

IT Management: Security
by Cliff Saran

Monday 21 October 2002

Government security experts urge Whitehall to adopt US cryptography standards

The Government's leading IT security advisors are to recommend that Whitehall departments adopt a US cryptography standard that many commercially available security products fail to meet.

The Communications Electronics Security Group (CESG) is expected to publish a policy document later this month recommending using the US FIPS-140 cryptography standard for non-classified government applications.

Government departments will be urged by the CESG to only deploy equipment validated against the US standard to handle any non-classified data concerning citizens, businesses and e-government applications.

The standard is mandatory in the US for cryptographic systems used for secure communications within government.

No such mandate exists in the UK and, while the CESG is set to recommend the use of FIPS 140 validated equipment, the group cannot demand it.

David Simpson, team leader for cryptographic standards and evaluation at the CESG, said: "We cannot ignore the problem of securing e-government data.

"More than 50% of products that go for FIPS-140 validation are found to have faults."

Problems with cryptographic algorithms and in the documentation required to install the product correctly were the main reasons for products to fail the FIPS-140 validation.

For Simpson, the high failure rate emphasises the value of the standard. "If you are protecting data, you should be using FIPS-140," he said.

Products conforming to this standard could be used to encrypt inter-government communications, such as NHSNET, Government Gateway and protect private keys within a public key infrastructure.

A strong statement from the Government supporting FIPS-140 would also boost compatibility within government communications and with the private sector.

Tom Patterson, a partner in charge of security services at Deloitte & Touche, said FIPS-140 standardisation in the US government has led to a "great cost saving and simpler interoperability".

Ovum analyst Graham Titterington said that by advocating the use of FIPS-140 equipment "the UK government is recognising what other governments around the world are doing", with regards to encryption technology.

Titterington said there had been growing industry interest in FIPS-140 during the past six months. The government has a useful role to play in helping to establish FIPS-140 as a standard for encryption within UK businesses, he added.

Earlier this week, Logica's UK arm opened the first FIPS-140 commercial evaluation facility outside the US.