



**NETWORK
NIGGLES**
Yurong Lin
CEO,
Deepnet Security

Councils face loss of Government Network Connection without CoCo compliance

As the clock ticks down on the Government's Code of Connection (CoCo) standards deadline of 30 September, it is apparent that councils are going to face a real threat of ID theft and loss of network connection to central Government departments if they don't comply.

The numbers show that over a quarter of local councils won't be compliant by the time the deadline takes effect. This statistic is worrying by itself, but combined with the sheer amount of calls which we have had seeking basic CoCo advice, it is truly astonishing how unprepared some councils are.

Whilst councils are looking for a quick fix to the problem, it is clear that it's the lack of knowledge around the topic which is holding them back and causing widespread confusion of what is required and who to turn to for a solution.

The easy answer is that achieving CoCo compliance isn't a quick job. There are many different areas which councils must comply with. From our experience we predict that there are five key areas that are going to prove a challenge for councils and they are: securing remote devices, developing secure processes, managing software centrally, managing a cultural change, and maintaining ongoing compliance.

For remote devices to be CoCo compliant they must be secure, encrypted, and only given access to the network through a secure virtual private network (VPN) using two-factor authentication. The simplest way to achieve this is to provide a unified authentication platform to prohibit unauthorised access to government networks, without the need to increase password complexity. Greater complexity invariably means users forget their passwords and need to call the IT help desk for a reset, or worse still put their data at risk by writing them down.

Two-factor authentication can be provided through a number of methods, such as a secure USB stick, mobile phone, biometrics, or a hardware or software token, whatever is easiest for the user.

Achieving compliance can appear complex and confusing, but councils must address this head on now by reviewing security processes, so that they are not burying their heads in the sand and have enough time to implement any necessary changes before the deadline arrives.