

# **1 Network Infrastructure issues**

---

## **Background**

This call was to look at issues around the network infrastructure. There is still some confusion around whether the entire network needs to be segmented or whether it is just the area of the network that will be accessing GCSX materials.

Because Local Authorities are all different, the methods and topologies of their networks will also be different. There is no one size fits all solution. What has to be clearly understood is that the governments networks must be protected. Therefore any local network which connects into the government network, must have the correct levels of separation.

The minimum requirement is a well separated / defined network with a dedicated firewall solution.

## **Firewalls**

A worry was expressed, where there is a router outside the controlled network in a DMZ, the solution here would be to have a separate network Card. The Government Connect Team are happy to look at network configuration diagrams and the central GC team can advise on topology issues.

The real key is to set it up and leave it – discourage changes. Where you have multiple firewalls, your encouraged to use different brands, ie one Juniper, one CISCO for example. That way if one firewall has a vulnerability, the other won't. The Government call this approach "Defence in depth".

See: <http://www.cpni.gov.uk/docs/re-20050804-00653.pdf>

GC Firewall requirements, they need to have a dedicated Level EAL4 firewall, for resilience if the configuration uses two firewalls, they should be different makes. Deploy separation using firewall to segment the internet connection.

See: <http://www.cabinetoffice.gov.uk/spf.aspx>

You need to consider what else is sharing the firewall? A separate domain within the firewall will be required for GCSx. Defence in depth, using firewalls from different vendors whilst realising that there are financial issues.

Defence in depth is part of CESG model , this is explained in the new Security Policy Framework, that replaces the Manual of Protective Security, which will be published soon on the CESG website.

See: <http://www.cabinetoffice.gov.uk/spf.aspx>

### VLAN and 3rd party access

VLAN – big problematic area. The Government Connect Team have prepared a specialist guide on VLANs. CESG has also produced Manual V which details the methods for deploying and configuring VLANs. Specifically, the advice is to use VPN encrypted connections over the VLANs within the council network and then onward from the council into the GCsX network.

### 3<sup>rd</sup> Party Access concerns:-

What access have they got

What controls are in place to monitor and log sessions

Outsourced services MUST Be compliant- as they may have access to GCSX mailboxes.

Access should be minimised  
Extend controls to 3<sup>rd</sup> Party providers  
Is Risk being actively managed.

How to deal with long term contracts which are already in place.

VLANs. High area of concern

VLANs are insufficient to provide secure connections use SSL VPN's

<b>Action point:</b>
----------------------

Identify the number of L.A's effected.
--

### IL3 (Impact level 3) – transmitting RESTRICTED Data

For many local authorities, this is a major architectural issue. To get signed off, GC will need to be provided with a date when by when SSL can be put on, and a statement around how will the risk be managed in the short term

<b>Action point:</b>
----------------------

Produce a guidance note on handling PROTECT and RESTRICTED
--

### GESG Book store

Every local authority can have a copy of the CESG bookstore. All you need to do is fill in a Business Case form obtainable from [enquiries@cesg.gsi.gov.uk](mailto:enquiries@cesg.gsi.gov.uk)  
Telephone: +44 (0) 1242 709141

Policy not guidance, various guidance documents will need to be produced.  
Specifically help is needed on:

## Government Connect Conference Calls Summary Report

---

- Static IP addresses
- Routable addresses
- CPNI guidance

Intrusion detection “ Should Control” – IDF

Symantec Host Bases- should NOT be on the firewall as it does not monitor the internal network.

### **Action point:**

Identify alternative products

MUST ensure users are authenticated

Windows 98 – NOT ALLOWED – I guess because of logon authentication not being strong enough?

### **Hardening**

Closing Ports

Close down services which are not being used

### **Malware**

AV – automatic detection and removal

For advice see: <http://www.cpni.gov.uk/Docs/currentAdvice.pdf>

### **Older legacy software**

- o Software which require elevated user rights ( ie admin)
- o Opens the door to malware to use admin rights of use
- o How long does it set compliant
- o Drop my rights
- o Mitigating Risk

### **Other issues**

- Effective Change control procedure
- Patch Management
- Identification from trusted sources
- Emergency patching procedures
- Identify un patchable software/ Operating systems
- Active X controls – need a business case
- Auto forwarding
- Libraries and public access.
- Clear separation of Traffic.

## **2 Training and user awareness**

---

The whole issue around training and awareness must be completely engrained in the organisations culture. The training needs to be at three Levels;

- Senior Management and Members
- IA Practitioners and Business Managers
- System users and Citizens

The top level training needs to be around corporate risk management and how the whole security and Information Assurance agenda within the organisation.

The IA practitioner training is to ensure all managers understand their responsibilities in looking after security and information assets. The IA Managers themselves, need to fully understand all of the security and assurance issues for GC, the Data Handling Review, the PCI DSS requirements for credit cards and other inter-linked initiatives, which all work towards a coherent strategy to ensure Information Assurance gets embedded in corporate culture, this will not happen overnight.

Systems users and citizens, also need to understand how to handle information and ensure its security, integrity, safe storage, proper processing and finally secure disposal.

The Cabinet Office, through the National School of Government, has launched free on-line e-learning to know how to properly understand their obligations in handling sensitive personal data.

There will be a widening of courses over the coming months through the National School of Government, with training around Data Handling for IA practitioners. Socitm Learning is developing courses [www.socitmlearning.co.uk](http://www.socitmlearning.co.uk) and Amberhawk Associates [www.amberhawk.com](http://www.amberhawk.com) To offer specific guidance around these issues.

For specialist training around penetration testing, managing penetration tests and a wide range of other associated issues, the TigerScheme provides a register of competent IA professionals, able to work with authorities to help them with their testing requirements. See: [www.tigerscheme.org](http://www.tigerscheme.org)

Understanding and dealing with protectively marked material.

A guide for Local Authorities will be written by March 2009. There is an excellent guide which has been produced by BECTA at: [http://schools.becta.org.uk/upload-dir/downloads/information\\_handling\\_impact\\_levels.pdf](http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf)

## **Government Connect Conference Calls Summary Report**

---

Belonging to a WARP – (Warning, Advice and reporting Point)

All Local Authorities are encouraged to join a WARP, some regions already have them, those that do not, have the opportunity to subscribe to one, during 2009. For further information see: [www.nlawarp.gov.uk](http://www.nlawarp.gov.uk)

### **3 Mobile and Remote Working**

---

This topic raised the most questions, issues and interest during the conference calls.

#### **Managed and Non Managed PC's**

Managed Kit –

- PC/ Laptop that is the property of the local authority
- The “connection” is also managed by the Local Authority
- The PC/ Laptop is controlled and managed by the local Authority  
( Proper Virus protection/ Desktop locked down, subject to authorities Security policies.)

It is clear that a distinction needs to be highlighted between Managed and Non managed home worker PCs.

L.A's with Non Managed PCs – will not comply with the CoCo.

Citrix – Is a good solution but does not automatically imply control, so Citrix solutions need to be directly managed through policies and locked down functionality. Citrix solutions are widely deployed in the GSI.

#### **Outsourcing**

Any L.A, with outsourced , then that provider had to meet the CoCo.  
Is there a list of outsourced providers – who are CoCo compliant?  
Again, third party supplier issues need to be carefully managed and policy driven.

#### **3<sup>rd</sup> Party remote maintainers**

Any third party suppliers need to be brought up to your organisations baseline standard as a minimum.

Awareness Training is essential for internal and external staff.

Baseline Personnel Security Standards must be deployed within the organisation and externally.

Identify what sort of access is required, grant only the minimum required for the business process.

The default state of remote access systems should be disconnected.  
Are the sessions Logged and monitored? They must be.

## **Government Connect Conference Calls Summary Report**

---

Degrees of access must be written down (Policies) and audited.  
Industry Best Practice should be followed.

Is there a network diagram, clearly identifying what remote access point are available? There should be a regular penetration tests should be scheduled.

### **Identify Risks**

CoCo compliance is required for those services which NEED to access the services remotely for maintenance purposes. A remote access point could be the single biggest weakness and therefore attack vector on your network.

Identify the users who need access to the services on offer. Keep a remote access register, who has access, from where? When? How? Why? Regularly review and remove those who do not need access.

Produce a plan of areas which are not yet compliant – but what the L.A intends to do to make them complaint and the timescale involved and what they are doing to manage the risks do not make promises which cannot be met. Have a risk treatment plan, key milestones.

## **4 Policy and Governance**

---

Policies and governance are the core to a successful GC implementation. The technology standards and solutions all exist and even the best of them will not solve problems unless they are implemented into a policy driven framework, with good corporate information and risk governance and an effective audit and monitoring regime.

Non Council devices will always be a n issue and will need to be brought within a framework, even if using a thin client solution, traces of sessions can be left on systems. When designing a network solution involving non-council owned devices, the assurance integrity of the network, cannot be compromised by a non-compliant component, this could well be a non-council owned PC or asset. The security and integrity of the entire network can only be as good as it's weakest link. This is why you can simply plug a home PC into the corporate network, which could in turn allow onward GCSx connection and potentially GSi compromise.

A properly implemented Citrix thin client solution, could be a way forward, using a product like BeCrypt trusted client, this is undergoing specific testing and the moment.

Web Browsing within the network, products like "Drop my rights" and "PS exec" can help.

Mobile devices must be council owned and managed  
VLAN segregation can help, as part of an overall approach.  
Sub network approach, a hardened bubble to connect to GCSx, this could be an approach, but long term the entire network should be GCSx compliant.

We need to develop some case studies and to get them written up.

Case Study on Mobile and remote workers how it has managed to be achieved. Logging and audit Products that work and are applicable need to be identified.

Windows bit locker for disk encryption should be ok. All laptops and remote devices/ removable media must be encrypted to handle protectively marked material. This is another reason why personally owned PC's are not suitable For corporate use.

Lock down and remove unnecessary windows functionality. Where possible use least privileged accounts on windows , do not use administrator PC account or access for daily work.

## 5 Audit & logging

---

Auditing and monitoring is a critical part of good information security and assurance. Attitudes towards auditing and monitoring needs to change significantly. The Audit and monitoring regime provides the ongoing diagnostics for how healthy and secure your network is.

The really good thing is that much can be automated. There are a number of products and services that can monitor aspects of the network, infrastructure, e-mails, remote access and usage.

Sites with a variety of Operating Systems – Unix, Novell , Microsoft, so products need to be flexible and appropriate for what needs to be recorded and retained to comply with the code of connection.

- Selective sampling
- Auditing strategy
- Audit individuals

### Controls

Good practice  
Aids investigation of incidents

### What is useful

Time stamped- event,  
when  
where  
who  
What processes  
Use this info to help resolve any future problem

Internal Ping- monitor this event, who is doing it? Why?  
Know what VPNs and encrypted links are embedded within you network.

Port scanning information – what occurred, by who and when.  
Proactive monitoring against specific applications.

The is a “SHOULD” requirement, which is part of a policy driven approach.

GCSx, compromises, MUST be reported to GovCert, they SHOULD also be reported to your regional WARP. By sharing incidents anonymously we will all learn from these incidents.

There is a white paper at:

[http://www.infosec.co.uk/ExhibitorLibrary/766/Govt\\_Connect\\_v5\\_20.pdf](http://www.infosec.co.uk/ExhibitorLibrary/766/Govt_Connect_v5_20.pdf)

## **Government Connect Conference Calls Summary Report**

---

Logging is about aiding incident management and response. Apart from the GC CoCo, this is good practice as part of ISO 27001 and for PCI DSS conformance.

This auditing and monitoring is for the GCSX connection and those connected to GCSX to enable GovCert, to investigate.

Version 4 CoCo is not live, you implement on version 3.2  
Having said that.....

Clarify how far into the CoCo process you need to be, before you get caught by version 4. Some SHOULD be MUSTS.