CONFIDENTIAL

18th December Meeting with IT Personnel 11.15-12.15pm
Independent Reviewer Sir Muir Russell (MR),
Director Information Services Jonathan Colam-French (JCF),
ICT Systems Director Iain Reeman (IR),
ICT Policy Manager Steve Mosley (SM)
(Mike Salmon unable to attend due to illness)
Notes taken by Lisa Williams (LW)

MR general outline: his intention would be to collect written evidence from critics and the CRU team – he did not favour court room style inquisitions. This was a scoping meeting, not intended to take definitive statements.

Timeline of events discussed.
SM – became aware of the email hack/leak on 18 Nov.
JCF aware from 17 Nov but thought it related to a specific dataset that had been previously accessed. (3 or 4 months prior there were many FOI requests dealing with CRU dataset. CRU had provided a particular station dataset to an American researcher. This was placed on an open ftp share which was therefore a risk).

By 18 Nov clear it was a different set of data. Over 1000 emails in different files. One of files published is a compacted file

19 Nov
SM - Mike Salmon administrator for CRU data did a preliminary investigation. Seemed to be a targeted hacking of back-up server used by all CRU staff and researchers. Looked like a sophisticated hacking attempt.

IR – SCI take a different approach to their IT to the rest of UEA.
In CRU the desktop PCs and laptop PCs don't talk to each other, and they back-up to different servers. Does server contain all the data? IR – yes, but in different areas.

Was some info kept separately? SM - Yes, on laptops. Difficult to know – need access to back-up server which is held by police.

JCF - Backup server does not contain all of the data. Hard discs are used for storage. Hard disc may be at home and at work. So may well not have been backed up as part of the CRU back up regime.

JCF – full CRU data set held electronically can be made available and can be accessible. However, part of it may not be electronic. Working data, emails, more transitory working information – may be stored in other locations.

JCF – For example Keith Briffa took home emails that were subject to FOI to ensure their safekeeping.

MR – There is a need to build confidence. Ideally he would like to give CRU an opportunity to expose what information they had and what they did with it. Then expose this to the judgement of whether what they did was reasonable given the time and also best scientific practice at the time.

SM –back-up server was taken out of action 20 Nov. Police took it away on 24th. Appears that hackers hacked 5 Oct. Upload to Realclimate website on 16 Nov. What happened in the interim?

JCF – hackers were in from Oct (we believe they offered info to BBC in early October) and again mid Nov. Not sure if they were continuously hacking in the meantime.

JCF – Data potentially accessed is estimated to be up to 5 terabytes once uncompressed on the server (substantially more than has been published). What is on the website is a selection of the overall data. Data comprises raw station data, evidence of what was happening to the data in analysis, emails and comments. Configuration of back-up server was unfortunate as it did not remove deleted emails. Centrally, UEA emails are held for only a month and then deleted permanently. Not the case on the CRU backup server.

MR – Hack or a leak?
SM – the attack did look targeted. Police are looking at both options.
IR – highly skilled individual must have done this. Two options – simple attack by internal person or sophisticated external attack.

JCF – back up was compressed, so whoever did this would need software to restore files. Could have been a staff member in CRU, or someone using a CRU computer. Much more difficult/sophisticated to do this externally. What was published on website included an "FOIA folder" – which was not a replication of what was on the back-up server. This is something which had been put together in this way by whoever published the data. .

Some of data available was mid Oct. Someone had access again in Nov.
Ie Hacker did it more than once. Perhaps someone had continuous access.

JCF on FOIA – many requests, 60 requests over 1 weekend. An approach was agreed with ICO, a month before the Oct date, as to how to handle these requests.

16 Nov there was an attempt to put some data onto Realclimate website (used by climate researchers). Attempt spotted by administrator at Realclimate who informed CRU. Mike Salmon then conducted an investigation.

Data might have been available elsewhere at same time. Russian website was main vehicle for dissemination of the published emails.
Why did BBC reporter know on 12 Nov (post hack) and prior to Realclimate alert?

MR – concern that there could be more to come. Month of October must have been a productive time for the hackers.

IR – laptops, PCs taken by police.

External drives which contain data could still be held at home – may not be with police.

MR would like to give team opportunity to demonstrate openness, frankness in their handling of the data – it will be difficult to demonstrate integrity but not impossible.

Notion that part of the data was selected, suppressed, deleted is damaging to UEA's reputation.

Have hackers massaged the data?
JCF No evidence to suggest it's been added to – other than just a selected sub-set published.

Have researchers changed it? To be assessed.

IR – Since the hack, UEA has employed an external security company (same one as police) to advise on/ ensure IT security and UEA's IT infrastructure, including SCI, and including penetration tests. Counterterrorism branch of the police are also advising.

MR - Will CRU's IT be made to comply with UEA practices? ET (UEA's Executive Team) will ultimately decide.

JCF – UEA has a distributed IT support structure. As a "Faculty University", Faculties have the scope to run things their way.
Central IT provide policies but difficult to force Faculties to adhere to them.
Internal auditors are looking at this.