



## **Cambridgeshire Constabulary generates savings and simplicity with new Confidential Network**

*CNS enables Police Force to meet Government requirements, without replacing entire network*

### **Situation**

Recent government requirements, to improve confidentiality and security of data transfer by mid 2010, 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.

In the light of this, Cambridgeshire Constabulary took 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 they were to meet the required classification levels.

Led by Tracey Hipperson (Director of ICT), the Constabulary commissioned CNS and 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. For many Police Forces the concern is that meeting the standard will involve replacing or outsourcing their entire networks.

At CNS 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 bodies involved to create a workable and compliant network blueprint.

"Our whole system was in need of a refresh" explains Tracey Hipperson, "so we called in CNS 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 CNS 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 21<sup>st</sup> century policing”.

### **Solution**

Along with internal Police Force IT teams, CNS was invited 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 were able to deploy FIPS encryption to manage risk, without the need for additional and costly architecture.

Paul Rose, Director of Strategic Development at CNS explains, “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 range. It’s about adhering to best practice and using levels of encryption that are already part of existing packages”.

For the Cambridgeshire Constabulary project, CNS deployed a combination of components, 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. Ian Bell explains, “we were very pleased to be able to use existing Cisco software for this project. Their



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 CONFIDENTIAL and RESTRICTED 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. Tracey Hipperson explains, “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 10 years”.

Paul Rose, from CNS commented, “Cambridgeshire Constabulary now has a future-proof and confidential network which will able to handle new technologies such as WAN encryption and VoIP”.

### **Trend**

The experience of Cambridgeshire Constabulary Force is one that is likely to be replicated across the country. There is concern that the new Guidelines from CESG will be costly and time-consuming at a time when Police Forces want to focus energy and resourcing on core police work. By leading the way, Cambridgeshire Constabulary and CNS have proved that a simple, intelligent use of existing technology can resolve the issue efficiently.

### **Contact details**

For Convergent Network Solutions  
Shannon Simpson, Sales & Marketing Director, CNS  
Tel: +44 (0) 7980 859 801  
Email: [shannon.simpson@cnsuk.co.uk](mailto:shannon.simpson@cnsuk.co.uk)

For Cisco;  
Will Owen  
Police and Agencies  
Tel: +447767 005089  
Email: [wowen@cisco.com](mailto:wowen@cisco.com)



## About CNS

CNS is a specialist security and networking consultancy, established in the City of London in 1999. The company is wholly owned by its employees and directors. CNS has built an excellent reputation for information security and networking consultancy & services to our customers across a variety of sectors on a global scale.

CNS's customers vary in size from FTSE 100 and large public sector organisations to SMEs, but are united in the importance of digital information to their business and in their desire for pragmatic, knowledgeable help in securing their systems and data and meeting their connectivity requirements.