

SBL'S ICS CATALOGUE CONTRACT LAUNCH EVENT

Thursday 17th July 2008
One Great George Street,
Westminster, London

Open to UK Public Sector Organisations & MoD

The Information & Communications Services (ICS) Catalogue, operated by DE&S Information Systems & Services Commercial Services, provides a supply route for IT/IS for the Ministry of Defence and other UK Public Sector organisations.

This event will provide an overview of the features and benefits of purchasing through the ICS Catalogue - What is it? How does it work? What are the benefits over other government frameworks? Who can take advantage of the benefits?

Places are limited, so please register your interest in attending by emailing sbl_secretariat@softbox.co.uk or phoning 01347 812176 and we will send you further details.



Software Box Ltd
East Moor House,
Green Park Business Centre,
Sutton on the Forest, York,
North Yorkshire YO61 1ET
T. 01347 812100
F. 01347 811225
E. enquiries@softbox.co.uk
W. www.softbox.co.uk

Issue 03

firmatters

The IT Solutions Journal from Software Box Limited

DO YOU NEED TO PROTECT YOUR DATA?

The ICS Catalogue is for you – the route to market for Information Assured products & services.

HOW SAFE IS YOUR SECURE DATA DISPOSAL?

Barron McCann addresses the data security issues regarding the WEEE (Waste Electrical & Electronic Equipment) directive.

This issue's focus

INFORMATION ASSURANCE IN THE PUBLIC SECTOR

Addressing the issues the public sector face, and featuring articles from DE&S, CSIA & CCTM.

Published by  SBL

CONTENTS

The Route to Market for Information Assured Products & Services
The ICS Catalogue **PAGE 4**

Canon
Have you ever thought of what data is held on your Multi-Functional Device?
PAGE 6

SBL's ICS Catalogue Contract Launch Event **PAGE 7**

How Safe is your Secure Data Disposal? Barron McCann address the issues **PAGE 8**

Delivering Confidence in Information Security An overview of the CESG Claims Tested Mark (CCTM) **PAGE 9**

Symantec Announces Launch of Endpoint Encryption 6.0 **PAGE 10**

SBL's Training Course Schedule **PAGE 12**

Purchasing through the ICS Catalogue An overview from SBL **PAGE 14**

SBL's Information Assurance Services **PAGE 16**

What is the Intelligent Customer Mechanism? **PAGE 17**

SBL's Mobile Device Encryption Service **PAGE 18**

Complete Data Protection Solution with SBL, Toshiba & FlagStone **PAGE 17**

Publication by **SBL**

Designed & Produced by Ghost Creative
www.ghostcreative.co.uk

WELCOME TO IT MATTERS

This issue's focus – Information Assurance in the Public Sector.



Welcome to the 3rd issue of SBL's publication "IT Matters".

IT Matters is a quarterly publication, and is a collation of business issue led articles around a specific industry theme. The primary aim of the publication is to create a useful resource of information for our customers on current issues within the IT industry.

SBL are attending IA08 – The Government's Information Assurance Event – and this edition of IT Matters focuses on issues around IA for the public sector. SBL are pleased to be partnering at IA08 with Canon.

SBL have been awarded contracts on the Information & Communications Services (ICS) Catalogue, operated by DE&S Information Systems & Services Commercial Services, to supply Information Assurance Products, and Hardware & Software. These contracts are available for both MoD & UK Public Sector organisations to purchase through.

SBL are Information Assurance Specialists & Market Leaders, and have the expertise and experience to assist you with your IA strategy.

We are pleased to feature an article from DE&S, providing an overview of

the Information Assurance section of the ICS Catalogue.

To help guide you through the new ICS Catalogue, and looking specifically at the IA section of the contract, why not register for SBL's ICS Catalogue Contract Launch Event, that is taking place on 17th July 2008 in London? Go to page 7 for more details.

In addition, we have articles from CSIA, looking at the Intelligent Customer Mechanism (ICM), which is at the heart of the Information Assurance Technical Programme, and an update on the CESG Claims Tested Mark (CCTM).

I hope you enjoy this issue of IT Matters - we are always interested in hearing your comments and suggestions on the publication, so please feel free to contact me or your SBL Account Manager.

Emma McGhin, Editor

Emma_McGhin@softbox.co.uk

IA08 Special Edition - JUNE 2008

IA08 marks a watershed, perhaps even a seminal, moment in the development of Information Assurance (IA) throughout the public sector.

Under any normal circumstances, IA08 would be significant enough; gathering as it does the leadership of the IA community across both the public sector and government. These, however, are not normal circumstances.

Last year, IA07 saw the combined release and launch of the new version of the National Information Assurance Strategy (NIAS). The new NIAS offered a strategic framework capable of giving coherence, structure and direction to the essential activity required if we were to translate the desire that IA should become a business enabler, away from a worthy exhortation, and in to some form of reality. As we left Brighton, we did so with the collective sense that the year ahead would be the 'year of IA'; that it would be challenging though rewarding; and, that IA08 would furnish us with the platform to advertise, assess and analyse our progress in twelve months time. As we now know, events were to transpire to take us in a different direction.

IA08 now takes place against a backdrop dominated by the IA implications of those significant events as they occurred from the autumn of 2007 onwards. These events have given us a high profile illustration of what happens to the public's trust in government's ability to operate as a custodian of personal data when effective IA measures are not applied.

Although these events were extremely unfortunate in themselves, in general, the response to them has had a positive and welcome effect. It has focused attention on the importance of good IA and has sharpened the sense of individual responsibility and accountability for the practice of IA outside the small community of IA professionals. In particular the activity

around Data Handling Review (DHR) has directed considerable attention and effort on what needs to be done to improve the treatment of sensitive data across both government and the wider public sector. Some of the activity prompted by the DHR has made a constructive contribution to the ongoing work of implementing the NIAS.

That said, the work on the DHR has brought with it a range of costs. Some of these have been opportunity costs in that effort and resource which was committed to work on the NIAS has been diverted to the DHR. Some of these have been more direct costs as departments have sought to remedy deficiencies in their IA product and service provision. Some of these costs have been less tangible and, regrettably, far less productive. Care must be taken that the current climate does not drive inappropriate procurement decisions, the longer term impact of which might be to erode confidence in the advice of IA professionals.

There are already indications that, in some quarters the work on the DHR and, indeed, the nature of the events that preceded it has been taken to bolster legacy and redundant notions of risk avoidance. This has, for instance, found form in the expression of the view that these events should lead us to question, and even restrict, the use of IT in the provision of public services because IT systems cannot be trusted to store and communicate sensitive personal data. This is essentially a view driven by a philosophy of risk avoidance rather than risk management. We should be attuned to recognise this danger and willing to counter it with a proposition based on the efficacy of minimum standards applied with pragmatism



and an awareness of the balance of business and information risk.

It is precisely the function of pragmatic, appropriate and cost effective IA to enable trust in, and therefore use of, computers across an ever increasing spectrum of human activity.

The reality of the Information Age is that IT is now pervasive across every sphere of human activity. We are reaching the point where it is impossible to conceive of a modern economy functioning without ubiquitous computing. And yet the vast potential of our IT capability remains unfulfilled. If this potential is to be realised then it is essential that we attain the provision of pragmatic, appropriate and cost effective IA. Likewise it is essential that we redefine the relationship between business and IA. The construction and maintenance of new trust relationships must be at the heart of this endeavour. IA is at the heart of these new trust relationships.

IA08 now provides us with a unique opportunity to synthesise the work on the DHR with the work on the NIAS. We can now increase the scope of our attention away from the important, but narrow, concerns around data handling, and towards the wider and more inclusive practice of IA. By so doing we can establish a forward momentum around IA, which, over the forthcoming twelve months we can harness to the task of building an era of renewed and deeper trust in both public sector IT systems, and in the ability of government to handle personal data.

Colin Williams
Director, SBL
Chair, IACG

THE ROUTE TO MARKET FOR INFORMATION ASSURED PRODUCTS & SERVICES

(Non High Grade Crypto)

Do you need to protect your data? Of course you do! Then the ICS Catalogue is for you!

The ICS Catalogue provides the interim pan government route to market. It is an effective and efficient route to market for **Information Assured (non High Grade Crypto) products and services** for the Ministry of Defence and Public Sector organisations via its IA Section of the Catalogue.

The ICS Catalogue is operated by the Defence Equipment & Support, Information Systems & Services, Commercial Services Team based at Minerva House in Swindon. The IA Section of the ICS Catalogue is the result of an initiative by the Ministry of Defence and supported collaboratively by the Office of Government Commerce (OGC), OGC Buying Solutions, the Central Sponsor for Information Assurance within the Cabinet Office and CESG (the National Technical Authority for Information Assurance) to ensure that a route to market exists for the protection of information that information systems handle.

Accessing this route to market is simple!

For MoD departments access is via the purchase to payment (P2P) which is an ORACLE 11i electronic procurement tool. Should you not have access then contact the EProc Team on **01225 815404/5497**.

For Public Sector departments you will need to register with the ICS Catalogue at www.dcsacat.mod.uk. Registration is easy! At the ICS Catalogue home page click on the New User tab and follow the registration process ensuring that you use an email address from which you will use to order. A password will be provided to you within 24 hours (Mon to Fri). Access to view and place online orders via the catalogue are then available through the Customer Service tab.

Why is IA Needed?

Information is fundamental to the business of government. Effective IA is core to ensuring that this asset is

safeguarded appropriately.

The continued growth throughout government in the use of ICT systems, all linked together, carries with it increased vulnerability. In addition these ICT systems are under threat of attack from foreign intelligence services, criminal gangs, and even individuals inside the organisation.

Protection against such threats and vulnerabilities is essential.

Across the Public Sector suitable precautions should be taken to safeguard its information. Therefore every ICT, or information related, system or service must contain Information Assurance (IA) requirements. Indeed IA extends beyond ICT contracts, since for example even in construction projects there is likely to be an ICT system used in designing, managing or communicating about the project, and this will have IA requirements.

Why this route to market is important!

The continued growth in the use of information systems, linked together in ever larger, faster and more complex

networks carries with it an increased vulnerability to attack against sensitive information. This threat ranges from foreign intelligence services to the criminal fraternity. Protection against such threats and vulnerabilities is essential. The products and services available, which have been technically assessed and certified by CESG, through the ICS Catalogue offers end users ready made assurance.

What are the benefits of using this route to market?

- Technically assessed products and services
- Public procurement compliant process
- ICS Catalogue free and easy to use
- Value for money solutions
- Procurement route which utilises best practice
- Dedicated technical and commercial teams that will support you the Customer
- Electronic ordering process
- Robust contract protection

IA Suppliers

The following four suppliers have been awarded contracts to cover the supply of all non high grade crypto IA products and services:

Centerprise

Contract no: CMHW/120991
Contact: Tony Atkin **01256 378008**

SCC

Contract no: CMHW/120993
Contact: Steve Greig **07976 014514**

Software Box

Contract no: CMHW/120992
Contact: Scott Cattaneo **01347 812100**

Trustmarque Solutions

Contract no: CMHW/121008
Contact: Rob Cornish **07909 366210**

For further information and advice:

Contact the Defence CIS Single Point of Contact (SPOC) on **0870 600 8910**, clearly stating "ICS Catalogue" when prompted, then follow the automated system instructions to be routed to

Customer Support.

The ICS Catalogue also provides MoD and the wider Public Sector with a competitive route to market for a broad range of IT/IS products and services.

Malcolm Rowland MCIPS
Defence Equipment & Support
ISS Commercial-Services
Development Team



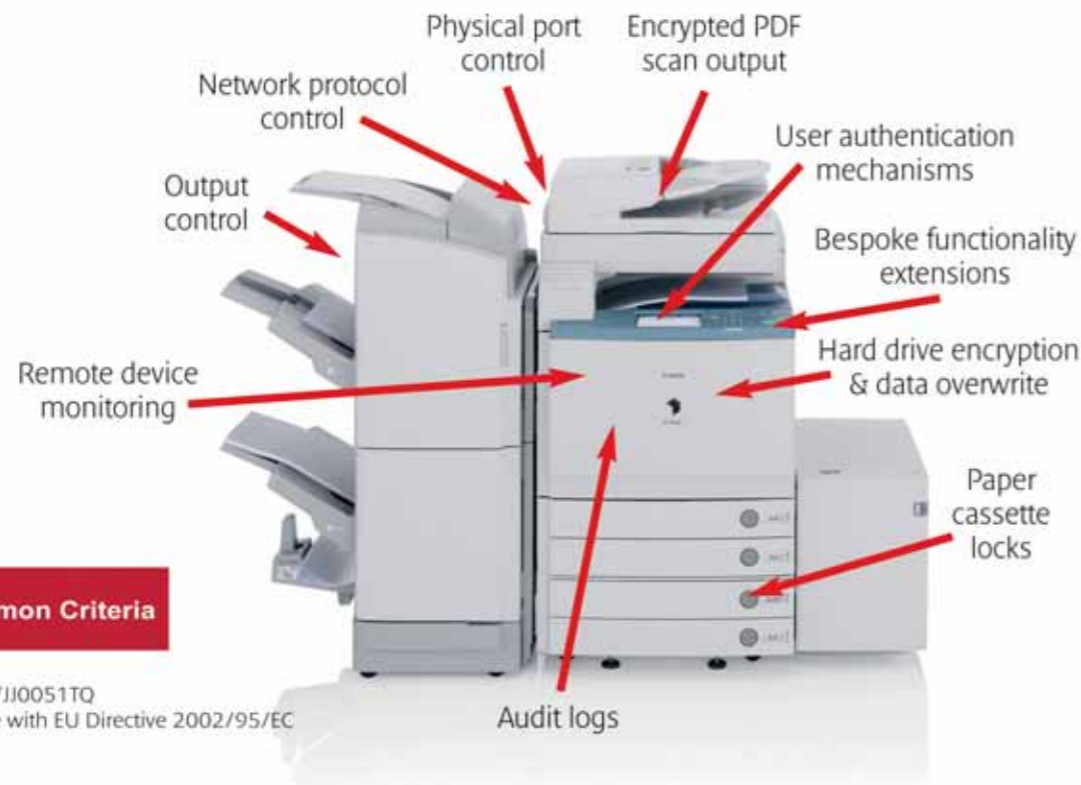
you can
Canon

Have you ever thought of what data is held on your Multi-Functional Device?



Have you left an area of your infrastructure insecure?

With a range of options designed to encrypt, overwrite, authenticate and manage your devices, Canon can work with you to provide a bespoke assurance solution to protect your valuable business information.



WEEE registration number WEE/JJ0051TQ
Canon is RoHS compliant in line with EU Directive 2002/95/EC

For further information please contact Jo Turner on 07967 674523 or jo_turner@cuk.canon.co.uk

SBL's ICS CATALOGUE CONTRACT LAUNCH EVENT



Thursday 17th July 2008
One Great George Street,
Westminster, London

Open to UK Public Sector
Organisations and MoD

The Information & Communications Services (ICS) Catalogue, operated by DE&S Information Systems & Services Commercial Services, provides a supply route for IT/IS for the Ministry of Defence and other UK Public Sector organisations.

SBL has been awarded one of the contracts which commenced on 1st May 2008 to supply the following on the ICS Catalogue:

- Information Assurance Products
- Hardware & Software

As Information Assurance specialists, SBL are an established supplier on the ICS Catalogue, and have the expertise and experience to guide you through this contract.

This event has been designed to provide MoD and UK Public Sector Organisations with:

- An overview of the ICS Catalogue – what is it? How does it work? What are the benefits over other government frameworks? Who can take advantage of the benefits?
- How your organisation can get assistance to purchase through the contract, and the value added services offered to help with your IT/IS requirements
- Presentations from key vendors, looking specifically at the topic of Information Assurance.

There will also be a mini exhibition of key vendors who can offer solutions through the ICS Catalogue and you will have the opportunity to visit their stands during the refreshment and lunch breaks.

Who should attend?

Anyone who is part of the decision making unit for the purchase of IS/IT solutions from within both the MoD and UK Public Sector organisations.

Places are limited, so please register your interest in attending by emailing sbl_secretariat@softbox.co.uk or phoning 01347 812176 and we will send you further details.

HOW SAFE IS YOUR SECURE DATA DISPOSAL?



Loss of sensitive data has generated embarrassing headlines for Government Departments and Commercial Organisations. It should be prompting you to check your data disposal service delivers all it promises.

As Chris Avis, Business Development Manager at Barron McCann Technology (www.bemac.com), observes, "The WEEE (Waste Electrical & Electronic Equipment) directive is a laudable environmental initiative, however it has created a market for companies that offer WEEE-compliant disposal, without effectively addressing the data security issues.

Does end of life mean end of data?

"Under WEEE, end of life IT equipment can be recycled or resold. Reselling raises all sorts of doubts about what happens next. The WEEE obligation simply moves on to the next party – with the risk that the equipment still has residual data which might be accessed and distributed."

The safest solution, Chris and other industry experts believe, is not reselling but recycling – right down to the base materials, combined with the data disposal and the assurance that the organisation responsible is accredited to the required standards.

All HMG protectively marked data, including Restricted, Confidential and higher, must be disposed of according to CESG, the National Technical Authority for Information Assurance, regulations. These set the standards for who can move and dispose of end of life IT equipment and data, how and where.

The complete CESG Claims Tested Mark (CCTM) approved managed service

Currently only one company has CESG Claims Tested Mark (CCTM) approval for a complete managed Secure Data Disposal service – and that is Barron McCann Technology. For the CCTM, Barron McCann Technology had to prove its effectiveness and compliance – ensuring, to borrow from a well-known TV commercial, their service does exactly what it says on the tin.

Uniquely, Barron McCann Technology offers secure on- or off-site disposal of protectively marked or sensitive IT equipment up to and including Top Secret. The on-site service is particularly welcomed by Barron McCann's Central Government, Law Enforcement and Military Department customers. They often find it too time-consuming to transfer their IT equipment to subcontractors for disposal. More critically, the sensitivity of stored data makes taking it out of a secure building and transporting it to the disposal site, an unacceptable risk.

Making sure of Information Assurance

In these cases, Barron McCann Technology sends in two trained Data Destruction Engineers, with SC level clearance to handle Government data at all levels up to Top Secret. They use CESG Higher Level approved degaussing equipment to erase all data from the IT equipment, which is then sent for recycling to its base material in compliance with the WEEE directive.

Constantly monitored

For the off-site service, the IT equipment is carried in security sealed cages, in a GPS-tracked vehicle accompanied by uniformed SC cleared staff. Vehicle and staff are checked both when leaving the site and arriving at the List X data disposal facility; a constantly monitored, controlled access secure environment. So the IT equipment is fully accounted for, from collection to destruction.

Total destruction with 90% recycling

Barron McCann Technology believes total destruction is the only safe option, so all IT material is broken down to its base material. Metal is smelted, plastic is chipped and PCBs are stripped of copper and solder. It's not only more secure, but better for the environment – the WEEE directive calls for a 65% reduction in landfill for IT equipment, but Barron McCann Technology aims for 90% recycled.

Audit trail

Vitality, Barron McCann Technology provides a complete audit trail for every stage of the operation and certifies its work. For example, every disk is scanned before the data is erased, with a real-time audit including time, date, serial number and operator details. So you can prove your IT equipment has been disposed of securely – vital assurance for Department Heads.

Barron McCann Technology has one of the data disposal industry's most impressive lists of accreditations, including full compliance to CESG Manual S and HMG IS5, the Data Protection Act and the WEEE Directive.

Setting the standards

Now the company is taking the lead in helping to set the industry standards for information assurance. Chris Avis points out, "although Barron McCann Technology regularly carries out HMG work up to Top Secret level, we currently have CCTM for up to HMG Restricted. That's simply because there's no current system for testing to Top Secret.

"We are working with CESG to establish rigorous, dependable benchmarks for testing and approving a service for up to Confidential, Secret and Top Secret levels of Protective Markings. As we have recently seen in the newspapers and on TV, no aspect of protecting sensitive data can be left to chance."

For more information on Barron McCann Technology's accredited Secure Data Disposal Service please contact SBL on **01347 812100** or you can email enquiries@softbox.co.uk



DELIVERING CONFIDENCE IN INFORMATION SECURITY

The CESG Claims Tested Mark (CCTM) - a mark for assurance, a mark for confidence, a mark for quality, a mark to trust.

Expanded team working to extend CCTM scheme

Since April this year, CESG, the Information Assurance arm of GCHQ, has owned and operated the CCTM scheme. This follows a successful pilot with CSIA Cabinet Office. CCTM fits well within the CESG portfolio of consulting and accreditation services. CCTM Secretariat Programme Director Peter Hayes comments "The CCTM scheme is going to be widely popular because of the simplicity and speed it offers and, because of the importance of data handling, it has to be!" Within weeks of the transition, the first award under CESG was announced, underlining that the simplicity and pace, designed in by CSIA, was working well. Throughout 2008 and beyond, the CCTM scheme is being more widely promoted and introduced to customers and vendors alike.

Data handling assurance high on the agenda

One of the items sitting near the top of the in-tray for policy makers in the wider public sector is data handling and information assurance. It competes for time and attention with other high level concerns, where outcomes need to be progressed and risk needs to be mitigated. For the CCTM team this means making a case for information assurance being seen as relevant as other corporate social responsibilities, particularly those where the policy makers are themselves accountable.

Government is transforming the way it delivers services to provide online public services to citizens and business when and how they want. These services will be delivered through ICT systems, and the Transformational Government programme recognises that "underpinning IT systems must be secure and convenient for those intended to use them".

Most public sector organisations use off the shelf information security products and commercial services. How can they be sure that these products and services will meet their security requirements and will do what they claim to?

Providing the public sector with an independent validation of claims made by Vendors of Information Assurance (IA) products and services gives assurance to both the organisation and ultimately to the citizen.

The CCTM scheme provides a government quality mark for the Public and Private sectors based on accredited independent testing, designed to prove the validity of security functionality claims made by Vendors. In more colloquial terms, the CCTM scheme is designed to assure public bodies that a product or service "does what it says on the box". Additionally, the CCTM scheme provides compliance testing against technical standards for degaussing (data erasure) set by CESG in its role as the UK National Technical Authority for IA. It is aimed primarily at products and services to meet IA requirements at Government Impact Levels 1 & 2, for purchase by Central Government and the Wider Public Sector, particularly the NHS, Education, Local Authorities, Police and Criminal Justice. The CCTM scheme satisfies the minimum assurance requirement for use in systems supporting the Transformational Government agenda.

The CCTM scheme will also help organisations meet their corporate governance obligations, for example, the Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley), the International Capital Framework (Basel II) and compliance with the Information Security Management standard (ISO/IEC 27001).

The benefits of the CCTM are:

- Clear and trustworthy information: details of claims and test results are published.
- Independent testing: testing is performed by independent Test Laboratories accredited against ISO/IEC 17025.
- Rapid and cost-effective: the whole process takes less than 12 weeks with testing typically taking about 1 month. This means that CCTM can fit within many IT procurement timescales, or can be part of a Vendor's commitment when bidding.

There are currently seven accredited test laboratories – BT, EDS, ENEX, Logica, SiVenture, Vizuri and West Coast Labs – all of these handle general testing while SiVenture specialises in hardware, smart cards and data erasure and West Coast Labs in anti-malware technology.

Since launch, more than 30 products and services have been awarded the CCTM certificate with the rate of applications increasing steadily. Public sector customers are increasingly specifying their IT security requirements in terms of the CESG Claims Tested Mark, and the costs and timescales involved mean that product and service vendors can respond quickly to meet these requirements.

Visit CCTM Secretariat online at www.cctmark.gov.uk, email us at Secretariat@cctmark.gov.uk or call for further information **020 7240 7220**



SYMANTEC ANNOUNCES LAUNCH OF ENDPOINT ENCRYPTION 6.0

ADVANCED ENCRYPTION SOLUTION FOR DESKTOPS, LAPTOPS, AND REMOVABLE STORAGE DEVICES

Data protection is a critical issue in many organisations today as an increasing amount of valuable information travels across various environments and is stored on an ever-growing list of endpoint devices, including PCs, laptops, and removable storage devices such as hard disks and USB memory sticks.

Symantec Endpoint Encryption 6.0 offers a scalable, enterprise-wide security solution that delivers comprehensive protection and prevents unauthorised access to these endpoints with strong encryption and access control technologies. Specifically, Symantec Endpoint Encryption 6.0 – Removable Storage Edition enables businesses of all sizes to maximise the productivity benefits of using removable storage devices while minimising the risks these devices pose to data security. Symantec Endpoint Encryption 6.0 – Removable Storage Edition is designed to protect all data on USB, FireWire, Compact Flash, iPod, and other storage devices and media.

Symantec Endpoint Encryption 6.0 – Full Disk Edition is a full disk encryption solution designed to protect all data on the hard drive of a Microsoft® Windows® – based machine. It allows administrators to encrypt the laptop's hard drive to ensure safe harbour and, more importantly, to prevent the exposure of sensitive data should a laptop be lost or stolen. With the Symantec advanced encryption solution, encryption is transparent to the end user and performed with minimal performance impact. As a result, proper endpoint security measures are taken on each of these corporate endpoints to help mitigate the increasing risk of potential data loss.

For more information on Symantec Endpoint Encryption, or other Symantec solutions, please contact SBL on **01347 812100** or email enquiries@softbox.co.uk



TRAINING COURSE SCHEDULE JUL-SEP 08



SBL specialise in security training which is delivered by CLAS & CISSP accredited consultants in our state of the art demonstration and training facility in York, sponsored by HP. SBL also offer training at your site, and our skilled consultants will design and deliver tailored courses to suit the needs of your organisation.



*SBL is THE ONLY authorised training facility for the Pointsec Product Range from Check Point.

Course	Dates	Duration	Price
Securing your Information	29th July & 16th Sept 2008	1 Day	£400.00
Reflex DataVault	1st July & 4th Sept 2008	1 Day	£600.00
Pointsec Protector (Reflex Disknet Pro) 4.8 Administration	2nd July, 20th Aug & 1st Sept 2008	1 Day	£600.00
Pointsec* for PC Certified Engineer	3rd July, 21st Aug & 2nd Sept 2008	2 Days	£750.00
Secure WiFi in a day	7th July, 25th Aug & 8th Sept 2008	1 Day	£400.00
Wireless Network Administrator	8th July, 26th Aug & 9th Sept 2008	3 Days	£900.00
BeCrypt Disk Protect Baseline & Enhanced	16th July, 19th Aug & 18th Sept 2008	1/2 Day	£300.00
Stonewood FlagStone Administration	16th July, 19th Aug & 18th Sept 2008	1/2 Day	£300.00
Microsoft Licensing with Virtual Machines	22nd July, 5th Aug & 24th Sept 2008	1 Day	£300.00
Microsoft Office SharePoint Server 2007 Basic User	24th July, 12th Aug & 25th Sept 2008	1 Day	£400.00
Crypto Custodian Refresher	17th July & 23rd Sept 2008	1 Day	£600.00
CAPS Product Overview	15th July, 18th Aug & 17th Sept 2008	1 Day	£350.00

SBL Security Training and Consultancy

SBL are a market leader in IT security solutions with over 18 years experience operating in Criminal Justice, Central and Local Government, Utilities, NHS and Corporate market spaces. We also have a strong relationship with the MOD, and are their preferred supplier for security products and services.

We are renowned for delivering best of breed IT Security products from anti-virus, filtering, network security, removable media management, back-up storage to secure remote access. SBL's Security Services Team possess

the qualifications, skills and experience to enable them to design, develop and implement 'custom built solutions' targeted to your company's individual needs, paving the way for a wide variety of future needs. Our experience in I.T. Security allows us to deliver unsurpassed expertise and business solutions.

Our range of services include; product evaluations, installation, training and security consultancy.

Course	Overview
Microsoft Licensing with Virtual Machines	This course provides an overview of the updates to Microsoft's licensing models for the server operating system and server applications. It will also clarify existing licensing policies to help you to deploy and use software under the MS updated virtualisation models. This course will help you to understand how to efficiently deploy MS server products with virtual machine technologies.

Microsoft Licensing

SBL are pleased to offer a new training course on our training schedule. This has been created to address the demand for non-product specific training in the area of Microsoft Licensing.

SBL also offer training at your site which will focus on your specific business and system requirements. These courses can be arranged at a

time convenient to you and can be tailored to an individual's needs. This is a cost effective solution which saves on travelling time. Please contact SBL for a competitive quotation.

For more information, contact your Account Manager at SBL on **01347 812100** or you can email us direct at enquiries@softbox.co.uk

THE SECURE VIRTUAL COMPUTER ON YOUR KEYCHAIN



Tom Rowan, Principal Security Consultant at Magirus in the UK

When touting the benefits of virtualisation, most IT administrators talk about big improvements in server utilisation or reducing their server footprint and energy savings. Seldom do they raise the benefit of security for mobile workers – until now that is.

Magirus, the IT solutions provider has harnessed the power of virtualisation to provide a secure alternative to the laptop computer – the virtual computer on your keychain.

Better known for its consultative distribution surrounding storage and virtualisation products, Magirus has built a thriving security practice. At Infosecurity Europe 2008, in London, it took the wraps off a new packaged solution that was described by Jiri's Notepad blog as "one of the most innovative uses of virtualisation" for its ability to transform secure mobile computing.

Essentially the device is a secure encrypted virtual computer on a USB memory stick. It comprises a software package that is pre-configured like any desktop 'build,' with a full Windows operating system, applications (including VPN) and player software operating within VMware's Assured Computing Environment (ACE) – all deployed on a standard 4GB USB memory stick. Plugged into a computer

it may run as a fully protected stand-alone system or as a securely networked system.

Such devices may well help resolve the conundrum of business leaders demanding increased flexibility for their mobile workforce and security officers anxious to protect data confidentiality and the integrity of their network.

"It allows employees or contractors to work securely using whatever computer they choose to plug into," explained Tom Rowan, Principal Security Consultant at Magirus, "and given that a 4GB memory stick costs as little as £18, it makes such a machine on average 30 to 50 times cheaper than a laptop."

Most modern business laptops are sieve-like and come loaded with an array of connectivity and data transfer options (Bluetooth, USB, WiFi, Ethernet, Firewire, DVD writer, etc.); conduits for data leakage, malware and virus attack.

The VMware ACE package has security built-in. Its encrypted virtual disk is difficult to attack without first knowing the decryption password. Having a firewall built in at the virtual hardware layer also makes it hard to hack. Furthermore, it is highly configurable. The firewall can be configured to allow the employee to access only corporate resources.

Importantly, USB and removable media can be denied from accessing the machine too – by removing the virtual hardware which supports the USB. This simply cannot be done on an ad-hoc basis with physical hardware.

The VMware ACE includes "virtual rights management," which allows stolen or lost USB sticks to be retired or killed remotely. The administrator determines when it becomes active and when it expires, controlling this via a management server. This makes the ACE device ideal for use with contractors as it eliminates the headache of collecting a laptop at the end of a contract.

"It won't replace the laptop, but does provide options," said Rowan, "for example IT managers may think twice about the number of laptops they issue."

As organisations consider virtualising their server environments, this secure option may just be one more compelling reason to make the move.

For more information on the VMware ACE package, please contact SBL on **01347 812100**, or email us at enquiries@softbox.co.uk



PURCHASING THROUGH THE ICS CATALOGUE

The Information & Communications Services (ICS) Catalogue, operated by DE&S Information Systems & Services Commercial Services, provides a supply route for ICT for the Ministry of Defence and other UK Public Sector organisations.

SBL has been awarded contracts which commenced on 1st May 2008 to supply the following on the ICS Catalogue:

- Information Assurance Products
- Hardware & Software

As Information Assurance specialists, SBL are an established supplier on the ICS Catalogue, and have the expertise and experience to guide you through this contract.

Who can purchase under this framework?

- MoD Organisations
- All UK Public Sector Organisations

Why use the ICS Catalogue?

- Tightly controlled framework
- Only specialist security framework - *Approved by DE&S, OGC, CESG and Cabinet Office*
- Simplifies Procurement Process
- Supported by Information Assurance (IA) thought leaders
- Employee benefits through home use programs
- Value for money through regular supplier benchmarking

Why you should put your trust in SBL:

- 21 years expertise in IT Solutions
- 16 years supplying through ICS Catalogue
- Information Assurance Specialists & Market Leaders
 - *Products & Professional Services for your IA strategy*
 - *Encrypted Laptop Bundles*
- Desktop and Notebook Advice,

- Supply & Compatibility Testing
- Software Licensing Experts
- Impartial advice & assistance with sourcing, evaluating & implementing your IT solution
- Commitment to achieving best value for customers:
 - *Various exclusive enterprise wide contracts negotiated*

- SBL play a key role in supporting Government
- Trusted advisor (100% CESG scoring)
- Free of Charge 1st line telephone support on all sales
- Calendar of FOC seminars, workshops & technology roadmaps
 - *www.softbox.co.uk/events for current listings.*

Experience Counts; Expertise Shows

"SBL's expertise and knowledge base on general and especially on security-based products has been of great assistance to us in the past. Their vendor independence means we can rely on them."

Steve Alexander, SO1 ICS Procurement
D CBM, HQ Land Forces

"SBL can be counted on to offer a first class service which allows me to focus on other aspects of my job..."

"The service provided by SBL to the DII(F) Commercial team and our Contracted partner Atlas EDS has been exemplary."

Harry Dale, Commercial Officer
DES DII Commercial Team

"I have always found them (SBL) to be a very professional organisation and in comparison to other suppliers on the ICS catalogue their customer service is second to none."

Marcus Graham, DE&S ISS (DISD C&IS West)
Asset Management

The SBL Team

For more information contact SBL on **01347 812100**. Alternatively email us using the relevant email address below:

MOD Sales Team

Tel: 01347 812100
Email: modsales@softbox.co.uk

NHS Team

Tel: 01347 812100
Email: nhs@softbox.co.uk

Local Government Team

Tel: 01347 812100
Email: localgovernmentteam@softbox.co.uk

IT Partner Team

Tel: 01347 812100
Email: itp@softbox.co.uk

Central Government Team

Tel: 01347 812100
Email: CentGov@softbox.co.uk

Professional Services Team

Tel: 01347 812100
Email: ITServices@softbox.co.uk

SBL's ICS Catalogue Contract Launch Event - 17th July, One Great George Street, London.

SBL is hosting an ICS Catalogue Contract Launch Event on 17th July in London. See page 7 for more details or register your interest in attending this event by emailing us at sbl_secretariat@softbox.co.uk



Experience Counts; Expertise Shows

Experience + Expertise = Excellence

Expertise in Information Assurance Professional Services



SBL are a market leader in the area of Information Assurance. Operating in both the public and private sectors since 1987, we are a preferred supplier for products and services for many organisations.

Our CLAS and CISSP security accredited consultants have an in-depth knowledge of the ISO27001 and BS2277 standards, and their implementation. As vendor independent consultants we offer impartial and unrestricted advice on the solutions which will be the "best-fit" for your requirements.

SBL offers the following Information Assurance consultancy services:

- **Security Policy Development**
The most basic indicator of an organisation's commitment to IA, promoting a positive security awareness to customers, employees & shareholders.
- **Security Strategy**
Defining a comprehensive security strategy tailored to your business needs.
- **Security Risk Assessment**
Identifying threats & vulnerabilities

to your systems.

- **Network Security Assessment**
Comprehensive analysis of your network to determine current position regarding IA.
- **Secure Network Design**
Building powerful & flexible safe guards in to your existing network.
- **Secure Mobile Working**
Advice on the protection of your mobile data, either at rest or in transit.
- **Disaster Recovery/Business Continuity**
Review/creation of procedures for the reinstatement of your IT & business systems following an unplanned event.
- **ISO27001 pre-Audit Consultancy**
Assistance for organisations that wish to design & implement an information security management system in compliance with ISO27001.
- **Crypto Custodian Consultancy**
Introduces a custodian to the practicalities of handling & managing bulk cryptographic and accountable material.
- **Accreditation Document Set**
Involves the production of the standard documents required for the accreditation of your security system.

Training Courses

SBL also specialise in security training which can be delivered in our state of the art demonstration and training facility in York, or alternatively on a customer site. SBL consultants design and deliver courses to suit the needs of your organisation.

More details on courses available can be found on the training schedule on page 12.

For more information on IA Services available from SBL, please contact us on **01347 812100** or you can email us at itservices@softbox.co.uk



THE ICM – COLLABORATION IN ACTION

What is the Intelligent Customer Mechanism (ICM)?



The ICM is a collaborative way of working which enables Government to manage its information in an assured way.

The ICM is at the heart of the work of the Information Assurance Technical Programme (IATP), which is a pan-government programme, directed by the Central Sponsor for Information Assurance (CSIA) in the Cabinet Office and delivered through CESG, the National Technical Authority (NTA) for Information Assurance, in partnership with Industry.

Why is the ICM needed?

Government needs a joined-up way of acquiring trusted IA capability. Traditionally the development of assured ICT solutions has been slow and, in the modern age, is not reactive enough. Industry has limited information on government's ICT/IA needs and is therefore unable to make sound investment decisions.

The ICM is a joined-up approach, which aims to remove traditional stovepipes and artificial boundaries, allowing government to speak with one voice. It also empowers Industry to respond to real government need within realistic timescales and allows development of profitable solutions which will help sustain the UK Industry base.

UK government needs to maintain a sovereign IA industry sector and the ICM will help to achieve a vibrant IA

market place to help ensure its survival.

How is the ICM encouraging this more collaborative approach?

- By capturing ICT/IA needs from government departments and identifying 'common good' (capability of use, of value or of benefit to more than one government department) needs
- By engaging with Industry to determine what ICT/IA products/ services are being produced/ developed and then carefully analysing the information to highlight any gaps which need to be filled, identifying potential market opportunities and supporting Industry in their solution development
- Through a "lead department" (the government department responsible for driving a procurement or acquisition opportunity through its lifecycle on behalf of a collaborative group) approach, the ICM is brokering the collaboration on a capability theme so that user requirements are gathered and made known to Industry to allow industry innovation to develop the "right" solution
- As development of capability reaches maturity, the ICM re-examines the 'common good' need for these products and services and brokers collaborative trials. The ICM has been overseeing these trials and sharing best practice
- Developing the new Information

Communication Services catalogue in collaboration with MoD, the Office of Government Commerce and others to include Government (NTA) assured IA products and services (launched at the beginning of May '08). This catalogue provides a competitive route to market for a wide range of IT/IS products and services and is available for use by the public sector.

The ICM is already showing that a collaborative approach is the way forward but there is more to do.

Phil Hill
Information Assurance Technical Programme Manager and ICM Delivery Lead, CSIA

If you would like to find out more about the ICM and what it can do for you and how you can play a part in this collaborative approach please email iatp@cabinet-office.gsi.gov.uk

IATP *Building IA Capability*



SBL's MOBILE DEVICE ENCRYPTION SERVICE

As the use of mobile technology increases, so does the risk to your business when your company's critical data is left defenceless against theft or unauthorised access.

Breaches to your security can result in significant financial loss to the company, and managers responsible at the time may be personally liable for infringements of data protection laws.

To make securing your laptops and mobile devices as simple as possible, SBL has created a complete laptop and mobile device encryption service, which ensures that the data on your laptop can only be read by authorised users. This service includes sourcing the hardware and the encryption products, installing them on your laptop, and retrofitting your applications.

To protect the integrity and

confidentiality of your data, the encryption solutions can be installed on your laptop at our high security, List-X facility in York. Alternatively we can install and verify the encryption solution at your own site.

Encryption solutions may involve replacing your laptop's hard drive with a new encrypting drive, or deploying software which encrypts your existing drive.

SBL offers four distinct device encryption options:

Device Encryption Option 1

We will replace the hard drive in a new laptop with an encrypting hard drive.

Device Encryption Option 2

We will replace the hard drive in your existing laptop with an encrypting hard drive, and retrofit your data and applications on to the new drive.

Device Encryption Option 3

This is the same as Option 2, but once we have installed the encrypted disk and retrofitted your data, we will perform an anti virus health check.

Device Encryption Option 4

Where you have chosen a software solution for your hard drive encryption, we will install the appropriate product on your laptop and verify its operation with existing applications.

Installing optional security products

While we are installing the encrypting hardware and software, we can also install a range of security applications to address access control, peripheral device management and operating system upgrade issues.

For more information, contact your Account Manager at SBL on **01347 812100** or you can email us direct at enquiries@softbox.co.uk

Case study: Delivering Laptop Device Encryption Solutions to the MOD

An IT procurement manager at the Ministry of Defence, George Yeomans, recently acquired a number of encrypted laptops as part of a long established business relationship with the York office of national specialist software supplier SBL.

George Yeomans, who manages the computer hardware and software procurement needs of thousands of MoD civilians and service staff throughout the West Midlands, Wales and the South West, including those off-site, selected SBL because of its multi-disciplined 'total solutions' capability for complex assignments.

He says: "Securely encrypted laptops are vital because, for key personnel, they are used to store highly-sensitive and often classified data which could compromise national security if it were to fall into the wrong hands. It is vital that this data can be accessed only by

authorised users."

As an organisation with significant purchasing power and in-house expertise, the MOD IT procurement department was able to identify, acquire and encrypt the necessary hardware and software for the assignment itself but chose to sub-contract to SBL for operational efficiency.

"Speed and efficiency are essential to our operation as one would expect from a military support body" says George Yeomans. "We know what the threats are and, while we could have carried out this complex project ourselves, it would have involved researching and acquiring the various items of software and specialist hardware separately and marrying them all together before carrying out the encryption.

"This would have been cumbersome, time-consuming and there is a chance

that, in a busy work schedule, it may not have received the priority it warranted or that, in spite of knowing exactly what we wanted to achieve, we may have got it wrong in some way.

"SBL was very good, very professional and fast. If the opportunity arises, I would not hesitate to use them again."

"The fact that we were working with a trusted supplier meant that we could obtain the necessary clearance and then hand the entire project over to them to deliver a total solution. This saved us time and trouble and also gave us the absolute confidence that it had been completed to a high-professional standard. SBL was very good, very professional and fast. If the opportunity arises, I would not hesitate to use them again."

TOSHIBA

FlagStone

Are there holes in your mobile data security?

There are no holes in our data encryption

As the level of data we hold increases, security is becoming a bigger concern for most organisations. With the high-profile stories in the press about notebooks containing sensitive data being left in taxis – what can you do to protect your organisation from the loss or theft of your data?

Working in partnership with Stonewood*, the company who produce the FlagStone product, Toshiba can make sure that your organisation's sensitive information remains secure, whether it is on a notebook or tablet.

FlagStone Technology – your foundation for security

Trusted globally by Governments, and chosen by the world's foremost financial, banking, law and medical corporations, FlagStone Technology integrates sophisticated authentication, entire disk encryption and data storage into tamper-resistant hardware that safeguards your data, without any adverse effects on your computer's performance.



SBL can supply fully encrypted Toshiba notebooks, using the FlagStone technology. To find out more about how Toshiba EasyGuard and FlagStone work together to create the ultimate data protection solution for your organisation, call SBL on **01347 812100** or email enquiries@softbox.co.uk

SBL