority of investigations already involve digital evidence/intelligence.

There are also six areas for “immediate” actions:

- Collate available evidence on the scale, nature and cost of computer-assisted crime. If this really does indicate a serious problem, convey this “privately but forcefully” (with “colourful” examples to add impact to statistics) to those who control the necessary decisions, budgets and resources.
- Build on the NHTCU brand, maintained and supported by an equally trustworthy host, as a trusted source of advice and support.
- Test the new CMA legislation and also bring forward legislation to update penalties under the DPA (referenced in the Transformational Government Implementation Plan).
- Organise adequate resources for the Office of the Information Commissioner to investigate and prosecute abuse and show whether current frameworks are adequate.
- Organise and evaluate local e-crime reporting and prevention pilots and the use of specialist specials to provide digital analysis and investigation skills in support of local forces.

Underlying the recommendations is, however, a growing conclusion that those who wish to preserve confidence in on-line transactions have to accept that they should stop wasting time calling for action from law enforcement, unless they are ready to pay for it. They also need to take action to persuade mainstream politicians that the subject is urgent as well as important because, even if they have no wish for new government initiatives, they need to ensure that they are allowed to take collective action to do what is necessary. This requires that co-operation takes place within credible governance frameworks. Hence the importance of exercises like the current Nominet consultation <http://www.nominet.org.uk/policy/consultations/Raising+Industry+Standards/> on the policing of “.uk”.

Changing the political climate

The planned parliamentary briefing on current Internet Safety activities, including the work and role of the new Child Exploitation and Protection Agency is being rescheduled into May and invitations will be sent to MPs and Peers shortly. Additional parliamentary briefings by high-profile speakers are being planned to cover the effects on mainstream policing (as traditional criminals make ever-increasing use of new technologies to organise physical crime) and on the impact on the take-up of e-commerce, e-banking and e-government. These are intended to help set the scene for a major event in October, when we expect to work alongside several of the all-party groups (including APIG and PITCOM), to brief MPs on the issues of convergence.

4) Communications Policy and Regulation

The politics of convergence

EURIM have agreed to address the issues of convergence of communications and products, in co-operation with All-Party Groups looking at ICT, Internet, Mobile and Telecoms issues, with the intention of bringing together leading companies, trade associations and lobby groups so that policy-makers can better understand the challenges, and the expected benefits to the economy and society. Part of that co-operation is due to be a major joint event in mid-October and part of the EURIM contribution will be a number of round tables on regulatory, policing and governance issues: to identify who is currently lobbying for what - as consumers increasingly access similar content over PC, Mobile, TV or Games Console (whether or not the owners have given permission). Please contact Dave Wright (davywright2@ntlworld.com) if you are interested in participating.

Relations with US Internet Caucus

Subject to the necessary support from our Corporate and Associate members, EURIM has also agreed to organise the next round of discussions with the US Internet Caucus, in London and Washington. Internet safety, electronic security and co-operation in the fight against computer-assisted crime and terrorism are expected to be top of the political agenda on both sides.

Building confidence in “.uk”

As part of the current Nominet consultation into the means of improving confidence in “.uk” domain names <http://www.nominet.org.uk/policy/consultations/Raising+Industry+Standards/> we have agreed to help organise a workshop to discuss issues such as whether “.co.uk” should be confined to those with a physical trading address in the UK, with “.ltd.uk” for those filing accounts with companies house (with registered office and company number included in the "whois" entry) and that we should have “.bank.uk” and “.fsa.uk”, available only to organisations regulated by the FSA. Other questions include whether the routine whereby domain names may be registered anonymously "in exceptional circumstances" should be replaced by an explicit “.anon.uk” or if those providing website services who register in their own name, as opposed to that of the client, should be liable for the content until such time as they have transferred the entry (i.e. given an incentive to follow "good", as opposed to "common", practice). The meeting (date and venue yet to be agreed) will also discuss possible UK priorities for the Internet Forum in Athens later this year. Please e-mail eurim@eurim.org if you would like to help organise or attend this workshop.

EURIM Timetable – May-June 2006

This timetable lists forthcoming meetings arranged by EURIM and events arranged by other organisations which are likely to be of interest to EURIM's Members and Observers. Unless otherwise indicated EURIM meetings are open to all members and accredited observers. There is no charge for attendance but prior registration is required. If you wish to attend or would like more information please contact the named individual or eurim@eurim.org. For information about meetings arranged by other organisations, please contact the person or website indicated against the entry. Note that for some events, there is an entry fee and pre-registration is essential.

May

- Date:* Friday **5** May 2006
Time: 09.30 for 10.00 - 12.30
Venue: BCS, Southampton Street, London WC2
Organiser: EURIM E-Crime Group
Description: Review of current situation regarding skills, courses & qualifications from end-user awareness & self-protection upwards & actions & recommendations arising.
Attendance: E-Crime participants & guests
- Date:* Monday **8** May 2006
Time: 13.30 - 15.30
Venue: Committee Room 8, House of Commons
Organiser: EURIM Transformational Government Group
Description: Planning Meeting to ratify objectives, explore issues, agree priorities & allocate responsibilities.
Attendance: EURIM Members only
- Date:* Monday **8** May 2006
Time: 18.00 - 20.00
Venue: Grimond Room, Portcullis House
Organiser: Conservative Technology Forum
Description: Television Without Frontiers
Attendance: More details at www.conservative-technology.org
- Date:* Tuesday **9** May 2006
Time: 15.30 - 16.45
Venue: 1 The Abbey Gardens, Great College Street, SW1
Organiser: EURIM
Description: Board & Council meetings
Attendance: Directors, Council members & invited guests only
- Date:* Tuesday **9** May 2006
Time: 17.00 - 18.00
Venue: 1 The Abbey Gardens, Great College Street, SW1
Organiser: EURIM
Description: Annual General Meeting
Attendance: EURIM Members only
- Date:* Tuesday **16** May 2006
Time: 09.30 for 10.00 - 13.00
Venue: BCS, Southampton Street, London WC2
Organiser: EURIM E-Crime Group
Description: Plenary Meeting to review Strategy & Recommendations with a focus on priorities, points of leverage & structures for co-operation, including for improving the end-over-end security of e-commerce & communications products & services.
Attendance: E-Crime participants & guests

Date: Thursday **18** May 2006
Time: 10.00 - 12.00
Venue: Room 'N', Portcullis House, Westminster
Organiser: EURIM Personal Identity & Transformational Government Groups
Description: Workshop on UK Interoperability, including the current & prospective role of e-GIF within the TG agenda (shared systems & services as well as data & identity).
Attendance: PI & TG participants & guests

Date: Monday **22** May 2006
Time: 18.00 - 19.30
Venue: Westminster
Organiser: PITCOM joint with All-Party Group on Telecoms
Description: Vulnerability of the Infrastructure
Attendance: PITCOM members only www.pitcom.org.uk

Date: Tuesday **23** May 2006
Time: pm
Venue: Westminster
Organiser: Westminster Media Forum
Description: From TV without Frontiers to Audiovisual Media Services Directive with James Purnell MP, Minister for the Creative Industries, DCMS.
Attendance: For details please contact pvg@westminsterforumprojects.co.uk

Date: Tuesday **30** May 2006
Time: 18.00 for 19.00 - 22.00
Venue: Westminster
Organiser: Real Time Club
Description: After Dinner Debate on ID Cards: introduced by Ian Angell, LSE.
Attendance: Contact Carmen.Harvey@btopenworld.com for details

June

Date: Monday **5** June 2006
Time: 18.00 - 20.00
Venue: Westminster
Organiser: Conservative Technology Forum
Description: Television without Frontiers
Attendance: More details at www.conservative-technology.org

Date: Tuesday **20** June 2006
Time: 18.00 for 19.00 - 22.00
Venue: Westminster
Organiser: Real Time Club
Description: IT on Stage: Musical, Opera or Rock Concert - the event is usually a multi-media extravaganza programmed in real time. Why IT is not just for nerds.
Attendance: Contact Carmen.Harvey@btopenworld.com for details

Date: Thursday **22** June 2006
Time: 09.30 for 10.00 - 14.00
Venue: Attlee Suite, Portcullis House
Organiser: EURIM Personal Identity & Data Sharing Group
Description: Showcase of successful examples of public sector sharing involving EURIM members & observers
Attendance: Invited MPs, Peers & Officials from Central & Local Government

Date: Monday **26** June 2006
Time: 18.00 - 19.30 Meeting 19.30 - 21.00 Reception
Venue: House of Lords Terrace
Organiser: PITCOM
Description: Meeting followed by 25th Anniversary Reception
Attendance: PITCOM members only www.pitcom.org.uk