From: [redacted]
Date: 13 June 2008
GCHQ Reference: A/9014/9105/55

Sian MacLeod

Mariot Leslie

Foreign Secretary

ISA-94: APPLICATION FOR RENEWAL OF WARRANT GPW/1160 IN RESPECT OF ACTIVITIES WHICH INVOLVE THE MODIFICATION OF COMMERCIAL SOFTWARE

ISSUE

1. GCHQ seek a renewal of warrant GPW/1160 issued under section 5 of the Intelligence Services Act 1994 in respect of interference with computer software in breach of copyright and licensing agreements.

TIMING

2. Warrant GPW/1160 is due to expire on 7 July 2008. Signature is requested by **4 July.** If renewed, the warrant will next expire on 7 January 2009.

PREFERRED OPTION

3. That the Secretary of State issue the warrant. If the Secretary of State agrees, he should sign and date the warrant instrument (GPW/R/167, immediately below this submission and flagged "Reference Here").

BACKGROUND

4. GCHQ's success as an intelligence agency is founded on technical knowledge and creativity. In particular this may involve modifying commercially available software to enable interception, decryption and other related tasks, or "reverse engineering" software (this means to convert it from machine readable code into the original format, which is

then comprehensible to a person). These actions, and others necessary to understand how the software works, may represent an infringement of copyright. The interference may also be contrary to, or inconsistent with, the provisions of any licensing agreement between GCHQ and the owners of the rights in the software.

5. Where this work is being carried out in support of a specific intercept operation or a specific computer network exploitation (CNE) operation, the preparatory work can often be taken to be included in the legal authorisation that applies to that operation. The provisions of RIPA and ISA apply in most cases to all such enabling activities. This will be the case for any software destined for operations covered by RIPA warrants and by operations carried out under the ISA section 7 authorisation held by GCHQ for CNE activities where the effect is overseas. Unless specifically authorised, however, it will not be the case for specific operations carried out under ISA section 5 warrants, or in those instances where the activity is being carried out not as preparatory to a specific operation but as part of GCHQ's continuing efforts to maintain its technical knowledge base and develop future exploitation opportunities.

6. In some other cases similar work is being carried out by CESG as part of Information Assurance (IA) vulnerabilities research. A variety of software products may be "reverse engineered" in order to identify and understand potential security vulnerabilities. Authorisation will not normally be sought from the supplier or copyright owner.

7. There is a risk that in the unlikely event of a challenge by the copyright owner or licensor, the Courts would, in the absence of a legal authorisation, hold that such activity was unlawful and amounted to a copyright infringement or breach of contract. The purpose of this warrant is to provide authorisation for all continuing activities which involve interference with copyright or licensed software, but which cannot be said to fall within any other specific authorisation held by GCHQ and which are done without the permission of the owner.

8. Under the terms of this warrant, the majority of products examined since last renewal have been in support of CNE operations, while a number were investigated in support of CESG's IA work and to enable police operations. In each case it was necessary

to use this warrant as the product licence explicitly forbade reverse engineering.

CNE

9. The products that were studied for CNE purposes included vBulletin web forum software, widely used to run terrorist web forums. Software reverse engineering (SRE) has enabled recovery of user credentials from web traffic and database content, research into vulnerabilities that can provide access into such forums, and investigation of opportunities for modifying a forum in order to mount attacks against target users. Similar inroads into Invision Power Board, another web forum product, have also been possible. Vulnerabilities in terrorist forum hosts using host management software CPanel have likewise been identified through SRE, while vulnerabilities identified in the PostfixAdmin software used by a targeted Internet Service Provider have allowed modification of an ISP site and a subsequent attempt at implant delivery.

10. GCHQ's CNE operations against in-country communications switches (routers) have also benefited from SRE. Capability against Cisco routers developed by this means has allowed a CNE presence on the Pakistan Internet Exchange which affords access to almost any user of the internet inside Pakistan. Our presence on routers likewise allows us to re-route selected traffic across international links towards GCHQ's passive collection systems.

11. Personal security products such as the Russian anti-virus software Kaspersky continue to pose a challenge to GCHQ's CNE capability and SRE is essential in order to be able to exploit such software and to prevent detection of our activities. Examination of Kaspersky and other such products continues.

12. SRE work also supports long term CNE research, which needs to be done to strengthen GCHQ's technical knowledge base and to sustain and improve its future Sigint capability, in particular to be able to respond effectively to changing target practices. In addition, the SRE courses run at GCHQ not only aim to train the students in SRE techniques but also offer an opportunity for them to examine new products or those that are of interest but have yet to be reverse engineered.

Information assurance

13. During the period under review CESG analysed a number of products that are or may be used by a wide range of government departments and officials. Examination of Microsoft's Mobile Data Manager, a management system for mobile devices such as PDAs, has assisted with evaluation of this product for government use, while SRE of a product in use by GCHQ for electronic data records management has contributed to the development of protection against electronic attack.

14. CESG have also analysed examples of malware, the malicious software such as viruses or worms with which computers are deliberately infected in order to cause harm. Malware is unconventional by design and its effect on a system can vary greatly depending on environmental factors or the attackers' intent. It is therefore important that we understand in great detail how a computer's operating system is affected and SRE of monitoring tools FileMon and RegMon, for example, has afforded significant insights into how malware can bypass these logging tools. Equally, malware is often delivered by targeting vulnerabilities in applications such as Microsoft Office or Adobe Acrobat, and the role of SRE in identifying such vulnerabilities is critical to understanding and counteracting the risks posed to government departments.

GCHQ assistance to law enforcement and intelligence agencies

15. GCHQ's unit providing specialist technical support to the law enforcement and intelligence agencies, the National Technical Assistance Centre (NTAC), has used this warrant to reverse engineer Acer eDataSecurity, allowing for the decryption of material relating to a high profile police case, and CrypticDisk, allowing for the decryption of material relating to a child abuse investigation. Software reverse engineering against commercial encryption products continues to play a crucial role in developing new capability for NTAC forensics.

RISK ASSESSMENT

16. The risk of any interference such as that described in paragraph 4 becoming apparent to the owner of copyright or licensing rights is negligible.

LEGAL ISSUES

17. When this warrant was originally submitted to the then Secretary of State, there was believed to be no precedent for the use of a warrant under section 5 of the Intelligence Services Act 1994 in relation to intellectual property as embodied in copyright or licensing agreements. However, the Intelligence Services Commissioner was consulted in 2005 on the applicability of a warrant in these circumstances and he was content that section 5 could be used to remove such liability.

18. I consider it necessary that the actions specified in the warrant be taken to assist GCHQ in carrying out its functions under section 3 (1) (a) of the Intelligence Services Act 1994, which in this instance are exercisable in the interests of national security and the economic well-being of the United Kingdom. I further consider that the taking of the action is proportionate to what the actions seek to achieve and that what the actions seek to achieve could not reasonably be achieved by other means. Information obtained as a result of the actions will be subject to the arrangements in force under section 4 (2) (a) of the Act.

19. GCHQ legal advisors have checked the text of the attached instrument and are content that it conforms in all respects with the Act. I have personally checked the attached instrument and certify that it conforms in all respects to the details given in the submission.

[redacted] GCHQ

(Please phone [redacted] 92 (Brent) for procedural queries)