BULLRUN CoI – Briefing Sheet

Introduction

1. The ability to exploit targets' encrypted communications is extremely fragile and is often enabled through sensitive ECI programmes. The need to take additional measures to protect that capability has long been recognised. Currently, virtually all decryption is carried out by PTD (ARTHUR) processing with decrypts going to the IIB in the NOCON CoI; some decrypts are placed in the ENDUE CoI due to the sensitivity or fragility of the exploitation capability.

2. In recent years there has been an aggressive effort, lead by NSA, to make major improvements in defeating network security and privacy involving multiple sources and methods, all of which are extremely sensitive and fragile. These include: Computer Network Exploitation (CNE); collaboration with other Intelligence Agencies; investment in high-performance computers; and development of advanced mathematical techniques. Several ECI compartments may apply to the specific sources, methods, and techniques involved.

3. Making the best use of these new capabilities requires that decryption processing be widely deployed beyond PTD and the results of that processing be available to a wide range of analysts. This inevitably makes it harder to protect this sensitive and fragile capability and we need to counterbalance this by introducing measures to control access to this material and heighten awareness of the sensitivities amongst those who have access.

4. To achieve this, NSA has introduced the BULLRUN CoI to protect our abilities to defeat the encryption used in network communication technologies. This covers both the "fact of" a capability against a specific technology and resulting decrypts (which may be either plaintext or metadata (events). GCHQ is also introducing BULLRUN. (CSEC, DSD and GCSB are expected to do likewise.)

Control Authority

5. The BULLRUN CoI is owned by [redacted] for Penetrating Target Defences (PTD). Authority to manage the CoI is delegated to [redacted] (currently [redacted]) and [redacted] ([redacted], currently [redacted]).

6. It is imperative to protect the fact that GCHQ, NSA and their Sigint partners have capabilities against specific network security technologies as well as the number and scope of successes. These capabilities are among the Sigint community's most fragile, and the inadvertent disclosure of the simple "fact of" could alert the adversary and result in immediate loss of the capability. Consequently, any admission of "fact of" a capability to defeat encryption used in specific network communication technologies or disclosure of details relating to that capability must be protected by the BULLRUN COI and restricted to those specifically indoctrinated for BULLRUN. The various types of security covered by BULLRUN include, but are not limited to, TLS/SSL, https (e.g. webmail), SSH, encrypted chat, VPNs and encrypted VOIP. The specific instances of these technologies that can be exploited will be published in a separate Annexe (available to BULLRUN indoctrinated staff).

7. In addition to the specific technologies that GCHQ or its Sigint partners are able to exploit, the methods used to achieve the exploitation must also be protected. These include support from other organisations, both internal and external to GCHQ. Access to BULLRUN does NOT imply any "need-to-know" the details of sources and methods used to achieve exploitation and, in general, there will be NO "need-to-know". Requests for access to information on sources and methods should be sent to OPC-SEC; if considered appropriate, this access may require clearance for certain ECIs.

8. BULLRUN material, data, and details must be protected with the use of the BULLRUN CoI and be marked with the label "BULLRUN," in addition to the required privacy marking and other descriptors. Use of the BULLRUN marking is restricted to GCHQ and its Sigint 2nd Parties.

Access and Security

9. Requests for access to the CoI must be sponsored by a GC8 or above and must be accompanied by a business case outlining the "need-to-know". Access for contractors will be limited and will require a strong business case; such requests should be discussed with the CoI Authority's delegates before submission. Requests for access are to be sent by email to PTDAccesses.

10. Knowledge of BULLRUN information and access to the BULLRUN CoI will only be granted to indoctrinated individuals.

11. It is the responsibility of sponsors (or their successors) to notify [redacted]

when an individual no longer require access to BULLRUN.

Handling Procedures

12. Owners of BULLRUN materials are responsible for correctly marking the information and for ensuring that it is handled according to guidelines for protecting classified or COI information.

13. Reports derived from BULLRUN material shall not reveal (or imply) that the source data was decrypted. The network communication technology that carried the communication should not be revealed.

14. Further dissemination, other than in product reports, of any data or information derived from BULLRUN data must be thoroughly justified and receive prior approval from [redacted].

15. All questions or concerns regarding BULLRUN material and information should be directed to [redacted].

Protective Marking Guidance

The following offers some guidance on Protective Markings (PM) for BULLRUN material. Questions regarding PMs can be directed to the CoI Authority's delegates.

At SECRET STRAP1 COMINT AUSCANZUKUS EYES :

The fact that GCHQ has unspecified capabilities against network security technologies eg TLS/SSL, HTTPS, SSH, VPNs, IPSec. NB capability does not necessarily equate to decryption capability.

At TOP SECRET STRAP1 COMINT AUSCANZUKUS EYES :

The fact that GCHQ or its 2nd Party partners has some capability against the encryption used in a class or type of network communications technology. For example, VPNs, IPSec, TSL/SSL, HTTPS, SSH, encrypted chat, encrypted VoIP.

At TOP SECRET STRAP2 COMINT BULLRUN AUSCANZUKUS EYES :

The fact that GCHQ or a 2nd Party partner has a capability against a specific

encrypted network security technology – see Annexe for details. (At a minimum, specific capabilities may be protected by additional ECIs and restriction on “Eyes”.)

The fact that GCHQ or its partners exploits specific encrypted network communications – see Annexe for details. (At a minimum, specific capabilities may be protected by additional ECIs and restriction on “Eyes”.)

Decrypts (plaintext or derived events / metadata) obtained from BULLRUN capabilities. (At a minimum, specific capabilities may be protected by additional restriction on “Eyes” and, in a few cases, additional ECIs.)

GLOSSARY

(U) HTTPS – HTTP traffic secured inside an SSL/TLS session, indicated by the https:// URL, commonly using TCP port 443

(U) IPSEC -- IPSec, or IP Security, is the Internet Engineering Task Force (IETF) standard for layer 3 real-time communication security. IPSec allows two hosts (or two gateways) to establish a secure connection, sometimes called a tunnel. All traffic is protected at the network layer.

(U) SSH – Secure Shell. A common protocol used for secure remote computer access

(U) SSL – Secure Sockets Layer. Commonly used to provide secure network communication. Widely used on the internet to provide secure web browsing, webmail, instant messaging, electronic commerce, etc.

(U) TLS – Transport Layer Security. The follow-on to SSL, SSLv3 and TLSv1.0 are nearly identical.

(U) VoIP – Voice over Internet Protocol. A general term for the using IP networks to make voice phone calls. The application layer protocol can be standards-based (e.g., H.323, SIP), or proprietary (e.g., Skype).

(U) VPN – Virtual Private Network. A private network that makes use of the public telecommunications infrastructure, maintaining privacy via the use of a tunneling protocol and security procedures that typically include encryption. Common protocols include IPSEC and PPTP.