

PANELLIST'S STATEMENT: DR JAMES HODSDON, CESG

Dr James Hodsdon,
Room 2/0506,
Communications-Electronics Security Group,
Fiddler's Green Lane,
CHELTENHAM
Gloucestershire
GL52 5AJ
United Kingdom

Tel: +44-1242-221491 ext 4195

The Communications-Electronics Security Group (CESG) is the UK government's lead authority on Infosec technical issues; administratively it is part of the Government Communications Headquarters (GCHQ). During the UK's 1994 Review of Protective Security, which looked at security issues throughout the government and armed forces sectors, CESG took an active part in meshing best practice in the Infosec areas, which already included several examples of "graduated response", with the new government-wide guidelines on risk management.

Since 1994, CESG has been a major contributor to the follow-through work generated by this Review. This work has been one of the chief tasks of the policy team which I head up, and has led to a complete overhaul of the UK government's top-level policies and guidance on IT and communications security. The outcome has been new documents which aim to describe the risks, the issues and the solutions in terms which **any** government user can relate to. This is important because our customer community is no longer restricted to the classic "Classified" users. The new classification ("protective marking") system in the UK intentionally embraces **all** official assets needing protection. We have to generate guidance that reflects all the different risks not just in military but also in normal public service environments. This harmonisation process has been a highly beneficial sanity check; too many of the rules devised for good reason in the old classified era had become fossilised and were only marginally relevant to today's government office environment and technologies.

There is little legislative framework or enforcement apparatus surrounding Infosec practice within the official sector in the UK. Generally speaking, new protective security policy cannot simply be imposed from the centre. Any proposed new Infosec policy has to be explained and demonstrated to be a credible realistic method for managing the risks. It also has to be endorsed by a committee system in which the security authorities and the user communities (military and civil) all have a voice. This consensus system, with all sides "buying in" at the start, is what gives the policies their practical strength.

In the risk management era, one of CESG's primary tasks is to explain to users what the Infosec risks are, and what the choices are for managing those risks. This is a far cry from the old days of "These are the rules and this is the kit which the rules dictate". It is also the only way to go when technology and risks are in constant change.