

Cambridgeshire Constabulary has generated savings and simplicity with a new confidential network that enables it to meet stringent government encryption requirements without replacing its entire network.



# Highly confidential



**Tracey Hipperson:** "Through sensible project management we've actually managed to meet regulatory requirements and the strategic needs of the force for the next ten years."

Recent government requirements to improve confidentiality and security of data transfer by the middle of this year have resulted in a rise in the necessary encryption levels for information shared with, and between, police forces. The Government's Communications Electronics Security Group (CESG) standards demand that specific encryption levels of all internal police force networks adhere to the Government Protective Marking Scheme (GPMS) caveat of 'restricted' or higher – Impact Level 3 or above.

Concern that the CESG guidelines will be costly and time-consuming at a time when forces want to focus energy and resourcing on core police work, led to Cambridgeshire Constabulary taking the opportunity to review its entire network.

With over 70 sites across the region, the force recognised that a transition programme would be necessary if it was to meet the required classification levels.

Led by Tracey Hipperson, director of information and communication technology (ICT), the constabulary started with an audit of the existing infrastructure. This process led to the creation of a new confidential network which will also meet the strategic requirements of the constabulary for the next ten years.

## Challenge

The new requirements demanded that a certain standard be met – networks would have to be accredited as both 'restricted' and 'confidential'. The concern voiced by many police forces is that meeting the standard would involve replacing or outsourcing their entire networks.

The aim was to meet the encryption requirements without having to start from scratch with a completely new network and the accompanying high costs. It was also important to work with the various departments involved to create a workable and compliant network blueprint.

"Our whole system was in need of a refresh," explains Ms Hipperson, "so we called in CNS (Convergent Networks and Security) to start with a network audit; this resulted in significant savings on our circuitry alone, through converting a piecemeal approach to one single and effective agreement. Our in-house team then worked with the security and networking consultancy to identify the issues within the network and we decided upon a complete revamp which would ensure the Cambridgeshire network was up to the challenges of 21st century policing".

## Solution

The internal police IT teams worked with CNS to design a solution to the problem. This collaboration created a plan for the Cambridgeshire Constabulary project, which is also being considered by other forces nationwide.

Ian Bell, head of service delivery at Cambridgeshire Constabulary, commented: "CNS was able to demonstrate to us that this doesn't have to be about replacing an entire network; in fact it should be an extremely simple process."

Using a combination of new Cisco software and upgrading existing technology, CNS was able to deploy Federal Information Processing Standard (FIPS) encryption to manage risk, without the need for additional and costly architecture.

Paul Rose, director of strategic development at CNS, explained: "We like a straight-forward solution to a problem at CNS. It is apparent to us that CESG guidelines can be followed through judicious use of firewalls and existing encryption software, such as that provided by Cisco's ASA adaptive security range. It's about adhering to best practice and using levels of encryption that are already part of existing packages."

The project saw a combination of components deployed at Cambridgeshire Constabulary, including:

- CESG Manual of Protective Security
- Encryption levels inherent in Cisco firewalls
- Thin client technology
- Strong authentication methodologies

For Cambridgeshire Constabulary it was reassuring to be able to use tried-and-tested technology to improve the network. Not only was this a budget-friendly approach, but it also meant the integration was less problematic and time-consuming.

Mr Bell said: "We were very pleased to be able to use existing Cisco software for this project. Its proactive confidential architecture gave us the confidence to deploy applications using Cisco commercial-off-the-shelf products."

## Result

This project has enabled Cambridgeshire Constabulary to meet the 'restricted' and 'confidential' networks standards. The project came in under budget and was transparent to the force's users, which meant minimal disruption to day-to-day work during the transition.

Ms Hipperson explained: "We wanted to revamp our network, but through sensible project management we've actually managed to meet regulatory requirements and the strategic needs of the force for the next ten years".

Mr Rose added: "Cambridgeshire Constabulary now has a future-proof and confidential network which will be able to handle new technologies such as wide area network (WAN) encryption and voice over Internet protocol (VoIP)."

■ For further information contact Shannon Simpson, Director of Sales & Marketing, CNS; email [shannon.simpson@cnsuk.co.uk](mailto:shannon.simpson@cnsuk.co.uk); telephone +44 (0) 20 7213 0922 or +44 (0) 7980 859 801 (mobile); or visit [www.cnsuk.co.uk](http://www.cnsuk.co.uk)

PP