

83-2064/6

S-E-C-R-E-T

15 September 1983

MEMORANDUM FOR: Chief, Planning Division, O/DDS&T

DDA REGISTRY

FROM:

DDA REGISTRY

100-24

25X1

DDA Planning Officer

SUBJECT:

FY 1986 Research and Development Program

REFERENCE:

Your Multiple Adse Memo dtd 4 Aug 83, Subject:
FY 86 R&D Planning Cycle

1. The attached statements of research and development requirements for the Directorate of Administration are submitted for your review and for forwarding to the research and development offices.

2. As you requested, we have provided fewer, broader, generic long-range requirements. For elaboration and clarification, we have included problem statements which address specific concerns within these generic topics. As in previous years, we have placed the polygraph research and development requirements in a separate category.

3. In view of the small number of generic categories submitted, we consider each category to be of Priority 1 rank. We expect multiple solution statements to be prepared for each of the generic categories. While we have tried to comply with your recommended format, we are concerned that these broad generic categories contain high and low specific priorities. To rank the generic categories against each other would undermine the possibility of needed research, should one entire generic category fail to be addressed. This approach can be used to develop a successful program only if all generic categories receive funding.

4. In order to further enhance the success of the research and development program, we encourage increased communication with the contact officers in this Directorate. We also request an update on the status of the FY 1985 program. This update will help us in our review of the proposed FY 1986 program and allow our offices to identify the appropriate contacts to support the research and development projects.

REGRADED UNCLASSIFIED WHEN
SEPARATED FROM ATTACHMENTS

S-E-C-R-E-T

S-E-C-R-E-T


5. We restate our interest in the Artificial Intelligence research and would like to see a proposed AI project in support of a requirement in this Directorate.

6. We look forward to the successful development of the FY 1986 research and development program.



25X1

Attachment

DDA/MS:  (15Sep83)
Orig - Adse (w/att)
1 - DDA Subject (w/att)
1 - DDA Chrono (w/o att)
1 - DDA/MS Subject (w/att)
1 - DDA/MS Chrono (w/o att)

25X1

S-E-C-R-E-T

S-E-C-R-E-T

DIRECTORATE OF ADMINISTRATION
RESEARCH AND DEVELOPMENT REQUIREMENTS

- o Security in the Electronic Office
- o Information/Communications Systems Security
- o Physical Security
- o Technical Security
- o Communications
- o General Computer Applications
- o Polygraph

S-E-C-R-E-T

SECURITY IN THE ELECTRONIC OFFICE (ONGOING)

The changes to the office environment that are creating both the "electronic office of the future" and advances in communications technology may have the greatest impact on the security threat. The electronic office explicitly includes word and data processing systems, electronic telephones and computerized branch exchanges, systems for mass storage on magnetic media, and local area networks (LAN's) that link telephones, word and data processors together. These new capabilities will certainly change how we handle intelligence information. How we protect this information can only be addressed after a thorough threat assessment. Along these same lines, advances in communications technology have the potential to change our present technical collection threat assessment. Countermeasures to new hostile systems can only be addressed after we have taken into account what our vulnerabilities are.

While technological change will create new security threats, it may offer new methodology to address both current and future threats. An all-encompassing program to investigate new technologies that have countermeasures applications against an updated threat assessment must be undertaken.

Specific Topics / Projects in priority order

- Office Electronics Security (ONGOING)
- Destruction of Non-paper Storage Media (ONGOING)
- Advanced Telephone Systems (ONGOING)
- Office Shielding Materials (NEW)
- Low-Cost TEMPEST Technology (RESUBMISSION)
- Device Security Profiles (ONGOING)

Contact :

25X1

SECRET

25X1
25X1

Problem Number DDA _____, OS _____ TSD _____

Office: OS/TSD

Title: Office Electronics Security (ongoing)
(Formerly Office Machine Protection)

Problem Description:

The market for new office electronic equipment is expanding so fast that it is not possible to keep pace with the security implications of each new device that appears to save time and money. Assuming the technological advances continue, it is extremely difficult to predict what new classes of equipment will be available in the near future. The security implications of these devices will not only include the traditional vulnerabilities, such as easy concealments, substitutions and emanations, but they will foster new security hazards. The concept of office automation is moving ahead much faster than the security measures which need to be associated with these new machines. [redacted]

25X1

Time Requirement:

Security problems associated with currently available office machines are a serious problem already since many sensitive areas have equipment which is not fully evaluated from a security standpoint. Similarly as even new equipment is developed additional study efforts will need to be undertaken promptly. [redacted]

25X1

Background/R&D History/References:

Traditionally only a few relatively simple office machines were available such as typewriters and copiers. Besides offering places for easy concealment of various types of bugs or sensors, some have been found to produce compromising emanations or characteristic signatures which can be easily read and translated back into plain text. Office of Communications tempest testing has detected and barred such machines from sensitive areas until they could be properly modified or contained. [redacted]

25X1

[redacted]

25X1

[redacted]

25X1

SECRET

Newer office machines such as word processors and computer devices that use magnetic recording materials for information storage, present additional problems that have not yet been defined. The CRAFT and similar programs are attempting to consider the security problems associated with massive network systems, but have now been forced into real time, ad hoc solutions. Protection is often discussed, but if the methods of exploitation are not known, it is difficult to determine what effect the protective measures will have. 25X1

Benefits/Description of Output:

The primary effort should identify the classes of office equipment that may soon be developed and marketed along with the inherent security risks that each may exhibit. A study of this nature should also include the vulnerabilities to exploitation that each will offer as well as quantities of these machines that are expected to be found in sensitive areas. This list will certainly include but not be limited to typewriters, copiers, word processors, and magnetic storage machines. 25X1

Once a comprehensive list has been compiled categorical vulnerabilities by class should yield a "security profile". This information should indicate corrective action to lower the "security profile" and further indicate how remaining weaknesses can be determined or detected in the field environment. The "security profile" should address the trend for having this "smart hardware" advise the custodian of tamper violations, after-hours power use, etc. Current security alarms are not appropriate for this function. 25X1

Policy/Basis Justification:

The world of office machinery is quickly advancing toward the point where there will be a totally paperless society. The DCI has expressed a strong interest in following this trend, as it will solve the current problems of paper document compromise. However, the developing market of automated office machines does not necessarily solve the compromise problem, it merely redirects it to unexplored territory. 25X1

Contact: 25X1

SECRET

Problem Number DDA _____ OS _____ TSD _____

Office: OS/TSD

Title: Destruction of Non-paper Storage Media [] (New) 25X1

Problem Description:

Many commercial devices and Agency unique hardware systems now contain assorted non-volatile storage schemes. RAM, ROM, EPROM, Bubble Memory, and the total variety of magnetic storage materials have no approved method of destruction - emergency or routine. [] 25X1

Time Requirement:

This requirement is currently critical due to imminent deployment of data processing systems to overseas facilities. Prototype systems have been deployed and are operating. [] 25X1

Background/R&D History/References:

On degaussing of floppy and rigid discs, and various sizes of reel tape there has been much discussion. What has not been forthcoming is a declarative summary of the performance, specifications, health and safety data on an approved final or terminal destruction device for magnetic materials. [] 25X1

The non-volatile electronic storage components and devices that will definitely be integral components or subassemblies of systems have not been addressed. [] 25X1

An additional concern must be a USG standard for degaussing and destruction. NSA was thought to be the referent authority but this has not been verified to date. [] 25X1

Benefits/Description of Output:

There should be a profile addressing the "writing" strength and density, and indicating the corresponding degausser strength and time required for total declassification of the data. The differences between AC degaussing and DC (rare-earth magnet) degaussing should be highlighted. The degaussing equipment may be AC powered but there must be a satisfactory equivalent capability that is independent of host power. [] 25X1

[]

25X1

[]

25X1

SECRET

SECRET

dispersed
The electronic component memories will likely be dispersed throughout a chassis or a system and could be considered inaccessible for a short notice emergency destruction event. A scheme for purging these devices, and possibly a recommendation on their location within a given chassis or system are essential.

25X1

A conclusive verification capability is essential for both data storage scenarios. It is preferred that the degaussing/destruction/verification have routine use similar to the emergency use so that situational stress will not be a dominant concern.

25X1

Policy Basis/Justification:

The Office of Security is charged with providing terminal destruction equipment appropriate for the classified material at all Agency facilities.

25X1

Contact:

25X1

SECRET

25X1

Page Denied

25X1

Next 4 Page(s) In Document Denied

25X1

25X1

25X1

25X1

S-E-C-R-E-T

OFFICE: OC

TITLE: Device Security Profiles

PROBLEM DESCRIPTION:

Data terminal and IH system populations are growing and, consequently, the physical and communications security overhead to protect them is increasing. The proliferation of these devices/systems to domestic sites (Agency and contractor) and overseas posts places new demands on our traditional security approaches.

It is becoming increasingly difficult and expensive to establish and maintain adequate security (physical and COMSEC) profiles for these systems.

- Parent room renovations and alarm systems are costly. Maintenance and periodic inspections will remain a resource burden. A new, innovative approach to provide and ensure adequate physical security for our IH devices/systems during and after normal duty hours is required. Methods to reduce the risk of tampering need to be developed along with methods that can alert a user that his or her system has been tampered with. We also need methods that will permit us to use IH devices securely in a signal flooded environment.
- Current methodology to test for compromising emanations requires highly skilled, scarce engineering and technical talent and is very time-consuming. New measurement and analysis techniques are needed for use in the field and the engineering laboratory.

CONTACT:

25X1

S-E-C-R-E-T

INFORMATION/COMMUNICATIONS SYSTEMS SECURITY (ONGOING)

Research to improve information systems security must lead to effective protection of data: (1) as it is being processed on a system or device, (2) as it is stored on a variety of media, and (3) as it is being transferred electrically within networks. There must be improvements in the sanitization of storage media that have contained classified information. More secure data processor designs should be a goal. And, the prevention or detection of tampering with system hardware should be improved. The user interface to the system should be examined to improve the authentication of users and the compartmentation of data.

Candidate Topics or Projects in priority order

- Sanitization and destruction of data storage media (ONGOING)
- Tamper detection for office ADP equipment (ONGOING)
- Data base encryption (ONGOING)
- User authentication (ONGOING)
- Development of a device to detect and prevent the unauthorized transmission of data. (ONGOING)
- Computer firmware verification (ONGOING)
- Telecommunications Security (ONGOING)
- Development of secure networks (ONGOING)

Contact:



25X1



25X1

25X1

SECRET

SECRET

Problem Number: _____

Office: OS/ISSGTitle: Sanitization and Destruction of Data Storage Media

Problem Description:

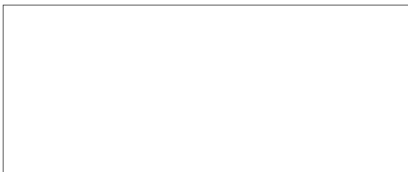
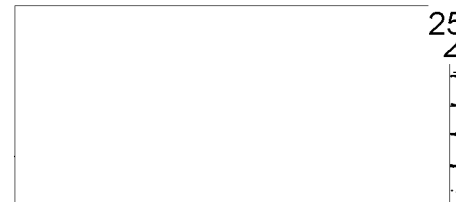
The Information Systems Security Group (ISSG) has given top priority to research leading to ways to deal with erasure of data from memory devices and the ultimate destruction of the devices when the need exists. These twin problems, sanitization and destruction, have been of concern for a long time, but they have been treated separately. This problem statement generalizes the requirement to eliminate stored data. ISSG believes that appropriate research into the physical processes of data storage will lead to methods and devices that are effective in sanitizing various storage/memory devices. This category of research is expected to continue in order to respond to new developments. Magnetic disks are examples of evolutionary design. Each new process or material will need to be considered. Higher coercivity materials cannot necessarily be erased magnetically by the same processes used on present disks. Plated disks, thin films and perpendicular recording will require new sanitization techniques that are based on specific research and testing.

Time Requirements:

There is an immediate need to determine the effectiveness of sanitization methods that are used on today's media. Continuing research will be required for new media.

Background:

Storage media for data processing routinely require sanitization and reuse and some types must be subjected to destruction under conditions ranging from routine to emergency. Some of the media that are based on present technology are: semiconductor memory and buffers, magnetic storage devices, and optical disks and strips. Developing technologies are likely to add new devices. Magnetic storage devices exist in a family that is represented primarily by rigid and flexible disks, bubble memories, rewriteable magneto-optical disks, ferrite cores, and tapes. Remanence in magnetic disks that have ostensibly been erased is a present concern.

**SECRET**25X1
25X1

SECRET

Benefits:

A measure of effectiveness will be established for sanitization methods. There will be greater assurance that media do not retain latent data that could be exploited by a hostile intelligence service.

Policy:

DCID 1/16.

Contact:

25X1

Off. Designator/Location: C/ISSG/OS,

25X1

Telephone:

25X1

SECRET

SECRET

Problem Number: _____

Office: OS/ISSGTitle: Tamper Proof Detection Design for Computer Peripheral Devices (e.g., WANG OIS 250 System) (New)

Problem Description:

Wang OIS 250 system hardware is being placed in domestic and overseas locations as part of the CRAFT program. Although the CPU's will normally be placed in vaulted and alarmed areas, peripheral devices (e.g., printers and terminals) will be scattered throughout work areas. The objective in designing a tamper proof device is to reduce the risk of hardware compromise in hostile environments. Successful completion of this effort will provide an additional option to the current requirement for volumetric alarms in overseas facilities, with cost savings. The developed device should not interfere with normal functions or cause service problems. Further, this device should not be vendor dependent, but should be multi-functional.

Time Requirement:

Since the first CRAFT overseas installation of the Wang OIS 250 system is expected in January 1983, a model tamper proof device should be developed as soon as possible.

Background:

In hostile environments, ADP peripheral devices are an attractive target for other intelligence services because of the large quantities of data which could be captured by technical means. The traditional method of protecting the peripheral devices is installation of volumetric alarms in the work areas housing the peripheral devices. This would result in a significant increase in the number of alarmed areas and in alarm maintenance. It may be possible to substitute tamper proof devices for alarms at some overseas locations, which would result in cost savings. It may be advisable to use both tamper proof devices and volumetric alarm at some overseas locations. The tamper proof devices would be an excellent backup to the volumetric alarm system in high threat areas.

SECRET

25X1
SECRET

Policy:

DCID 1/16.

Contact:

25X1

Off. Designator/Location: C/ISSG/OS,

25X1

Telephone:

25X1

Page Denied

Next 2 Page(s) In Document Denied

25X1

25X1

25X1
25X1

Problem Number: _____

Office: OS/ISSG

Title: Computer Firmware Verification

Problem Description:

A major area of concern is the integrity of electronic components used in the computer systems and networks of the Agency. Any compromise of system firmware can nullify any protection provided by software security utilities. The advent of Large Scale Integrated (LSI) circuits and Very Large Scale Integrated (VLSI) circuits have permitted powerful computer systems to be concentrated in single printed boards. Methods must be developed to verify the integrity of firmware prior to bringing up classified Agency systems, after maintenance activities, and after the installation of new or replacement components. The methods must be capable of identifying unauthorized alteration (i.e., bugs, implants) of circuit components.

Time Requirements:

This vulnerability potentially exists now and adequate means of verifying firmware must be developed as soon as possible.

Background:

LSI and VLSI technologies have facilitated the spread of powerful distributed computer systems and network. These technologies could also provide for the verification of the physical separation of the respective levels of multilevel systems.

Benefits:

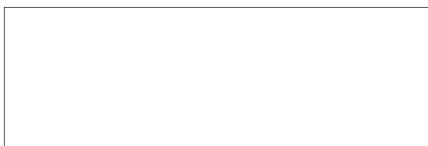
Firmware verification will increase Office of Security confidence in trusted computer systems.

Policy:

DCID 1/16



25X1



25X1

SECRET

S-E-C-R-E-T

OFFICE: OC

TITLE: Telecommunications Security

PROBLEM DESCRIPTION:

Comprehensive software and firmware design and maintenance techniques are needed to prevent unauthorized access to networks and terminals and to detect unauthorized modifications. COMSEC profiles of new communications systems are often determined after procurement. This leads to costly changes to software or firmware and delays in systems deployment. Solution to this problem would radically reduce costs of software changes and eliminate delays in system deployment. Low cost techniques for end-to-end encryption warrant particular consideration.

CONTACT:

25X1

S-E-C-R-E-T

SECRET

Problem Number: _____

Office: OS/ISSGTitle: Development of Secure Networks (New)

Problem Description:

With the proliferation of major Intelligence Community networks and Agency Local Area Networks (LAN) the potential for accidental misuse and purposeful abuse of computer services are increased. Clearance and need-to-know security issues are exacerbated with the connecting of various systems and networks. In order to provide sufficiently secure networks, the following research and development efforts are recommended:

1. Development of Secure Gateways: Gateway systems of varying size and complexity will be required at nodes on Intelligence Community networks to serve as security control monitors. The requirements for a network gateway must be defined. At a minimum, the gateways must provide network access control, data and service authorization checking, flow control, and auditing. The design specifications for a gateway must be provided for a packet switched environment.

2. Development of Security Filters for Local Area Networks: Similar to gateways, security filters provide a checking mechanism that authorizes access between subjects (i.e., users) and objects (i.e., data files) in LANS. The security filter should contain a data base rules access list which mediates all access to system resources on LANS. The design specification should be compatible with Ethernet-type networks and other planned LANS in the Agency.

3. ISO Model Development: The International Standards Organization has developed a seven layered Open Systems Inter-connection (OSI) model for communications protocols in computer networks. The OSI is now an informal standard and provides guidance to computer vendors and network designees. Research is needed to determine at which levels security features (e.g., access control) should be incorporated into the seven layer model.

Time Requirements:

The development of secure networks will become increasingly more significant as projects such as the NPIC Development Program and Mercury progress.

225X1

SECRET

Background:

Computer network design projects are now underway and involve increased involvement of Agency computer systems.

Policy:

DCID 1/16, OMB Circular A-71



25X1

SECRET

SECRET

PHYSICAL SECURITY (ONGOING)

The physical protection of Agency facilities, personnel and material is achieved through maintenance of "concentric rings of defense." Every layer of physical security must be based on a well established need and implemented with the highest regard for the user. A major concern that does not appear to have an immediate comprehensive solution is the prevention of unauthorized removal of classified material from Agency facilities. The problem is far-reaching in that the material may be paper(original or a copy), film or magnetic media. Another physical security issue is pouch protection. Even though acceptable systems are available now, the possibility of compromise of these systems dictates that backup systems be developed for future use.

Candidate Topics or Projects in priority order

- Secure Pouch (ONGOING)
- Document Control / Protection (ONGOING)
- Physical Security General Support (ONGOING)

Contact :

25X1

25X1

25X1

SECRET

Page Denied

Next 1 Page(s) In Document Denied

Problem Number DDA 32 OS 16 TSD 11

Office: CS/TSD

Title: Physical Security General Support (ongoing) 25X1

Problem Description:

Limited investigations are needed at times in general support of physical security programs. Evaluations of commercial systems are also needed from time to time. 25X1

Time Requirement:

This is a needed ongoing program. 25X1

Background/R&D History/References:

Past programs have included a market survey of commercially available document tagging concepts, a tray for the storage and destruction of microfiche, and smoke generators used in anti-terrorist tactics. An expected project will be radiological evaluation of combination locks for safes and vaults. 25X1

Benefits/Description of Output:

Areas of support may include quick reaction contract (QRC) programs, test and evaluation of new and existing hardware, modification of existing equipment, and other short-term support projects. 25X1

Policy Basis/Justification:

TSD has over the years unscheduled quick reaction requirements in the physical security areas that are unfunded. These have been answered thru this program. 25X1

Contact: 25X1

25X1
 25X1

SECRET

SECRET

PROGRAM CALL FY-86

TECHNICAL SECURITY (ONGOING)

Monitor various emerging technologies and describe their possible influence on the complexity of the hostile technical threat. Concurrently, monitor these emerging technologies for substantial or significant enhancement of the Agency's countermeasures capabilities. All permutations of "old/new" with "threat/solutions" are viable. For the threat, address all techniques and media that can support and convey information. For countermeasures, the expected research outcomes can range from procedural changes, through enhancement of existing capabilities, to total upgrade or replacement, or elimination of traditional processes.

Candidate Topics or Projects in priority order

Advanced Receiving System (ONGOING)

[redacted] detection and demodulation (ONGOING)

25X1

Countermeasures General Support (ONGOING)

Acoustics / Ultrasonics (ONGOING)

Magnetics (NEW)

Fluidics (NEW)

Contact:

[redacted]

25X1

[redacted]

[redacted]

25X1
25X1

SECRET

25X1

Page Denied

25X1

25X1

Next 8 Page(s) In Document Denied

25X1

25X1
25X1

S E C R E T

COMMUNICATIONS

The Office of Communications faces a number of challenges through the end of this decade. Agency and Community needs for various types of secure communications continue to increase both overseas and domestically. The OC overseas operating environment is very different than that of most other communications organizations in that we operate under international political constraints, generally in confined space for equipment and antennas, and sometimes in a hostile signal environment. Because of our need to operate at many stations worldwide, our production systems need to be affordable, reliable, and relatively easy to maintain. These operational constraints need to be considered in any R&D program.

To meet these challenges, OC is interested in applying advanced technologies, as appropriate, to the following problem areas:

- Predicting the communications network capacity required through the year 2000 and defining alternate network concepts and architectures to meet Agency and Community requirements. The results will influence decisions related to communications satellites (Community-owned, military, commercial, mixed, etc.).
- Expanding and improving current capabilities including satellite communications. Any planning activity in the area of satellite communications must seriously consider OC requirements.
- Monitoring complex and interrelated systematic activities to rapidly isolate failures and identify effective corrective actions.
- Precluding undetected, unauthorized access to information handled in communications networks or processed at communications terminals.
- Reducing the power and space presently required by standard communications facilities.
- Improving crisis and contingency communications support.
- Accommodating new requirements without changing basic systems and utilities.

S E C R E T

S E C R E T

Technologies of Special Interest:

- High data rate communications.
- Artificial intelligence techniques appear to offer means of meeting some of our needs. Some of these are discussed in more detail below.
- Meteor scatter technology.
- Anti-jam technologies for satellite and HF communications.

FY1986 Research and Development Requirements in Priority Order:

Satellite Communications - Using satellite carriers is rapidly becoming the CIA's primary means of communicating. OC currently uses the DSCS, [redacted] and FLTSATCOM satellites to meet Agency communications needs. The DSCS system, as currently programmed, will be around through the mid-90s; programmed UHF systems will be operational through the end of this decade. In addition to meeting requirements for increased data communications, we foresee a need to develop "tactical" systems to support contingency or crisis situations.

25X1

Improvements in High Frequency (HF) Radio Communications Systems - HF channels must achieve high reliability over longer paths than have been common. HF channels must also support higher bit rates. Existing HF equipment cannot satisfy either requirement. A method of attacking the difficulties outlined above is needed in the form of a new HF modulation subsystem which makes use of OC's existing radio terminal equipment. This subsystem should cost less than \$30,000 per terminal and provide a data rate of 2400 bps. An effective error rate of less than 1 bit error per 1 million bits should be attainable by coordinating the development of the HF modem with other OC projects intended to provide error protection for all types of circuits.

HF Antennas - OC deploys three basic types of HF transmit antennas to field stations: vertical whip, fan dipole, and loop. Increasing data rates, which inherently require higher link gains, will demand that small (comparable) antennas with gains exceeding 8 dB which can be easily erected and demounted be developed. Many antenna manufacturers produce high gain LP and RLP antennas, but they are inordinately large, bulky, hard to install and maintain. Our goal is to obtain a design which will satisfy gain, size, construction, interference and equipment interface constraints.

2

S E C R E T

S E C R E T

25X1

[redacted] - Results of the current ORD program are providing beneficial contributions to the physical security of cryptographic material. We have a continuing need for further research activities in this area.

Fiber Optics Data Bus - An extension of current point-to-point fiber optics technology to permit bus-type communications is required. Program efforts must be centered on development of a low-cost bus interface unit(s) that will afford bus access to a limited number of very high speed (5-10 Mbps) terminals and a large number (2000-5000) of medium speed (2.4-64 Kbps) terminals. The bus interface units must be TEMPEST protected and should include a 64 Kbps A/D-D/A capability for secure telephone use.

Advanced Network Support Tools - As Agency networks grow and become more integrated, and become more critical to the performance of the Agency mission, better tools are needed for planning, operations, and maintenance. The objectives of this effort are to define support tools which will be required over the next 10 years to monitor, analyze, control, and maintain networks. Centralized tech control is to be a primary consideration. Expert systems using artificial intelligence technology should be explored as a tool for analyzing network faults and initiating corrective action.

Advanced Secure Voice - We need to assess technologies and general designs to provide the Agency with alternatives for a forward-looking worldwide secure voice network. The various new technologies and associated services becoming available should be addressed. The concepts and architecture selected must be supportable with available carrier systems and designed to provide convenient, reliable worldwide customer service.

3

S E C R E T

GENERAL COMPUTER APPLICATIONS (ONGOING)

The use of data processing resources plays an increasing role in the Agency. As the number of users, systems, and requirements for new solutions increases, we seek innovative mechanisms for addressing problems. We need to incorporate technical advances in our environment.

We revalidate ORD's program "Language School Upgrade" and encourage the research into Computer Based Education (CBE) in additional areas.

Candidate topics for this generic category include:

CBE in the Language School (ongoing)

CBE/CAI (general)

Personal Computers in CIA

Artificial Intelligence for Software Design

~~ADMINISTRATIVE - INTERNAL USE ONLY~~

Problem Number _____

Rank _____ of _____

Office: ODP

Title: Personal Computers in CIA

Problem Description:

As more and more large organizations in the private sector struggle with the role of the personal computer, it is clear that no consensus exists with respect to its use. Having developed the concept of personal computing to a very high level via the VM timesharing service the obvious question arises -- does anybody really need a personal computer in the CIA? More importantly, is there a place for the personal computer in the ODP network, or should we just ignore the entire matter? A serious examination of the place for the personal computer in the CIA and the role of ODP is in order. With the continuing large investment in software for personal computers, a second question arises -- would it be better to migrate the best of the software from the commercial world to the ODP timesharing system as an alternative to supporting the personal computer as a part of the ODP network?

Time Requirement: ASAP

Benefits/Description of Output: Development of an Agency architecture that makes optimal use of personal computer technology.

Contact:
Office Designator DD/ODP

25X1

25X1

~~Administrative - Internal Use Only~~

Problem Number _____

Rank ____ of ____

Office: ODP

Title: Artificial Intelligence for Software Design

Problem Description:

The use of artificial intelligence to assist the analyst in software design. This would consist of the conversion of detailed requirements into design specifications using some automated (or more likely, partially automated) means.

Time Requirement:

Continuing

Benefits/Description of Output:

An automated (or partially automated) means of generating design specifications from detailed requirements could, in theory, result in better, more timely and less costly ODP service.

Contact:

[Redacted]

25X1

Off. Designator/Location SSD/ODP

[Redacted]

25X1

~~Administrative - Internal Use Only~~

POLYGRAPH DIVISION ONGOING INITIATIVE

Problem Statement:

Rank 1 of 2

Alternative Lie Detection Systems (Ongoing)

There is continuing need for additions and alternatives to conventional polygraph sensors to increase the effectiveness and flexibility of present polygraph activity. [redacted]

25X1

[redacted]

25X1

[redacted]

25X1

[redacted] These lines of research should continue and other measures should be sought and evaluated.

25X1

CONTACT:

[redacted]
OS/Polygraph Division HQS
[redacted]

25X1

25X1

POLYGRAPH DIVISION NEW INITIATIVE

Problem Statement:

Rank 2 of 2

Development of Next Generation Polygraph (Ongoing)

Polygraph Division is interested in long-range development of a polygraph system which will accommodate current sensors, sensors presently under development and, as yet, undeveloped sensors. The system is envisioned as a departure from commercially produced polygraph instrumentation in its capability, derived from computer technology, to store, retrieve and analyze polygraph signals. The system should have the capability of soft-copy display, hard-copy output and remote telecommunications.

CONTACT:

[Redacted]

OS/Polygraph Division HQS

[Redacted]

25X1

25X1

Page Denied