

(49)

~~CONFIDENTIAL~~

49

25/2/46

20, December 1985

Director
National Security Agency
Fort Meade USA

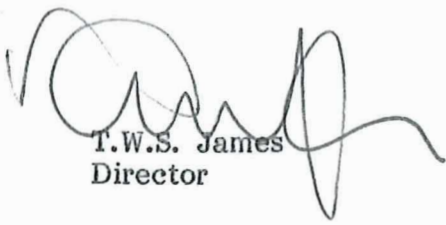
EXPORT LICENCE FOR CRAY XMP-22 TO DSD

Dear Sir,

I am pleased to enclose (Attachment A) a statement of the end-use to which the CRAY XMP-22 supercomputer will be put by DSD together with the security procedures which we will employ. I should like to confirm that DSD will fully observe these conditions and will promptly consult with you if any suspicious activities occur with the use of the supercomputer.

The contractor, Cray Research Incorporated (CRI) has full responsibility for the transport of the supercomputer, customs reception, and local travel. I have been assured by CRI officials that the necessary certificates with respect to this export have been lodged by CRI with the US Department of Commerce; apparently much of this documentation was linked with that provided for the export of a supercomputer from CRAY US to the European Medium Range Weather Forecasting Centre, Reading UK.

Yours sincerely



T.W.S. James
Director

~~CONFIDENTIAL~~

Declassified by ASD - 15/03/2022

Attachment A to
25/2/46 of
20 December 1985**SUPERCOMPUTER END-USE AND SECURITY PROCEDURES STATEMENT**

Name of Importer-End-User: Defence Signals Directorate (DSD)

Address: Victoria Barracks, St Kilda Road

City/Country: Melbourne, Victoria, Australia

DSD attest to the following in connection with the proposed export of a super-computer.

End-Use Description

1. DSD will use the Cray XMP-22 for Government research related to intelligence matters.
2. There will be no retransfer of the system or change in use or method of use without prior notification and approval by the United States Government.

Security Procedures

1. The Cray computer will be installed in the DSD headquarters building. The building is a secured government installation under 24-hour guard protection. All uncleared visitors are escorted at all times. No COCOM proscribed nationals will be admitted into the building.
2. Appropriate checks will be employed to ensure that access to the computer centre is limited to authorized persons. The bona fides and legitimacy of purpose will be established for key computer centre personnel and others who would have access to the full computational capability of the computer before such access is granted.
 - (a) Computer Centre - The computer operating centre will be manned 24 hours a day seven days a week, although the computer room in which the super-computer will be installed will be manned 16 hours a day 7 days a week. Access to the computer room is controlled via a cypher lock. When this room is unattended, additional doors with key locks are also closed. These doors are electronically alarmed and monitored from within the building. When the room is unattended operation of the system will be controlled by a remote console within the computer operating centre. Additional security and privacy controls will be provided as part of the supercomputer operating system to prevent unauthorized use of the machine. Access will be strictly on a need-to-know basis.

- (b) Computer Room - Access to the computer room will be controlled by DSD data processing personnel.
- (c) Passwords - Passwords for access will be required for all users. No passwords or IDs will be issued to any nationals of COCOM-proscribed countries, organizations, or representatives of such organizations.
- (d) Software Controls - No information derived from use of the computer, including CAD/CAM and software, will be sold or otherwise shared with any proscribed destinations, or company or individual thereof.

3. The supercomputer will be used only in a closed facility, containing no lines to remote access terminals. The computer will be electrically connected to other computing systems within the computer centre, however access between the systems will be controlled to prevent unauthorised use of the supercomputer or access to its data.

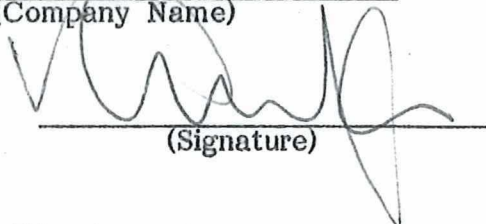
4. There will be no conscious or direct ties to the network of COCOM-proscribed countries or their subscribers.

5. Computer usage will be monitored appropriately. Any indications of use or requests for runs which give rise to suspicion will be promptly investigated by Director, DSD and where there is reason to believe that attempted access can be attributed to a COCOM-proscribed country, company or national thereof, Director NSA will be informed.

Certification

The undersigned overseas end-user attest to the accuracy of the end-use description and agree to undertake and abide by the security procedures detailed above.

End-User: Defence Signals Directorate
(Company Name)

Certifying Official: 
(Signature)

T.W.S. JAMES, Director
(Print Name and Title)