

# Whitepaper

## **UK GSi Code of Connection Controls Mapping for Bradford Networks' NAC Director**

**Jim Hietala**

CISSP, GSEC, GCFW Principal Analyst

Compliance Research Group



# Contents

Introduction.....	1
<i>What is the Code of Connection (CoCo)?</i>	
<i>The GSi Connection Process</i>	
<i>Who is Required to Comply?</i>	
<i>How does Bradford Networks Helps Organisations Achieve Compliance with CoCo ?</i>	
Bradford Networks' NAC Director.....	2
<i>Identity Management</i>	
<i>Endpoint Compliance</i>	
<i>Usage Policy Enforcement</i>	
<i>CoCo Requirements and NAC Director Mapping</i>	
Summary.....	4
About Bradford Networks.....	5
About Compliance Research Group.....	5

## Introduction

All UK government organisations must comply with Code of Connection (CoCo) security requirements before connecting to the Government Secure Intranet (GSI). Organisations connecting to the secure GSi must document security compliance, have connection authorized annually, and be subject to on-site audits. Non-public organisations may connect to a related secure network with a public sector sponsor, and demonstrated compliance with the CoCo controls.

Bradford's NAC Director helps UK government organisations to comply with CoCo. NAC Director provides full or partial coverage for 18 of 28 CoCo control areas, easing the GSi connection process, while strengthening security for sensitive information and systems.

### ***What is the Code of Connection (CoCo)?***

The UK government, as a part of a 2005 government technology initiative, has created a secure intranet network known as the Government Secure Intranet (GSI). The GSi is a Managed Service operated by OGCBuying.solutions, and delivered through a partnership with Cable & Wireless UK. In order for government organisations and local governments to connect securely to the GSi network, the UK government developed a set of security standards and requirements. These requirements, known as the Code of Connection (CoCo), describe a set of security controls which must be in place prior to connecting to the GSi network. The security controls described in the CoCo were developed by the Communications-Electronics Security Group (CESG), and are based on their technical security policies and on BS7799/ISO27001 controls guidance. A government department known as OGC buying solutions (OGCbs) is responsible for enforcing GSi security compliance.

### ***The GSi Connection Process***

The GSi connection process requires that organisations wishing to connect to the network:

1. Obtain a copy of the Code of Connection
2. Read, understand, and implement the security controls described in the Code of Connection
3. Provide evidence and self-attest that the organisation has indeed implemented the controls

Organisations connecting to the GSi are required to obtain re-authorisation for their connection on an annual basis. This means updating the submission information, and documenting network and security changes that might affect compliance status. In addition, OGCbs may conduct on-site compliance audits of GSi organisations.

The Code of Connection is itself a protected document, meaning that its contents cannot be reproduced and distributed by third parties. For the purposes of this functionality mapping whitepaper, we have used the exact CoCo reference numbers and control areas, and have paraphrased the control language. Potential users of the GSi who obtain the Code of Connection will have no trouble relating the information presented here to the actual controls as described in the CoCo.

### ***Who is Required to Comply?***

In reality, the GSi network is comprised of five different communities of user organisations and distinct networks (xGSI, GSI, GSE, GSX, GCSX), each with different requirements regarding the sensitivity level of the data that may be shared on it. Access to the GSi network is limited to UK public sector organisations including UK and national government departments and agencies, non-departmental public bodies and local authorities. In addition, non-public sector organisations are eligible to join the related GSE network. They are required, however to have sponsorship from a public sector organisation. Such organisations are also required to comply with the connection process, and with the controls identified in the CoCo.

All organisations wishing to connect to the GSi network are required to undertake the connection process described above. This includes county council governments, UK and national government agencies, and all others.

### ***How does Bradford Networks Helps Organisations Achieve Compliance with CoCo ?***

CoCo requires organisations to have a prescribed set of security controls in place prior to connecting to the GSi network.

A relatively new class of security technology, Network Access Control (NAC), secures networks by ensuring the health and identity of the devices that connect to them. NAC solutions address network control issues that older legacy solutions like firewalls, host-based identity, and access management products were never designed to counter.

Bradford Networks offers NAC solutions that help organisations to secure and control access to their networks. NAC Director enables compliance with CoCo in numerous ways by automating enforcement of strict access control policies and ensuring that devices attaching to networks satisfy specific security requirements.

NAC Director is an out-of-band solution that leverages an organisation's existing network infrastructure for security policy enforcement. Leading analysts have characterised out-of-band NAC implementations as the most secure, most scalable, most flexible, and most cost-effective solutions for automating network access control.

## **NAC Director**

NAC Director provides a comprehensive NAC solution through active enforcement of network usage policies. As employees, contractors, and others access network resources via wireless, wired, and VPN connections, NAC Director automates the process of ensuring that users and devices are authorised for access and that they meet specific security policy requirements.

NAC Director's identity management, endpoint compliance, and usage policy enforcement capabilities can help retail enterprises to enforce specific access policies with role-based access to network resources, protecting against authorised users and non-compliant devices.

### ***Identity Management***

With employees and others using a range of devices to access network resources from diverse locations, effective network security for retail organizations must start with a robust identity management process. NAC Director requires all users and devices to be registered and authenticated prior to granting access to the network.

Role-based access functionality ensures that users are allowed access only to specific network resources, depending on the type of service authorized. The result is tight control over network access and a consistent, real-time view of users and devices accessing network resources.

### ***Endpoint Compliance***

NAC Director ensures that all devices accessing the network meet required security standards by performing registry-based scans on endpoint devices prior to allowing network access. Port-based vulnerability scans can also be performed using the open-source Nessus application.

Devices failing to meet specified security standards are placed in a secure 'quarantine' state to prevent access to network resources. From this quarantine state, legitimate users are given the ability to remediate any compliance issues so as to regain network access.

NAC Director's endpoint compliance features validate: operating system types and patch levels, anti-virus / anti-spyware application types and definition version levels, presence of required applications such as firewalls or prohibited applications such as peer-to-peer communications.

In addition, customisable registry scans with monitoring capabilities detect files, processes, and other registry keys that enable a range of other endpoint compliance criteria.

### ***Usage Policy Enforcement***

NAC Director applies role-based identity information and endpoint compliance criteria to enforce user-specific network access policies at the network edge -- in other words, at the point where endpoint devices physically attach to the network.

Usage policy enforcement actions can include blocking network access completely, limiting network access to only specific resources (such as for remediation), and alerting network administration and/or security personnel to policy violations, as well as a wide range of other configurable actions. NAC Director also interfaces with third-party solutions such as IDS, IPS, and firewalls to gather additional information for enforcing access control policies. The result is network-wide control over access to network resources and automated enforcement of specified network usage policies.

## CoCo Requirements and NAC Director

The table below identifies 18 specific CoCo requirements that NAC Director addresses. Requirements not addressed by NAC Director are excluded from the table.

Code of Connection Control Reference Number		Control objective	NAC Director relevant functionality
2.2	User Education	Organisation must provide awareness training.	NAC Director provides the ability to communicate with all connecting users via text box on the desktop or captive portal page, allowing communication of educational information as well as real-time alerts, such as notifying users of potential security policy violations.
2.3	Incident Response	This control objective requires the organisation to quickly report security incidents to management.	NAC Director facilitates the discovery and reporting of security incidents through alarms and alerts that can automatically report incidents to help desk staff and/or management. NAC Director can also initiate security actions automatically, such as isolating a network user or device in response to a particular incident or risk.
2.4	Compliance Checking	Organisation is required to check the health of IT systems every twelve months.	NAC Director enables pre- and post-connection compliance checking for all network endpoints. Frequency is determined by the organisation, and checks can include all aspects of the endpoint's security posture, including patch level, anti-virus and anti-spam signature file versions, and more.
2.5	Access Control	This control objective requires unique user ID's for all users	NAC Director enforces ID checking for all users and integrates with existing directory and authentication systems including Active Directory, LDAP-based directories, and RADIUS. NAC Director also uses of a 7 point identity profile to match each unique user ID with a user role; device name; MAC address; IP address; network access point; and time of day.
2.5.1	Access Control	Users of the secure network must be authenticated with complex passwords.	NAC Director Guest/ Contractor Services (GCS) can enforce the use of complex passwords when user ID's and passwords are stored in the system's local database. When using external directory and authentication systems, such as Active Directory or RADIUS, NAC Director and NAC Director GCS integrate with those systems to authenticate users prior to allowing network access.
2.6	Network Schematic	All organisations connecting to the secure network must submit a network topology diagram that details all connected network nodes and all remote access points, and the remote access users.	NAC Director performs a network discovery to identify all network devices and nodes. This greatly reduces the effort and time required for IT staff to generate the required network schematics and associated details.
2.7	IP Addressing	IP Address blocks used in internal networks must conform to RFC 1918	NAC Director enhances the capability of the DHCP server by providing detection and alerting of invalid IP addresses attempting connection to the internal network.
2.7.1	IP Addressing	Requires the use of static addresses for servers.	NAC Director verifies that device addresses for all network connected devices are valid/known IP addresses.
2.9	Intrusion Detection	Attacks should be identified with intrusion detection defenses.	NAC Director works in concert with intrusion detection/prevention systems to identify, locate, and stop potential attacks and threats. When an IDS/IPS device detects a threat, NAC Director can pinpoint the source of the threat to a specific device, user, and location, and can automatically isolate the source to eliminate the threat.
2.9.1	Intrusion Detection	Intrusion detection systems should monitor the organisation's secure domain and areas between the secure domain and connected networks.	As mentioned in 2.9, NAC Director significantly expands the utility of IDS/IPS devices to react to threats.
2.9.5	Intrusion Detection	When inline network connections are used for intrusion detection systems, organisations should protect the intrusion detection system and limit access to authorized users.	NAC Director helps to segment the internal network, limiting access to the network segment containing the IP to only authorised users and roles.
2.10	Mobile Working	Mobile users of the secure network must follow the guidance provided by OGCbs in Guidance Notes.	Mobile users (VPN, wireless, or dial-in) accessing a network protected by NAC Director are subject to the same identity management, endpoint compliance, and usage policy control as are internal network users.
2.13	Protective Monitoring	Organisations should be able to identify and investigate suspicious activity, and achieve a "Partial" rating as defined by CESG Infosec Memorandum 22.	NAC Director provides real-time identification of invalid access attempts and failed policy checks, and can provide notification, quarantine, and self-remediation for devices with suspect security health.
2.13.1	Protective Monitoring	Audit logs of all user activities and events must be produced to assist in investigations and for monitoring access control.	NAC Director delivers extensive audit logs of all internal network activity for wired, wireless, and VPN connections.
2.13.3	Protective Monitoring	All logs of user activities and events must be retained for at least six months, and organisations must be knowledgeable of any requirements for longer log retention.	NAC Director provides logs in a standard MySQL format for log management requirements. Logs can be exported to external storage devices and/or to external reporting and analysis tools.

## UK GSi Code of Connection Controls Mapping for Bradford Networks' NAC Director

2.15	Configuration		Requires security hardening of all Hosts.	NAC Director provides extensive assessment of endpoint security posture using persistent and dissolvable agents, and Nessus-based scanning for agent-less assessment. These capabilities simplify and automate the process of identifying hosts that have security deficiencies.
	2.15.1	Configuration	Any host infected with malware should be adequately disinfected.	NAC Director can enforce policies for endpoints to have appropriate anti-virus and anti-spyware programs running to minimise the chance that a host infected with malware will be allowed to connect. Hosts without these programs can be isolated to protect the rest of the network.
2.16	Software Policies		Organisations should have policies and technical safeguards to prevent unauthorised software from executing on protected host systems.	NAC Director assesses hosts for the presence of required and prohibited applications and processes, and can prevent hosts with unauthorised software from connecting to the network.
2.17	Patch Management		All software must use a patch management process for system and network upgrades.	NAC Director integrates with patch management solutions including BigFix to verify compliance and auto-remediate non-compliant devices.
	2.17.1	Patch Management	All applicable software and service upgrades from vendors and GovCertUK must be deployed.	NAC Director integrates with patch management solutions including BigFix to verify compliance and auto-remediate non-compliant devices.
2.18	Vulnerability Scanning		Security vulnerability scanning should be conducted quarterly at a minimum.	NAC Director provides extensive assessment of connected hosts and enables further assessment by Nessus vulnerability scans.
2.21	Personal Firewalls		Requires that personal firewalls should be enabled on all systems.	NAC Director can enforce policies requiring that personal firewalls be installed and operational on each endpoint system.
2.23	Removable Media		Requires that removable media be disabled or controlled, and not used unless a business case exists.	NAC Director can scan system registry information for detection of USB or other media. Policies for removable media can be enforced by user or by device, such that some may be allowed while others are not. When unauthorised media are detected, NAC Director can isolate the offending device as well as notify help desk staff and/or management.
2.25	Mail Servers		Several requirements specifying that traffic to/from mail servers should be segmented, and access to the mail server subnet restricted.	NAC Director uses VLANs and access control rules on a per group basis to provide fine-grained access control to network segments and devices.
2.27	Multi-Domains		Organisations should use multi-factor authentication for remote access to applications connected to both the secure network and less protected or unsecure networks, with the secure applications segregated on the unsecure networks.	NAC Director can enforce device registration and user authentication, and integrates with existing directory and authentication systems including Active Directory, LDAP-based directories, and RADIUS.
2.28	Voice Over IP		Requires VOIP security as described in NIST documents.	NAC Director can segregate VOIP devices on different VLANs to provide network segment isolation. In addition, the ability to support agentless operation provides a seamless way to support VOIP endpoints.

## Summary

Bradford's NAC Director helps UK government organisations comply with Code of Connection (CoCo) security requirements for the Government Secure Intranet (GSi).

- NAC Director helps organisations to comply with 18 of 28 CoCo security controls
- NAC Director eases the GSi connection effort and CoCo compliance process
- Organisations deploying NAC Director will benefit from stronger network, system and data security

## About Bradford Networks

Bradford Networks develops advanced network access control solutions for wireless, wired and VPN networks. Bradford's patent-pending, award-winning, out-of-band appliances leverage existing network infrastructure to automatically enforce policy at the network edge, making networks more secure and efficient. Privately held, Bradford Networks is headquartered in Concord, NH. For more information, call (603) 228-5300 or visit [www.bradfordnetworks.com](http://www.bradfordnetworks.com).

## About Compliance Research Group

Compliance Research Group is a consulting and research firm focused on these areas:

- IT Risk
- Compliance
- IT Security

We conduct end user research into various aspects of risk, compliance, and security. We also research and provide analysis on the supply side of the risk, compliance, and security markets. Compliance Research Group provides consulting services for organisations in these areas as well. Our focus is on helping end users, vendors, and channel participants to better understand the critical issues and requirements that exist in these dynamic markets. The principals of Compliance Research Group have a deep technical understanding of the risk, compliance, and security markets and technologies. Our analysts and consultants hold multiple CISSP and GIAC certifications, including GSEC-Gold and GCFW-Gold certifications from SANS/GIAC.

Compliance Research Group is proud to have been able to partner with other leading organisations in the security, risk, and compliance areas, including the SANS Institute, Logical Security, and The Open Group. We maintain active memberships in ISC(2) and ISSA. For more information please visit [www.complianceresearchgroup.com](http://www.complianceresearchgroup.com).

### DISCLAIMER

This document provides general information about personal privacy and compliance initiatives in North America. It is intended to be used for resource and reference purposes only and does not constitute legal advice, nor should it be construed as providing any warranties or representations with respect to the products and/or services discussed herein. Readers of this paper are encouraged to speak with their legal counsel to understand how the general issues discussed above apply to their particular circumstances. Compliance Research Group and Bradford Networks disclaim any and all liability for damages, costs, lost profits, fines, fees or financial penalties of any kind suffered by any party acting or relying on the general information contained herein.