Automated Compliance with the GCSx Code of Connection

Produced on behalf of New Net Technologies by

STEVE BROADHEAD
BROADBAND TESTING

www.nntws.com

The Government Connect Secure Extranet

The UK Government's initiative to prescribe a security standard to any organization accessing the Government Connect Secure Extranet is a move designed to keep government organisations one step ahead of the inexorable increase in security threats. There have been too many high profile data thefts and losses by Government organizations, highlighting both the risk to, and the importance of, ICT Security and the governance of citizens' data.

The result is the Government Connect Secure Extranet (GCSx). HM Government has mandated the way in which public authorities and government departments can securely transfer data between each other.

So, for example, how does a local authority needing Housing Benefits data access the Department for Works and Pensions (DWP) database? Via the GCSx of course!

Similarly, Job Centre Plus communications with local authorities will only accept communications via the GCSx, and likewise, communications with the Police and the NHS will only be provided through this connection.

"The concept is a "community of trust" and the GCSx is one of a number of secure Government extranets, including GSx, GSi and GCJx. See our Glossary of Terms at the end for details of these other networks"

The concept is a "community of trust" and the GCSx is one of a number of secure Government extranets, including GSx (Government Secure Extranet), GSi (Government Secure Intranet) and GCJx (Criminal Justice Extranet).

So how does a district council access the GCSx? Via a secure connection, the security of which is governed by the Code of Connection, or 'CoCo'.

CoCo—The Code of Connection

The Code of Connection takes into consideration how best to protect the "community of trust" taking into account all potential threats, including

- Attack from the GCSx itself
- Attack from the Internet
- Mobile data theft and loss
- Attack from the internal user

Code of Connection (CoCo) for the Government Secure Intranet (GSI) and GCSx, Memorandum Number 22. According to CESG Infosec Memorandum Number 22, protective monitoring has traditionally been the most underrated and least effectively used security measure.

CoCo - The Details...

The scope of the GCSx Code of Connection can be summarised as follows:

- Physical Security and Access Control, restrict and control access to the GCSx, including use of Firewalls, Intrusion Protection technology and with particular focus on Mobile/Remote Worker security
- Policies and Procedures, in particular Change Management Processes, approvals and documentation.
- Configuration 'hardening', to ensure that known threats and vulnerabilities are eliminated from all systems, with a zealous patch management process combined with anti-virus technology, regularly tested and verified as secure.
- Strong Monitoring for security incidents and events, with all event logs being retained for 6 months

> *"it makes sense to consider measures for CoCo compliance in the context of PCI DSS, since the same technology that helps deliver CoCo compliance should be relevant for PCI DSS"*

Sound Familiar ?

In fact, the scope of the standard is quite similar in respect of its approach and its measures to the PCI DSS (The Payment Card Industry Data Security Standard), which is another security standard all local authorities will now be familiar with.

The PCI DSS is concerned with the secure governance of Payment Card data, and any 'card merchant' i.e. an organisation handling payment card transactions, such as a District council collecting Council Tax, must comply with the details of the security standard.

Therefore it makes sense to consider measures for CoCo compliance in the context of PCI DSS, since the same technology that helps deliver CoCo compliance should be relevant for PCI DSS.

Or to put it another way – compliance with one will significantly assist compliance with the other.

Conclusion - How can NNT help?

- **Compliance Auditing** – multiple 'out of the box' and 'made to order' reports allow you to quickly test critical security & configuration settings for servers, desktops, network devices and firewalls. NNT Compliance Hub provides reports detailing your administrative procedures and technical security mechanisms. Typically these reports will identify some security gaps. Once rectified you can re-run reports to prove to auditors that your IT systems are compliant. Using the inbuilt change tracking described below you can ensure systems remain compliant. It's really that simple!

- **Change Tracking** – once your firewalls, servers, workstations, switches, routers etc are in a compliant state, you need to ensure they remain that way. The only way to do this is to regularly verify the configuration settings have not changed, because unplanned, undocumented changes will always be made while somebody has the admin rights to do so – legal or otherwise! We will alert when any unplanned changes are detected as well as keeping an audit trail of planned changes to be reconciled with the request for change details if needed. This provides a closed loop change management safety net.

- **Planned Change Audit Trail** – when changes do need to be made to a device then you need to ensure that changes are approved and documented – we make this easy and straightforward, reconciling all changes made with the RFC or Change Approval record

- **Device 'Hardening'** is enforced and audited – we run automated templates for a hardened (secured & compliant) configuration for servers and desktops and network devices to show where work is needed to get compliant, thereafter we track all planned and unplanned changes that affect the hardened status of your infrastructure. Specifically we cover registry keys and values, file integrity, services and processes are whitelisted/ blacklisted, user accounts, installed software, patches, access rights, password ageing and much more.

- **Event Log Management** - All event logs from all devices will be analyzed, filtered, correlated and escalated appropriately. Event log messages are stored in a secure, integrity-assured, repository for the required retention period for any governance policy.

- **Correlation of Security Information & Audit Logs** – we provide Log Gathering from all devices with simple correlation for security event signature identification and powerful 'mining' and analysis capabilities. This provides a complete 'compliance safety net' to ensure, for example to name just a few, virus updates complete successfully, host intrusion protection is enabled at all times, firewall rules are not changed, user accounts, rights and permissions are not changed without permission.

FOR A FREE TRIAL OR TO DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT **info@nntws.com**

About NNT

NNT build the worlds best solutions for tracking and managing change, managing and protecting users, maintaining system performance and ensuring availability across the entire enterprise.

Understanding and managing the day to day changes within your environment is critical to establishing and maintaining reliable service. NNT Solutions are affordable and easy to use.

NNT help you establish and maintain a 'known and compliant' state for your IT systems. Including: PC, Network, Software, Host Machine and Database.

www.nntws.com

UK Office - Spectrum House, Dunstable Road, Redbourn, AL3 7PR
Tel: +44 8456 585 005

US Office - 9128 Strada Place, Suite 10115, Naples, Florida 34108
Tel: +1-888-898-0674