

87123-SV17

To: Mr. Stockton Vandermaar.
Requesting Officer: Dr. Duncan Waterhouse, UKGC Research.
Subject: LIBRIS evaluation.

Mr Vandermaar,

Enclosed is the basic outline of the systems and their evaluation products. As may be evident, some of the equipment has additional capabilities not originally planned for in the LIBRIS specification that are relevant to the UKGC (e.g. installation of CheyTac sniper software on the PDA).

As per OGCbuyingsolutions specification I have noted evaluation systems and where there is a chance of suppliers gaining market advantage should adoption be taken up.

Also enclosed is a report which explains the significant price tag. This hardware is non-standard and represents innovation on existing military technology. It will enable UKGC personnel to perform their functions in IT-hostile environments and provide additional options to personnel in the field.

Ironically, software costs have been driven down by selection of open-source software; while this may appear to fly in the face of OGC/HMG preference, there is precedence for doing so provided by MOD.

The specification also enables them to work in the field longer, with increased communications security and in a more environmentally-mindful manner than with existing equipment.

If you have queries on any aspect of this purchase order, please don't hesitate to contact me.

Regards,

Duncan Waterhouse Ph.D, CISSP, FBCS.

Item 1:

1 x Customised TerraLogic Toughnote M15 option with 2Gb RAM and solid state drive.

<http://www.terralogic.co.uk/files/Toughnote%20Series%20M-15%20Specifications.pdf>

The following options have been selected:

- 1.6Ghz processor
- 15" 1024x768 touchscreen
- 2Gb RAM
- 500Gb solid-state drives. TerraLogic typically offer 32Gb SSDs but functions within the same system footprint and without compromise of other certifications. (*On evaluation with Fujitsu Systems UK; may offer market advantage to FSUK and TerraLogic – DW*)
- MIL-STD-810F/EMI461E (allows rugged operation and resists electromagnetic interference; especially from antenna and radar mast radio frequencies as well as EM/RF jamming by other hostiles).
- TEMPEST AMSG 784/788 – Dampens compromising emanations to pickup at effective 20m open range (NATO Zone 1 rating) for Van Eck radiation/side-channel attack. Effective against ECHELON/CARNIVORE/ONYX class surveillance; without TEMPEST, snipers with ELINT/SIGINT training can pick up signals beyond 100m distance with ELINT/SIGINT tools.
- 2x 6600 M2E cell used instead of standard Li+ cell. Effectively self-powering due to Faraday energy-harvesting and double typical battery life even if unit is at rest with 7x output and 50% weight of typical cells. Cell recharge from 15 minutes of physical movement carrying unit. (*Batteries on evaluation from M2E systems, Idaho. M2E supply cells for the US Patriot laptops and TerraLogic have now initiated contact with a little help - DW*)
- 1.2Mpx webcam & Sphinx-4 speech recognition software. Compatible with Britannia Rhino comms package; requires 30 hours training for full SR effectiveness.
- Internal components include
 - Fax modem
 - Bluetooth
 - Wireline; Wireless LAN (WPA-PSK) & Fibre-optic connectivity.
- Removable DVD-RW can be swapped out with secondary battery.
- All other elements to match Toughbook specification.
- Customised Knoppix/WINE OS configuration with AES/TwoFish authentication and 2048-bit disk encryption. Appears identical to Windows with increased security, additional software options, full Windows compatibility and grossly reduced costs. (*Typical Windows & Office GAP package will cost you about £750 and needs clearance by CESG (4 weeks+); this costs you nothing and gives you increased security and FIPS140-2 encryption. Precedent for HMG open-source use with the QUASIMODO project co-sponsored by MOD and Qinetiq – DW*)
- Other software includes GPS modeling and RFID inventory database.

Recommended supplier: TerraLogic (under existing MOD contract).

Auxiliary suppliers: Fujitsu Systems UK (under OGC framework)
M2E Systems, USA (under OGC framework)
Knoppix.de (under MOD framework)

TCO: £2000

Amortisation: 3 years.

Operational Life Cycle: 10 years +

Item 2:

1 x Toughnote DA05-M Rugged Handheld PDA

<http://www.terralogic.co.uk/files/Toughnote%20DA05-M%20Rugged%20PDA%20Specs.pdf>

Win CE.NET Mobile Phone 5.0

GPRS/GSM/GPS/Bluetooth/Wifi options chosen. GSM phone options enabled.

1.2Mpx Camera

M2E cells x2 (effective running of 5 days between recharge; 15 minutes movement recharges cell); unit now weighs 330g. *Batteries on evaluation from M2E systems, Idaho.*

Phillips/Vodafone Near-Field Communications card. On evaluation from Vodafone UK.

Software applications

- CheyTac sniper computation
- GPS modelling
- RFID database
- Personal Information Manager.
- Twofish authentication & disk encryption (faster than AES and to same standard).
- AES authentication & disk encryption.

All other items to match the specification.

Recommended supplier: TerraLogic (under MOD contract).

Auxiliary suppliers: M2E Systems, USA (under OGC framework)

TCO: £1200

Amortisation: 3 years.

Operational Lifecycle: 10 years +

Item 3:

Vodafone HMG communications contract.

These is required to run phone services on the PDA and test compatibility/security with public systems as well as provide alternate communications other than military systems. It is my intention to evaluate the effectiveness of this equipment for civilian and military arenas and request Ptmarmigan access from Brigadier Kincaid pending approval of this purchase.

Recommended supplier: Vodafone UK (under HMG contract)

Item 4:

50 passive RFID tags fitting Topaz specification (these are encrypted using existing KASUMI technology which can be compromised by ELINT/SIGINT and are therefore unsuited for field use). These are to be used as proof-of-concept tests of NFC and Bluetooth and evaluate the effectiveness of the RFID database in identifying multiple RFID signals and provide meaningful inventory data.

Any RFID implementation would require rewriting the tags to meet a different encryption standard. This has been discussed in other reports.

Recommended supplier: Siemens Electronics (under OGC contract)

TCO: £50.

Amortisation: 2 years.

Operational Lifecycle: 4 years.

Evaluation Report on LIBRIS specification

LIBRIS is deliberately above specification for typical HMG/military systems from the nature of the threats and risks faced by UKGC systems and personnel. LIBRIS is a response based on existing technologies. Future versions may incorporate other UKGC findings to innovate further and to provide additional resistance against ELINT/SIGINT.

Following events in January where a Ga'ould AI (current designation 'CYNTHIA') was able to broadwave jam the majority of systems, hack into adjacent systems using side attacks (use of incidental Van Eck radiation from screens to pick up signals and co-opt them) and neutralise UKGC systems by rapid electromagnetic overwriting of magnetic hard drives, it was established UKGC were vulnerable to existing ELINT/SIGINT tactics and threats beyond current Earth-standard technology.

The very nature of UKGC work means systems cannot afford to be compromised by dust, water, increased radio frequency activity or being knocked around by military personnel. The risk of hacking UKGC systems is readily apparent and the nature of our work poses extraordinary risk to the liberty of UK citizens and other nations. Recent events have only served to highlight this.

MIL-STF-810F

The current military standard for physical and environmental resilience used by British Army.

SSD (solid state drives)

SSD has been proven to have significantly greater resilience compared to existing magnetic disk media. Though currently more expensive due to limited realization of this technology, prices will significantly reduce and storage will significantly increase in the next 18 months.

With hardcoded software to prevent damage to specific sectors (wear levelling), SSDs have guaranteed physical resilience and increased longevity (no need for hard drive replacement during accounting life, drives will last effectively 20 years before needing to replace). Other advantages of SSD include consistent performance, faster start up (under 10 seconds compared to 30 seconds – 1 minute for UKGC laptops) and reboot times as well as minimal noise, reduced weight and increased physical resilience.

EMI461E

Devices with this standard resist electromagnetic (EM) interference originating from radio frequency (RF) and other sources of EM interference. Field operations may place devices in areas of increased EM activity (unshielded communications/radar is one obvious example, solar flare activity is a little more obscure but still valid given current theatres).

TEMPEST AMSG 784/788

This is a NATO recognized standard of protection against compromising emissions (Van Eck radiation) that allow side channel attacks and infiltration of systems (colloquially called 'phreaking'.) which can be typically carried out through rudimentary communications experience.

Twofish encryption.

This encryption system is commercially viable despite being open-source. It has been used in a variety of industrial, law-enforcement and military theatres. While AES has been preferred by NIST for encryption, Twofish has demonstrated significant resilience against brute-force attacks and has maximum interoperability between Windows, Linux and Mac OS. It is relatively simple to switch from Twofish to AES (and Knoppix allows you to do so).

M2E

Motion to Energy cells recharge using Faraday principles to convert kinetic energy into electrical energy for powering the device. 15 minutes physical exertion will recharge a battery to

90% of capacity. Manufacturers claim seven-fold output, practical experience indicates slightly less but will negate need for battery expenditure over accounting lifecycle and exceed sustainability targets imposed by Whitehall under the European Union WEEE directive.

NFC

Near Field Communications is the technology used in Oyster cards to provide transactions for users; this technology will be useful in identifying field presence of assets and additional authorization for communication of data while conserving battery power. The proximity of the NFC field makes it suitable for identifying RFID tags on an individual, allowing rapid system identification or inventory.

Recommendations:

1. Adoption of LIBRIS standard on successful evaluation. Criteria for evaluation include:
 - 1.1. MIL-STF-810F compliance.
 - 1.2. Improved TEMPEST protection (NATO Zone 1) compared to current UKGC systems which are not so protected with a few notable exceptions.
 - 1.3. Test to evaluate unit against EMI461E. This can be simulated by using the unit near a comms relay or overhead power pylon.
 - 1.4. Evaluation of software to ensure speech-recognition is effective and that GPS data can be mapped effectively.
 - 1.5. Successful penetration testing of systems by experienced independent hacker (I am happy to suggest any UKGC personnel with comms/computing personnel as suitable).
 - 1.6. Evaluation of long-term field operations based on battery usage.
 - 1.7. Communication using Near Field Communications, Bluetooth and passive RFID tags.
2. An immediate audit of all UKGC sites to validate security against ELINT/SIGINT. It is apparent that a number of recent security breaches have been carried out by those with insider knowledge and the computer system has suffered a series of significant power losses which would allow any attacker to implant key logging devices on workstations.

Glossary:

AES – Advanced Encryption Standard
CARNIVORE – US EM/RF surveillance.
ECHELON – UK EM/RF surveillance.
EM – electromagnetic radiation
ELINT – Electronics intelligence
FIPS140-2 – Government standard for encryption of data on IT systems.
GAP – Government Accredited Package
Mpx – Megapixel (1 million pixels)
NFC – Near Field Communication
ONYX – Swiss EM/RF surveillance.
RF – Radio Frequency
RFID – Radio Frequency Identification
SIGINT – Signals intelligence
SSD – Solid state drives
TCO – Total Cost of Ownership
WEEE – Waste Electronic & Electrical Equipment
WPA-PSK – WiFi Protected Access – Pre-Shared Key