

# WE HAVE THE TECHNOLOGY

In order for modern police forces to work efficiently, new technological solutions are needed. **AEP Networks** discuss how their products can help.



**A**EP Networks offers a comprehensive policy networking solution that provides complete security starting at the endpoints and working throughout a network – from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, high assurance IPSec-based VPN encryptors, and hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises, on an international scale.

Protecting the security of data in demanding settings presents challenges to traditional security architectures and solutions. Examples include transporting highly sensitive data over a communications bearer of opportunity, enabling deployed officers to use a partner organisation's communications to facilitate access to his/her host force's data and using a common infrastructure to transport data of different sensitivities.

The Information Assurance (IA) Authorities PITO, CSIA and CESG are working very hard to develop pragmatic security solutions to meet the expanding and increasingly complex problem.

AEP Networks is proud to be able to offer a range of products that provide the level of security assurance and functionality to meet IA standards and policies for Criminal Justice systems.

The following questions and answers illustrate how AEP's security products can help solve some of the most challenging problems, but please feel free to get into contact us on the telephone number below to discuss your force's particular requirements.

**"Can my officers access police confidential data from home?"**

Yes, AEP Net ED Remote is CESG approved to

protect confidential data across all communications media including the internet – "AEP Net Products meet the requirements laid down in CESG Memo 35 ('Remote Access to Public Sector IT systems via the Internet, v2.0') for direct connection to the Internet" – extract from CESG approved Security Procedures.



**AEP Networks is proud to be able to offer a range of products that provide the level of security assurance and functionality to meet IA standards and policies for Criminal Justice systems.**

**"Is it possible to set up a remote operations centre with access to central databases without compromising the security of the infrastructure network?"**

Yes, AEP Net products are approved boundary devices and can be used to extend the accredited

infrastructure into the remote operations centre. Deployments can be rapidly implemented using whatever communications bearer might be available (e.g. ADSL, satellite).

**"Can especially sensitive data be transported over my infrastructure at low cost and minimum management overhead?"**

Yes, AEP SmartGate, a FIPS certified application layer VPN, and AEP NSP, a CCTM certified SSL VPN, are both capable of providing the required network level data separation and offer simple and effective management with a highly competitive cost of ownership.

**"How do I check the integrity of a partner's terminal before allowing them access to my network?"**

AEP NACpoint validates the integrity of terminal equipment accessing the network and, if the application fit is not current or otherwise invalid can place the user into an isolated zone for remediation.

AEP Networks ([www.aepnetworks.com](http://www.aepnetworks.com)) is a privately held company based in Somerset, New Jersey, and London. The AEP Networks Logo is a trademark of AEP Networks, Inc., with registration pending in the U.S. Netilla and SmartGate are registered trademarks of AEP Networks, Inc. All other trademarks or registered trademarks are property of their respective owners. ■

Steve Lewis, V-P Business Development

t: +44 (0)788 783 4016

e: [stephen.lewis@aepnetworks.com](mailto:stephen.lewis@aepnetworks.com)