SV00 1256Z 02-08-1983 PAGE 01

ADD ADS CH SM CN CA AGR-18/3/33 AGR-33/7/1 DIR ADC

VZCZCRBA169

RR

DE #0152 2141123

ZNY MMNSH

ZKZK RR DE

R 021122Z AUG 83

FM DSD

TO FALSEC

AUSTONA

JIO

INFO CLO

ZEM

~~T O P S E C R E T UMBRA~~

ADC-233-83

FALSEC FOR FASDN

AUSTONA FOR DIRECTOR GENERAL

JIO FOR DIRECTOR

CRYPTANALYTIC CAPABILITY AT DSD.

DSD*S CRYPTANALYTIC CAPABILITY RELIES HEAVILY ON THE USE OF A LARGE AND RELATIVELY POWERFUL MAINFRAME COMPUTER, THE CDE CYBER 175, WHICH WAS INSTALLED IN 1977. THIS COMPUTER IS AT PRESENT ALMOST FULLY OCCUPIED ON A 24 HR, 7 DAY WEEK BASIS WITH DAILY PRODUCTION PROCESSING. VERY LIMITED CAPACITY IS NOW AVAILABLE FOR APPLIED RESEARCH OR FOR ADDITIONAL PROCESSING DEMANDS ARISING FROM IMPROVED COMSEC PROCEDURES INTRODUCED BY DSD TARGET OR FROM ANY REQUIREMENT FOR DSD TO UNDERTAKE NEW TASKS. HENCE TWO YEARS AGO WE MADE A BID TO INCLUDE FUNDS FOR A NEW, MORE POWERFUL, MAINFRAME COMPUTER IN THE DEFENCE FYDP FOR INSTALLATION IN FY 1985/86. THIS BID WAS ACCEPTED.

2. A MORE PRECISE DEFINITION OF THE COMPUTER CAPABILITY REQUIRED TO MEET ANTICIPATED CRYPTANALYTIC COMMITMENTS IN THE LATE 1980*S AND 1990*S HAS RESULTED IN A NEED TO SEEK ADDITIONAL FUNDING PROVISION IN THE CURRENT FYDP ROUND, AND WE ARE NOW PREPARING A CASE FOR

SUBMISSION TO DEFENCE. THE PURPOSE OF THIS MESSAGE IS TO ACQUAINT YOU WITH THE LIKELY CONSEQUENCES, IN TERMS OF SIGINT PRODUCTION, WHICH WILL FLOW FROM AN INABILITY TO ACHIEVE THE COMPUTER CAPABILITY WE ARE SEEKING, AND TO INVITE COMMENT ON THE INTELLIGENCE IMPLICATIONS AS SEEN BY YOU.

3. THE GENERAL RATIONALE UNDERLYING OUR BID FOR A MORE POWERFUL COMPUTER IS AS FOLLOWS:

(A) DURING THE 1970*S THERE WERE SIGNIFICANT DEVELOPMENTS IN THE APPLICATION OF MODERN ELECTRONIC AND COMPUTING TECHNOLOGY TO COMMERCIAL CRYPTOGRAPHY. THESE DEVELOPMENTS HAVE RECENTLY BEEN FURTHER STIMULATED BY AN INCREASED GENERAL AWARENESS OF THE POWER OF CRYPTANALYSIS. PROGRESSIVE IMPROVEMENTS IN COMSEC DISCIPLINE ARE BEING ACHIEVED BY SOME OF DSD*S TARGET ENTITIES; THESE HAVE ALREADY PLACED SEVERE STRAINS ON OUR COMPUTER RESOURCES, AND HAVE RESULTED IN SOME REDUCTION IN THE TIMELINESS AND FLEXIBILITY OF OUR PROCESSING.

(B) THE MORE MODERN CRYPTOGRAPHIC DEVICES, WHOSE ANALYSIS DEMANDS WORK FACTORS BEYOND THE EFFECTIVE REACH OF THE CYBER 175, ARE ALREADY IN USE BY SOME OF OUR CURRENT SIGINT TARGETS (FOR EXAMPLE AND BY CERTAIN OTHER . TYPICALLY THEY ARE DEVICES PROCURED FROM COMMERCIAL SOURCES; ALTHOUGH THEY ARE IN FAIRLY LIMITED USE , THEIR USAGE MAY BE EXPECTED TO GROW, BOTH NUMERICALLY AND IN DIVERSITY OF TYPES. ALSO, INVESTIGATING THE SUITABILITY OF SEVERAL OF THE MOST ADVANCED CRYPTOGRAPHIC EQUIPMENTS AVAILABLE COMMERCIALLY.

(C) IN ADDITION THERE IS A TREND TOWARD THE DEVELOPMENT OF INDIGENOUS (NON-COMMERCIAL) SYSTEMS. SUCH SYSTEMS ARE . MOREOVER THE INTRODUCTION OF NEW FORMS OF ENCYPHERED COMMUNICATIONS SUCH AS ENCYPHERED SPEECH, FACSIMILE AND MULTI-CHANNEL DATA, WILL FURTHER THREATEN OUR SIGINT CAPABILITY IN THE YEARS AHEAD.

(D) AMONG OUR MAJOR TARGETS,

WHOSE
ANALYSIS WILL PROBABLY REQUIRE AN APPRECIABLE INCREASE IN COMPUTER POWER IN THE VERY NEAR FUTURE. RECENT DISCLOSURES OF DSD*S SIGINT COLLECTION CAPABILITY WILL NO DOUBT ADD FURTHER IMPETUS TO THE INTRODUCTION OF THIS AND OTHER MODERN AND MORE DIFFICULT SYSTEMS.

4. LACKING ANY INCREASE IN COMPUTER POWER, DSD*S RATE OF CRYPTANALYTIC PRODUCTION OVER THE MEDIUM TERM IS CERTAIN TO FALL SUBSTANTIALLY. THE RATE OF DECREASE CANNOT BE PRECISELY QUANTIFIED SINCE IT WOULD DEPEND UPON THE NATURE OF NEW TARGET CRYPTOSYSTEMS AND UPON THE TIMING AND RATE OF THEIR INTRODUCTION. OUR BEST ESTIMATE, BASED ON PREVIOUS TRENDS AND ON AVAILABLE INFORMATION ON OUR TARGET OBJECTIVES, IS THAT WITHIN THE NEXT FIVE YEARS THE EXPLOITATION BY DSD OF:

(A)

(B)

(C)

5. IT IS NOTED THAT CURRENTLY ABSORBS SOME 70 PERCENT OF THE CYBER*S CAPACITY AND THUS REPRESENTS THE MOST DEMANDING CRYPTANALYTIC TASK, IN TERMS OF COMPUTER TIME, UNDERTAKEN BY DSD.

6. IN ADDITION TO A PRECEIVED DEGRADATION IN DSD*S CAPABILITY TO EXPLOIT THESE SYSTEMS, THE TIMELINESS WITH WHICH TRAFFIC IS DECRYPTED WILL INEVITABLY DETERIORATE IF OUR COMPUTER RESOURCES ARE NOT UPGRADED. SIMILARLY THE SPEED OF REACTION TO THE INTRODUCTION OF NEW CYPHERS WILL BE ADVERSELY AFFECTED.

7. SHOULD DSD BE UNABLE TO MAINTAIN ITS CURRENT LEVEL OF CAPABILITY AGAINST TARGETS FOR WHICH WE ARE PRIMARILY RESPONSIBLE OUR ONLY RECOURSE WOULD BE TO SEEK AN EXPANSION IN . WHILE IT IS LIKELY THAT THEIR PRIORITIES WILL DIFFER FROM OURS, AND THIS COULD BE EXPECTED TO RESULT IN SOME FALLOFF IN RESPONSIVENESS

8. WE BELIEVE THAT DSD SHOULD RETAIN A CAPABILITY TO ATTACK EXPLOITABLE SYSTEMS OF INTEREST. WOULD VERY LIKELY ERODE AUSTRALIA*S POSITION IN THE INTERNATIONAL SIGINT COMMUNITY AND COULD PREJUDICE OUR NATIONAL INTERESTS: FIRST BECAUSE IF WE WERE NOT SEEN TO BE PAYING OUR CLUB DUES THERE MAY BE SOME QUESTIONING AND SECOND BECAUSE IN TIMES OF STRESS WE WOULD HAVE LITTLE CONTROL OVER THE PRIORITY OFHIGH INTEREST TO AUSTRALIA.

9. THE ABOVE HAS FOCUSSED ON CURRENT AND FORESEEN CRYPTANALYTIC TASKS WHICH FALL ON DSD. IN MORE GENERAL TERMS IT SEEMS REASONABLE TO ADD THAT THE VOLUME AND IMPORTANCE OF COMMUNICATIONS WORLD WIDE IS INCREASING GEOMETRICALLY, AND WITH IT THE SOPHISTICATION OF METHODS USED TO ENCRYPT THE MOST VALUABLE INTELLIGENCE MATERIAL. CONTINUED TIMELY INVESTMENT IS VITAL IF SIGINT AGENCIES ARE TO RETAIN A CAPABILITY TO REACT TO NEW DEVELOPMENTS, AND ESPECIALLY TO UNFORESEEN CRISES OF ONE KIND OR ANOTHER.

10. WE WOULD BE MOST GRATEFUL FOR YOUR COMMENTS ON THE ABOVE, SINCE WE BELIEVE WE MUST HAVE AN INDICATION OF THE LIKELY IMPLICATIONS FOR INTELLIGENCE ASSESSMENT ON SPECIFIC TARGET BEFORE WE PROCEED WITH OUR FYDP PROPOSALS. AN EARLY RESPONSE WOULD THEREFORE BE APPRECIATED.

#0152
NNNN