Ransomware Attack on Eurofins Forensic Services (EFS)

I write further to my letter of 11 June to update you on progress.

Following extensive work to recover and rebuild systems and data, provide assurance that rebuilt EFS systems and recovered data were unaffected and ensure that any necessary disclosure could be made in cases in the Criminal Justice System (CJS), the decision was taken on 23 July to allow EFS to recommence processing work for the CJS. This decision was taken by a National Police Chiefs’ Council (NPCC) led platinum group, which relied on a detailed assurance map, which had been prepared with input from EFS, Dell Secureworks (which is a cyber incident response company certified by the National Cyber Security Centre (NCSC), commissioned by EFS), NPCC, NCSC, the Crown Prosecution Service (CPS), the Office of the Senior Presiding Judge, the United Kingdom Accreditation Service (UKAS) and myself.
During the c. 7 weeks that EFS was unable to provide forensic science services to the CJS, significant backlogs of work were accumulated and will take some time to clear, although precise timings will vary by discipline. This process is being overseen by the NPCC’s Forensic Marketplace Gold Group, supported by the commercial team from the Transforming Forensics programme.

NCSC has visited all major forensic science providers to provide generic advice on information security as well as specific advice relating to the form of ransomware deployed in this incident. I will shortly be commencing a consultation on incorporating information security requirements, drafted by NCSC, into my Codes of Practice and Conduct. Although information security could be argued not to be a “forensic science quality” issue, the impact of any failure is such that application of appropriate standards across the entire sector (including private providers, Government laboratories and policing) is important.

Yours sincerely

[Signature]

Dr Gillian Tully

Tel: +44 (0)121 2003830
Email: FSR enquiries@homeoffice.gov.uk