Zenith loses Ministry of Defence contract

Following the security incident in January (see March issue of *CFS*), the UK's Ministry of Defence (MoD) has reviewed its policy of laptop purchasing and has consequently cancelled a multi million pound deal with Zenith Data Systems which was awarded last October. Results of the enquiry into the theft of a laptop containing classified Gulf War plans resulted in a new requirement that all laptops must have removable hard disks.

MoD procedures for sensitive data require the information to be stored on removable media. Traditionally laptops procured by the MoD include normal Zenith and Toshiba systems, with Grid Systems being purchased for 'secure laptops'. Following the review, all laptops must now be 'secure'.

The original October deal was for the Zenith Slimport. In these the disk is housed under the keyboard and is therefore inaccessible. Zenith then modified an older, heavier model which it hoped would be an acceptable replacement, but the contract eventually went to Compaq's removable hard disk version of its LTE 286.

UFO-hunters infiltrate US government computers

In search of data on possible UFO sightings in US wheat fields, a group of British hackers broke into a US Government data network in October 1990. The intrusion was apparently not discovered until January of this year. The network was operated by the US Agriculture Department's Animal and Plant Health Inspection Service Known as APHIS, it inspects imports to the US of plants and animals and connects 500 terminals at its headquarters with more than 175 terminals at its 40 field offices.

The hackers gained access to the APHIS network through the US Sprint Communications TeleNet public network. They used relatively sophisticated file search methods and appeared to have access to the source code used with the APHIS network. They were active in the APHIS Jefferson City, MO, and Wilmington, NC, field offices as well as in the Hyattsville headquarters segment of the network. APHIS representatives indicated that, shortly after the unauthorized access to the network was discovered, the passwords in use were changed and more complex user personal identification codes were installed.

Belden Menkus

Sun designer admits hacking

Robert Gilligan, a senior software designer at Sun Microsystems, has pleaded guilty to obtaining confidential customer information from Pacific Bell. He will serve three years probation and pay the telephone company $25 000 in compensation. As part of the plea bargain, Gilligan has agreed to help US authorities bring prosecutions against Kevin Poulsen and Mark Lottor, also accused of the eavesdropping offences. Gilligan has additionally offered to help the victims of the hack plug the gaps in their network security.

Gilligan, Lottor and Poulsen were charged last year (see April 1990 issue of *CFS*) on 19 counts of using personal computers, stolen Pacific Bell equipment and stolen access codes to tap into government and telephone network computers to obtain classified military documents and FBI information on associates of the late Philippine president Ferdinand Marcos. If convicted on the original charges, Gilligan faced up to 20 years in prison and a $30 000 fine.

Gilligan's attorney maintains that his client fell in with bad company who wanted to use his networking experience. Gilligan has admitted accessing the US Army's Masnet Computer network, but claims that he got no further than the login screen which warned against unauthorized entry. This he printed off and later gave to Poulsen. Federal officials say that the