

# CESG AGENDA

JULY 07



NATIONAL TECHNICAL AUTHORITY  
FOR INFORMATION ASSURANCE

## INSIDE THIS ISSUE



**Silent  
revolution**  
– BRAVE NEW  
IA WORLD

PAGE 02



**Industry  
finds a voice**  
– IA COLLABORATION  
GROUP

PAGE 03



**Industry  
Forum 07**  
– CESG New  
Assurance Model

PAGE 04



**Government  
given access  
to VISTA**

PAGE 07



**National  
IA Strategy**  
– IA07 PROVIDES  
A LAUNCH PAD

PAGE 08

# SETTING THE AGENDA



**W**elcome to Agenda, an informative newsletter that we have launched to improve communications between CESG, Government and Industry, at a crucial time for Information Assurance.

This issue covers the CESG Industry Forum, which attracted a capacity audience from the commercial ICT sector, with strong representation from UK and International companies.

Focusing on the CESG new Assurance Model, the Forum reflected a serious commitment by Industry to work with CESG in finding creative, practical ways in ensuring that Information Assurance becomes an enabler to the business of Government.

We also look forward to the crucial IA07 event which will feature the launch of the National IA Strategy. I hope that you find this publication helpful and informative.



JOHN WIDDOWSON  
DIRECTOR, CESG

## SILENT REVOLUTION

**T**HE sheer scale of the Government's Information Assurance challenge requires 'a huge mindset change by all sides – Government, Industry and the National Technical Authority', believes Sir David Pepper, Director, GCHQ.



Sir David Pepper, Director, GCHQ at the Forum

"Against a backdrop of accelerating change in the IT Industry itself, Information Assurance must play a critical role in delivering the Transformational Government and Shared Services agenda," he believes.

"As the momentum of this agenda gains pace, departmental and corporate boards must take Information Assurance risk management very seriously – people must understand the threats that they face."

CESG, as the National Technical Authority, must also rise to the challenge: "Acknowledging the need for some quite radical changes in the way in which we interact with Industry," said Sir David.

"We must be much more intelligent and imaginative in recognising that Industry has much more to offer, which we have not tapped into. Industry offers the answer to many of the capacity problems that we face."

The need to involve Industry in all kinds of ways is critical, he said: "Because we will always be constrained in terms of skills and resources."

A priority for CESG is:

**"To develop new and informal ways of working with Industry – I don't think that it would be unfair to call this a quiet revolution,"** he said.

Important progress is being achieved.

At the Industry Forum in March, CESG and Industry worked hard together to review the CESG new Assurance Model, ensuring that this is robust and effective in operation – effectively targeting resources at the greatest risks.

At the end of June, CESG will bring together representatives of Industry and Government at IA07, for the launch of the National IA Strategy. This will be a vital platform for reviewing and refining tactics and approaches that will allow this much needed strategy to be implemented quickly and efficiently.

Critical to the success of the new Strategy will be the crucial role of the CIO and CTO Councils in its implementation believes Sir David: "A key objective for the centre will be to call for much greater use of the expertise of CIO and CTO Councils to enable implementation of the strategy alongside implementation of the Transformational Government agenda."

All sides must rise to the challenge. It is vital that IA becomes part of the ICT mainstream. To achieve this: "We have got to get Departmental Boards engaged and supportive," he said.

"There's a big mindset change needed to get boards to realise that IA is fundamental to what they need to do at the start of a project," said Sir David. "If it is ignored, it will be a blocker," he said. "But it's not us blocking them – it's the issues that they haven't thought about."



# INDUSTRY FINDS A VOICE

**A** PRODUCT of IA06, the Information Assurance Collaboration Group (IACG) provides a robust, representative voice for the Information Assurance Industry. We heard from the Group's chairman, Colin Williams, outlining its aims and objectives and the progress achieved in the first 12 months.

"It was Craig Pollard at CESG who called together the key business representatives to form an Industry group – a body of willing collaborators, a coalition of the willing," explains Colin Williams.

The group has a number of very specific, targeted and measured goals. "Essentially, it is an Industry group that exists to serve the interests of the Industry and to promote the development of the market. The market in this case is a very inclusive definition. It includes not just both sides, but all sides of the piece."

The core aim is to help CESG operate as the National Technical Authority for Information Assurance. "The view of the IACG is that it is imperative that we have a strong, properly constituted National Technical Authority, which in turn contributes to development of strong, intelligent customers," said Colin.

The IACG is committed to delivering two key items in the short term. The first is a report, which will contribute to the on-going process of re-defining product certification and evaluation. "We chose this because it is central to the development of the market," explains Colin.

"Our intention in producing this report is to present the encapsulated wisdom of Industry – that is how we think product certification and evaluation should move forward."

The second task is to respond to the National IA Strategy on behalf of Industry, identifying how the private sector can help implement the strategy. Colin explained that this will be a 'hands off critique', but an attempt: "To come to an understanding of what Industry can do in response."

Once these initial tasks are accomplished, then the IACG will move forward with the other items on its extensive programme of work. The IACG is delivering one of the keynote addresses at IA07. A platform that the Group will use to present its report on Certification and Evaluation and its report on the IA Strategy and the Delivery Plan.

Colin Williams emphasised the urgent need for change: "We are attempting to solve the problems of the information age with ways of thinking and doing that are 50 – 60 years old. The world that those ways of thinking and doing was relevant for has gone forever and it's not coming back.



"We, therefore, have to change the way that we think and change, crucially, the way that we behave."

Colin highlighted the critical role that IA must play in realising the real potential of Government networks: "Government is saturated with IT on which it has spent phenomenal amounts of money. This is woefully underutilised and one of the key reasons is the absence of an adequate Information Assurance stance. It is central to the health and well-being of the UK as a whole that these IT systems realise their full potential."

In a final thought Colin paid tribute to the leadership shown by CESG: "They demonstrated leadership at IA06. They have reinforced that consistently in the intervening months. Now the focus is very much back on Industry. So to those of you who have said we would love to change the world but CESG won't let us – this is no longer true. The spotlight is very firmly on us – we have now to respond to their leadership position."

## ACTIVE LEADERSHIP

**L** eading the drive to a new threat-based approach to Information Assurance, CESG is fundamentally changing the way that it operates. Here Mike St John Green, Deputy Director, Operations, CESG outlines important progress that is being achieved.

Concluding IA06, the chairman, Sir Edmund Burton, challenged delegates: "So what are you as individuals going to do about it? What must we now collectively be doing differently? It is up to us as the enlightened community to give an active lead."

Much progress has been achieved since IA06 in delivering the 'quiet revolution' referred to by Sir David Pepper. The launch of the new IACG has significantly strengthened our dialogue with Industry, which together with our work with the CDF, creates a powerful

forum to achieve a common understanding with Industry. Together we must rise to meet the Government IA challenge – this must involve Industry acting as a force multiplier with CESG in delivering the new assurance services that will meet our customers' needs.

This dialogue has achieved powerful consensus in the introduction of the CESG new Assurance Model, which has received a positive reception from Government and Industry and is now undergoing an important pilot with BT's Next Generation Network.

Risk owners and business decision makers must determine the balance between IA risks and the business benefits arising from using ICT in their particular business context. By moving away from reliance on the evaluation of products to gaining assurance from a wider range of sources, the CESG new Assurance Model provides rich information that helps inform decisions.

Board members must increasingly demand greater knowledge of the threat they face so that they can get their risk-based decisions right. To meet this requirement, it is essential that CESG provides information that is clear, accessible and supports decision taking.

The essential role for CESG is to issue Good Practice for IA to Government. In delivering this task, it is essential that we continue to engage with our customers in ensuring that our advice is relevant and meets requirements. We must consider carefully the current set of documents that we produce and consider whether these still best meet requirements.

At its heart, these activities will provide rich risk information, richer than our customers are accustomed to seeing today. This change points to the need to move away from the simpler, rule-based risk decisions by our customers, in order that they gain the maximum benefit from the large ICT investment.

## CESG Industry Forum 2007

# CESG NEW ASSURANCE MODEL

The Industry Forum attracted a capacity audience, reflecting a serious commitment by Industry to engage with CESG in tackling the change agenda, finding effective, pragmatic solutions.

Concluding IA06, the chairman, Sir Edmund Burton, challenged delegates: **“So what are you as individuals going to do about it? What must we now collectively be doing differently? It is up to us as the enlightened community to give an active lead.”**

The Forum reflected how CESG and Industry have risen to Sir Edmund’s challenge, working together to deliver what Sir David Pepper, Director GCHQ described at the event as **‘a quiet revolution.’**



The 2007 Industry Forum focused on the **CESG new Assurance Model**, with structured sessions examining and providing feedback on its four key elements – Intrinsic; Extrinsic; Implementation and Operational Assurance.

Feedback captured at this event will be used to inform IA07, the Government’s Information Assurance event.

## INTRINSIC

Dave Teague at the Forum



**Definition: Building assurance in at the design and development stage; raising the assurance level of emerging COTS (commercial off the shelf) products; standards, guidance, advice, collaboration; determination of the extent of extrinsic activities required based on the level of confidence in the developer.**

Setting the scene for discussion over how best to achieve Intrinsic Assurance, Dave Teague identified the need for the relationship between CESG and developers to evolve significantly, identifying key factors that can build trust.

“What sort of trust can we have with developers?” Dave asked. “Being based in the UK or in ‘friendly’ countries is an advantage. Their taking a systematic approach and having a development methodology can build trust.”

They might have considerable competence and experience that CESG has witnessed over the years – a track record. “But, a track record is quite a hard thing to define legally,” he said.

**“So the issue is, how do we enforce good practice? How can we test them legally? How do we defend what we do?”**

One issue identified was concern that a lot of componentry comes from overseas: and is not manufactured by ‘friendly’ countries: “Quite honestly, we have some worries about what is inside,” said Dave.

The need for developers to act with integrity and take a responsible approach was emphasised: “If someone gives a developer advice do they learn from it? Will they do things the same again next time or do they learn and do things better?”

The development environment is another key factor. “Do they have tools and libraries?” asked Dave. “Is there a system engineering principle behind it all or is there a ‘let’s try and see what we can get away with’ approach?”

The opportunity for CESG to participate in the development of projects and systems is another important factor. Dave identified a number of ways in which this collaboration might occur – ranging from embedding staff into developer organisations to providing consultancy.

In summary, Dave believes: **“We are entering a realm of using Industry to a far greater extent. We’ll be outsourcing those things we can. Intrinsic Assurance is intrinsically about baking in assurance. Not assurance bolted on at the end, because that tends not to work very well.”**

## CESG NEW ASSURANCE MODEL

### INTRINSIC

- Design & build in information security
- Standards & guidance
- Confidence in developers

### EXTRINSIC

- Targeted evaluations
- Residual risks

### IMPLEMENTATION

- Build a trusted system
- Design security into architecture

### OPERATIONAL

- Through-life assurance
- Network monitoring & intrusion detection
- Config management
- Patching & updates
- User awareness

## EXTRINSIC

Nigel Jones at the Forum



**Definition: Targeted search for vulnerabilities in a product; iterative feedback to the intrinsic stage to improve current and future products; determination of residual risks that must be mitigated/managed.**

Nigel Jones focused on the changing nature of Extrinsic Assurance, moving from a simple pass/fail evaluation concept to one that is more clearly focused on the greatest threats. He also reviewed a new determination at CESG to work in closer partnership with Industry.

In the past Extrinsic Assurance was where most of the effort was focused in terms of product assurance. Considerable time and resources were invested in determining the level of confidence in a product through formal evaluations, but this is now seen to be too slow and costly and in itself does not generally provide an adequate level of assurance.

**“The result was a pass/fail concept of evaluations and this led very much to an accredit it and forget it view,”** said Nigel.

Too often products were evaluated once and then the IA aspects were forgotten.

**“We’ve got to move away from that to a much more through life view of assurance,”** explained Nigel. One of the concepts he was most keen to emphasise was the need for a holistic and whole life view of assurance.

Evaluations will continue to play an important part in the overall assurance picture, but Nigel insisted that they must be undertaken in different and smarter

ways: **“Make evaluations less prescriptive and better targeted at the greatest risk,”** he said.

## IMPLEMENTATION

Rick Crosby at the Forum



**Definition: Building a trusted system/network from components of varying trust; mitigation of residual risks from extrinsic; confidence in network/system architecture design and implementation; availability and integrity considerations.**

Rick Crosby provided an update on the Infosec Standard No.1 (IS1), which focuses on risk management and risk assessment and IS2, which covers risk management accreditation. He explained how IS1 has been fundamentally reviewed with the emergence of Version 3. He explained how this standard now uses a classic risk model, concentrating on threats and vulnerabilities.

Rick believes that IS1 Version 3 is an important step forward from the previous version: **“In my opinion IS1 Version 2 was a pretty blunt tool. The new Version has to cope with Transformational Government and Shared Services, identifying areas where attention should be focused. It models information assets and the risks of their being compromised – so for the first time, now you have to model the thing that you’re looking to measure the risk on.”**

IS2 Version 2 is another radical departure from previous versions. **“Whereas the earlier standard identified how to write an accreditation document set, the new version sets out how to accredit the system itself,”** said Rick.

**“Cradle to grave advice is provided on the accreditation process, which is tied directly to the OGC Gateway process and to project and programme cycles.”**

Rick concluded his talk by summarising the implications of these changes for Industry: **“There is now much more emphasis on threat and vulnerability analysis throughout the project and programme lifecycles.”**

**“There will be much more emphasis on implementation and operational security than we’ve ever done before at CESG.”**

## OPERATIONAL

Kevin Thacker at the Forum



**Definition: Continual through-life assurance; advice to customer/user on risks, threats, vulnerabilities and mitigation measures; configuration and change management; patching and updates policies; audit and accounting regimes; network monitoring and intrusion detection; penetration testing; feedback to intrinsic, extrinsic and implementation to improve future products and systems.**

Kevin Thacker, set the scene for the Forum discussion covering operational Assurance and Network Defence. He highlighted the importance of Operational Assurance becoming accepted into the mainstream as part of the CESG new Assurance Model.

Kevin believes that Operational Assurance is the element in the CESG new Assurance Model with the greatest potential to **“transform the way that we protect IT systems and the information on them.”**

Kevin identified the need for a very active three way partnership in providing Information Assurance, bringing together the risk owner, the IA Centre and Industry. The CESG new Assurance Model gives a new status to operational assurance, embedding Network Defence as a key element of the IA framework: **“Network Defence becomes mainstream as part of the CESG new Assurance Model,”** said Kevin.



## CESG Industry Forum 2007

# FORUM OUTCOMES

**A**t the conclusion of the Industry Forum a series of key issues were identified for urgent review and debate at IA07.

## BASELINE

At the event there was a clear difference in opinion over the relative merits and values of FIPS and CAPS and other evaluation methodologies, 'playing in the baseline space'. It was agreed that a 'serious piece of work' is needed to reach an agreed position to the question: "What do the accreditor and risk owner actually gain from these various processes?" How do these relate to each other and specifically to provide a view on FIPS – 140 – 3.



It was agreed that CESG and the CDF should jointly lead a workshop at IA07 to engage with this issue. The baseline developer community will also be invited to join this activity.



At the Forum there was considerable discussion over the role of the CLAS community in meeting the fundamental changes in the approach to IA that were debated. Some of the key questions included: How does the CLAS scheme have to develop and change in response to the CESG new Assurance Model? Should CLAS consultants be specialists? What additional training is required and who should provide it?

It was agreed that the emerging CLAS Forum should hold a workshop at IA07 to explore ideas and produce recommendations. The CLAS Forum was encouraged:

**"To think big about the professional changes required by this model."**

## SELF CERTIFICATION

There was considerable discussion over potential for self-certification at the Industry Forum. Discussion focused on the question's: **"What is a realistic model for self certification?"**

**Can the UK operate more of a trust and verify model?**

**Where is self certification a tool that we all realistically feel we can use?"**

The Industry Forum referred this issue to the IACG to develop ideas under their evaluation/certification work item and report back at IA07.

## IMPACT OF CESG NEW ASSURANCE MODEL ON RISK OWNERS

Engaging with Risk Owners was identified as a priority. The focus was placed on **"How best do we work together to educate customers and their accreditors about the CESG new Assurance Model – with its emphasis on richer risk information."**

It was agreed that an education campaign will be needed with the focus on convincing a community of risk owners and accreditors to understand and take seriously the risk that they face and to embrace the CESG new Assurance Model.

It was agreed that CESG will take the initiative in engaging with this issue, bringing together people who are able to devote **'some time, energy and thought to the question of how we can communicate this widely'.**

It was agreed to establish a user assurance team bringing together representatives from the Industry Forum, ITSO and Accreditors Forum. This will also have SIRO representation.



## UNTRUSTED COMPONENTS

There was also discussion of the impact on IA of untrusted components. The core issue is whether it is possible **'to architect your way out of trouble when using untrusted components'.**

It was agreed that CESG should brief on concepts/ideas in a workshop at IA07.

## IMPACT OF CESG NEW ASSURANCE MODEL ON EXISTING SLAS

During this discussion of outcomes from the Industry Forum, a further issue was identified from the floor. The view was voiced that there may be a mismatch between existing contracts held by service providers and the introduction of the CESG new Assurance Model.

It was agreed that the IACG would lead a stream on contracting at IA07 with support from the IATP Commercial Project and OGC.



# FOCUSING RESOURCES ON THREAT

Reflecting the new imperative to focus resources on tackling the greatest threats, CESG has launched an important new service for those responsible for assuring Government IT systems and networks.

The CESG Tailored Assurance Service (CTAS) is designed to significantly raise the standard of vulnerability detection – whilst offering greater flexibility and simplicity in delivery.

Delivered by CESG in partnership with assured, commercial evaluation houses, the service is designed to provide assurance for an entire system – rather than focusing simply on component products.

The new service is compliant with Infosec Standard No.1 (IS1) – this Standard is used to calculate residual risk when developing a Security Target and Evaluation Work Programme.

Each Evaluation is precisely tailored, drawing on a range of specialist activities, including:

- Development and procedures review
- Product functionality and design assessment
- System architecture and design review
- Security function testing
- Vulnerability analysis and testing
- Installation and operational procedures review
- Assurance maintenance plan review
- Source code analysis



Evaluations are carried out by CESG-approved contractors to a specification detailed in the Security Target and Evaluations Work Programme.

CESG agrees the scope and technical approach of the evaluation as well as reviewing the work of the contractor. CESG also makes recommendations on the significance of any issues that are discovered.

A clear accessible evaluation report summarises the results, lists any security vulnerabilities or major functionality errors and highlights any additional residual risks and (where known) their business impact.

The CESG Assessment Statement will confirm the extent to which the evaluation achieved the desired aims and summarise the significance of the main findings, highlighting any security risks or (where known) business impacts. It will describe the connection of the results to IS1 and any additional information that may be required.



## NEW VISTA FOR GOVERNMENT

Following collaboration with Microsoft, CESG has endorsed the adoption of Windows Vista for Government use.

The announcement was made by John Widdowson, Director, CESG, at a special launch event attended by senior directors responsible for information assurance across Government.

Engagement between CESG and Microsoft enabled the development of a UK Government specific configuration of Windows Vista known as the Government Assurance Pack (GAP).

This development allows the Civil Service and other public sector organisations across the UK access to the new Windows platform just three months after it was released.

Approximately 80 per cent of central Government organisations are already licensed to use Windows Vista under their existing enterprise agreements.

Through the Government Security Programme (GSP), CESG was given full access to Windows Vista months before the launch of the new platform.

John Widdowson said: "Our early collaboration with Microsoft has made it possible for CESG to endorse a rapid adoption of Windows Vista by the UK public sector.

"This means that the benefits of this product, which raises the bar in terms of information security, can be realised some 15 – 24 months earlier than would normally be expected.

"Delivering the Transformational Government and Shared Services agenda requires the latest technologies, achieving in Government the agility that private sector organisations enjoy.

"Today's announcement is a further example of our commitment to collaborate closely with industry to achieve more secure, safer and faster ways to assure new products and systems."

Graham Harrop, Director for Central Government, Public Sector, Microsoft UK said "Through programmes like the GSP, security and information assurance become an enabler to the business of Government, by building trust and understanding it enables our customers to realise their full potential through the latest software".

## INTERNATIONAL BRIEFING

**A**lison Whitney, Head of CESG International, provides a brief update on International IA issues:

**NATO TEMPEST Standards** have now been released to the EU following three years of preparation. The EU Infosec Office is now in the process of creating its own version of these standards.

**NOMAD Project** to provide a restricted network for the EU Council to allow remote working amongst other things, is currently mothballed and it seems unlikely that it will be revitalised. There is a temporary solution in place and there may be a tendering exercise to provide individual components for the network.

Initial orders for the **EU Secure Voice Capability** are for a relatively small number of handsets, but this project could turn into the basis of a much larger EU Council network.

There is a significant demand for **EU Restricted Level Products**, for example, to meet a requirement for a Restricted VPN for the EU mission in Baghdad; whilst the EU military service is looking for a USB type external crypto device.

**SESAME** is a Secret network for the EU Council and an example of a really significant international project opportunity. The latest information is that tendering for this project, which has been in planning for years, is finally expected to begin next year.

### INTERNATIONAL ADVICE

For products to be acceptable to the EU Council they must undergo a second evaluation (the first being carried out by the national IA authority) through the Council Infosec Selection and Procurement Scheme (CISPS). To achieve this, the product must be evaluated by one of the Appropriately Qualified Authorities (AQUAs).

Early planning is required to get through this process – CESG's International Relations team should be contacted as soon as a company is aware that it requires an evaluation.

Using a VEGAS algorithm in products helps speed the second evaluation through CISPS, because this algorithm is well known and well understood.



## NATIONAL IA STRATEGY... ON THE LAUNCHPAD

**T**he individuals that lead and shape IA in the UK are meeting in Brighton at the end of June, to attend IA07 the nation's most influential Information Assurance event.

**"IA07 will act as the launch pad for the Government's National IA Strategy,"** explains Mike St John Green, Deputy Director, Operations at CESG.

"The event will provide a vital platform for the public and private sectors to develop a joint understanding of the Government's new strategy for Information Assurance, identifying opportunities for improving the effectiveness and tempo of its delivery.

**"Our approach will be to identify and assign the specific actions and goals required to implement this strategy through true cross sector collaboration."**

To be held at the Hilton Metropole in Brighton on 27 – 28 June 2007, the event will bring together Government Departments and public sector organisations with National and Global business leaders and academia.

Hosted by CESG, in its role as the Government's National Technical Authority for Information Assurance, IA07 is the highpoint of the IA calendar. Open only to invitees, it will attract some 500 decision takers, thought leaders and those involved in setting the course for IA in the UK at the highest level.

Mike St John Green said: "IA07 is the national Information Assurance event for those shaping and delivering Information Communications Technology in Government."

Leading players are supporting the IA07 event. Symantec is the Pan Event Sponsor; with Associate Sponsors including BT, Harris, Microsoft, Research in Motion and Thales. HP is sponsoring the Communications Lounge at the event.

CESG  
A2j  
Hubble Road  
Cheltenham  
Gloucestershire  
GL51 0EX

Tel: +44 (0)1242 709141  
Fax: +44 (0)1242 709193  
Email: [enquiries@cesg.gsi.gov.uk](mailto:enquiries@cesg.gsi.gov.uk)



NATIONAL TECHNICAL AUTHORITY  
FOR INFORMATION ASSURANCE