ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM:
Edward J. Maloney
D/OIT

STAT

EXTENSION

NO. DD/A Registry 87-2173X

DATE 8 Oct 87

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DDA \ EXA Room 7D18 HQS	13 OCT 1987	14 OCT 1987	CJ	Bill:
2. DDA	14 OCT 1987		ND	Attached are two documents for you to read. The first is a draft of a paper describing future architecture in the computing area. This is the one I mentioned to you on Monday in our one-on-one session. Actually, it talks about one portion of the network dealing with work group computing. It is not global network architecture, but, nevertheless, shows significant new thinking on the subject, at least for our organization.
3.				
4.				
5. DDA Reg Subj File				
6.				
7.				The second paper is a copy of a memorandum talking about the diskless PC. Work is underway. We are working closely with IMS and it looks as though something useful may come of this.
8.				
9.				
10.				I appreciate any comments you might have on either or both subjects.
11.				
12.				
13.				
14.				
15.				

STAT

Edward J. Maloney

50-1

FORM 1-79 610 USE PREVIOUS EDITIONS

Future Architecture: Agency Work Group Computing

Summary

A concept for a new architecture for the Agency's work environment is proposed as an evolutionary replacement for the existing mix of clustered word processing and centrally provided interactive services. The concept emphasizes use of commercial technology and the need for a gradual migration of new systems into the workplace. The proposed architecture migrates as much as possible of the work down to the work group level, retaining central services as a backbone network, a database repository, and a base for transaction-oriented central services. By migrating in this direction in a timely manner, growth in central computer resources can be redirected away from attempting to keep up with demands in personal, interactive computing and toward more naturally centralized services. A more effective balance between work group computing and central processing is the goal. 25X1

The proposed architecture consists of personal computers as workstations with a small local area network for each physically co-located work group. The small LAN would include a file server, communications server, print server and be managed by customer personnel. Restricting the size and scope of the LAN to a physically secure area is essential to eliminating otherwise intractable security problems. The small LANs are connected as necessary either to mainframe systems for central service or, via bridges, between LANs. 25X1

The interface between the worker and any other system is mediated by the PCs. Those customers who do not have PCs will continue to see the current services, and the older systems will interface with the new architecture at regular points so as to allow a mixed population of old versus new environments during transition. The central VM systems will remain as general computing resources to which the PC users have 3270 terminal access and will continue to serve as the "personal computer" for customers who do not have PCs or LANs needed to participate in the new architecture. It will be assumed that the connections between the work group computing systems and central systems use a minimum number of interfaces that can be adapted as technology changes, and these interfaces can use standards as they emerge to assist in allowing changes in component parts of the overall system without major redesign. 25X1

In many ways, the architecture is not entirely new. Many of the ideas have been proposed previously and discussed broadly within the Agency. Extensive prototyping of an analyst's work environment has been done in efforts by both the DI and DDS&T. Most of these efforts have focused on comparatively high end workstations with substantial coding investment, connected to each other via a local area network. Essentially what is proposed is to provide this sort of capability on a broader base of more commercial technology, answering various security and connectivity questions, and extending the applicability of the architecture into new areas. The architecture is just that, an overall plan to guide the design of systems. The intent is to provide a commodity system for delivery of the services of common concern for which OIT is primarily responsible. It is not an answer for specific customer requirements; it is a technological and conceptual base onto which development organizations are expected to add value in producing customer-oriented specific solutions. 25X1

25X1

25X1

Background

To explain the architecture, it is most instructive to see how it applies to providing gradual replacements for the OIT services as provided today. The most visible of these services are the cable handling systems, data base services and applications, the VM interactive services, the AIM system, and applications built on AIM, including SAFE. OIT also provides terminal and PC services, and clustered word processing equipment and services. All of these services are affected in some way by the proposal. 25X1

The historical OIT architecture has employed VM front end user interface machines, with back end MVS data base and batch processing engines. More specifically, the MVS back end for SAFE handles cable receipt and dissemination, retrospective search of cables, and updates and queries of private index files, which are cables that the analysts save with keywords. The VM front end provides the man-machine interface, electronic mail, composition, coordination and printing. These services are provided basically by the AIM system, with interfaces to the cables being provided by applications software unique to SAFE. The architecture was designed so that the personal computing of the OIT customer was done on VM, with an intelligent, but non-programmable terminal on the desk. 25X1

The older architecture has not yet evolved to take significant advantage of newer trends, specifically the "PC revolution". For many reasons, the direction for some time has been away from merely intelligent terminals to fully programmable workstations. The concept of a person's work environment has to expand to include the local processing capabilities and files inherent in this migration to PC capabilities. Long standing requirements for better user interfaces to services, more graphical displays, more text processing functionality, higher availability, and more customer control can all be addressed when terminals give way to workstations. PCs are now available and inexpensive enough to become the standard workstation in place of mere terminals. But PCs can do a great deal more than just act as terminals, and the challenge is to take the next step and use them as a base for more than just an unintegrated combination in one box of standalone personal computing and terminal-oriented host access. The inherent power of PCs to provide interfaces between customers and systems and to provide services complementary to central services begs to be exploited. With PCs as the basic building block of an architecture, customers and devleopers can provide solutions well matched for specific environments, ranging from secretarial work up through complex analytical tasks. 25X1

Design

The following design is proposed as a strawman. A sampling of products will be called out and an attempt made to design a basic system by interfacing these products together with existing OIT services. Actual selection and procurement or products and the integration are all engineering and development activities that would have to be performed if the concept is successfully prototyped and accepted. The goal in this discussion is to exhibit feasibility and identify minimally qualifying implementations of the architecture, not necessarily the best ones. 25X1

Equipment:

On each person's desk, an IBM PC/AT or upward compatible machine (generic Intel 80286 or 80386 processor, including PS/2 models 50 or higher) with as much speed and screen resolution as can be afforded (1280 pixels wide is available and desirable). An acquisition is being conducted by OIT to supply a source for such equipment. Each individual's PC would have a mouse, LAN adapter card and, optionally, a floppy disk drive modified to be read-only. In vaulted areas, the PCs could also have internal hard disks for software and working storage. The role of the LAN, the floppy disks, and the hard disks will be discussed later. For at least a transitional period, each PC should also have a 3270 communications card and attach to the PBX for interactive host access. Theoretically, with the right LAN products, host access can also be achieved via a communications server on the LAN, but the PBX phone access has some advantages for the moment, especially for LANs other than IBM's Token Ring. The LAN-based communications server is an alternative path which might in the future offer some performance or functionality not available via the PBX. For
25X1 offices outside of the headquarters i.e. where Intecom PBX connectivity is not available, use of a LAN-based communications server is an attractive alternative to using coax connections to a 3174 remote cluster controller and should be considered from the very beginning. 25X1

Two specific LAN configurations and products should be supported if at all possible. One is an Ethernet LAN, built from 3COM Etherlink Plus cards or competitive products (Ungermann Bass), but running Novell's Advanced Netware. Novell has by far the best network software and market share and can include excellent security, reliability, fault tolerance, automatic backup and other features which we really should require from the architecture. The other configuration is IBM's Token Ring. For offices with 3270 PC/AT or PS/2's, this is the only real option currently. A hybrid network, running Novell software on the IBM token ring network hardware should also work. This is the best choice for "hedging" one's bet and would be what a pilot office should be wired for unless specific Ethernet requirements are identified. In the near future, a new LAN manager product from Microsoft (the OS/2 LAN Manager) promises to be competitive with Novell and yet stay more within the IBM family of supported products. When available, the OS/2 LAN Manager would be evaluated as a competitor. 25X1

Wiring would then consist of data grade (equivalent to IBM Type 1) copper wire. In the old headquarters building, for example, this would be run inside Panduit-type covered cable runs along the inside walls and ceiling areas of a vaulted area to a chosen point where the actual network is formed by joining

the individual wires together via an IBM Token Ring junction box (MAU). In the new headquarters building, these runs can be made under the floors even more easily. Either at the central connection point or in a separate "computer equipment room" (CER) such as where the Wang Alliances sit, the LAN server is placed and wired to the central point. This wire run, and only this one, might be through the building's secure grid of either copper or fiber, depending on distance. It is desirable to physically isolate the LAN server from the office and only allow physical access to it by the system's administrator, as is done for the Wangs. All of the equipment proposed is normal PC hardware, suitable for desk tops in office environments. All of it is customer owned and operated
25X1 and located in customer areas, so this is mandatory.

The LAN file server has enough disks to support the customer population, with sizes of 300MB being typical. The file server would best be either a 386-based or OS/2 compatible machine optimally configured for the task. A Novell LAN server can be configured to be fault tolerant, including automatically double-writing all disks and automatic back-up to tape. It has the best "security" access logs and permission control by the systems administrator, and actually has enough security access control to consider putting the server in the customer's vaulted area instead of a separate CER. If the OS/2 LAN Manager can do all this as well, it might be preferable to Novell since it is an avenue
25X1 for future growth of applications on the file server.

The print server has a high quality laser printer capable of desktop publishing. The PC acting as print server may also be able to double as a communications server. It needs to be only a regular PC/AT or PS/2 machine just like the general desk-top model. As the communications server, it provides alternate path host access via an SNA link. For a TRN network, this "alternate" link can be via a TRN "spur" all the way to a mainframe channel-attached 3174 controller at 4 Mbps (probably increasing to 16Mbps soon) without even involving the communications server. Thus TRN networks with this kind of spur may supplant the need for PBX connections unless the customer has needs to access various systems (like CAMS or DESIST) that can be reached via the PBX but not via the SNA network that includes the internal Agency systems. The interoperability of such a TRN connection and Novell LAN software is currently unknown, however, which is another reason why parallel investigation of operating over a more IBM compatible network (IBM LAN software based on
25X1 Microsoft LAN technology) is desirable.

The main reason for the communications server is NOT to provide mainframe interactive access unless it is better than other paths (like the PBX) for this in a particular situation. The communications server is primarily there to provide store and forward exchange of data between the LAN and other LANs or mainframe systems. For this purpose, it needs one or more communications adapters. The desire has been expressed in some environments to have direct LAN-to-LAN exchange of items without any mainframe dependencies at all. The communications servers can form a network of their own using a variety of links, ranging from just asynchronous RS232 lines to complex LAN gateway products. The requirements for LAN-to-LAN mail exchange need to be validated and products selected to accomplish it. It is by no means clear that exchange through a central OIT server is not the best solution, using a processor with high availability for this task. Investigation of LAN gateways should be pursued for other reasons, since there will be requirements for larger logical

LANs than one physical LAN wire can accommodate. Physically secured LAN gateways may offer adequate compartmentation security to link two local work group LANs without allowing customers on one to access data on the other. Enough research is required in this area that using separate LANs with mainframe hubs represents a conservative, interim architecture, however. 25X1

Software:

The most important interfaces for the new architecture will be those between the communications server and the mainframe. There may be several such interfaces depending on the requirements for a particular environment. The PC LAN architecture base can exist without any host links at all, in which case it can serve as a replacement for stand-alone, clustered word processing systems. Links can obviously be added for other purposes, including mainframe interactive access (3270) as discussed above. The less obvious links are those which provide transfer of information, specifically files of data -- documents, data bases, pictures, or anything else. There is a great deal of hyperbole about distributed data bases and remote file access protocols and other advanced communications concepts. The proposed architecture is designed to be open for these possibilities as they mature, but these concepts generally assume high speed, dedicated communications and a great deal of very complex network functionality. The design objectives for the proposed architecture are that it scale down to situations where there are relatively slow speed or non-dedicated (switched) circuits, including the particularly slow speeds characterizing the Agency's overseas network. For this reason, the only interfaces presumed between the LAN and a host are an electronic mail one plus an interactive 3270 link if needed for specific requirements. 25X1

Electronic mail in this instance is defined as the directed transmission of electronic objects, of whatever internal form, between the filing systems of one computer system and another. The transmission is assumed to be non-synchronous in nature; i.e. the origination and destination systems do not have to be both up and communicating with each other on a real-time basis. The model for transfer of information is a "store and forward" network. The sending and receiving customers never see the transmission process directly -- it is all done in the background. The actual mechanism is a link between an electronic mail system on the LAN and a host mail server. One method for this is a synchronous communications adapter that can support SDLC/LU6.2 protocols using "program-to-program" communications. The prime candidate for use as the backbone mail mechanism is the SNA Distribution Services (SNADS), with cable formats being an alternative for the overseas environment where re-use of our existing network facilities is required at least for transition. 25X1

The user interface to the entire system should be based on a graphical presentation. The migration path for achieving this has been identified by Microsoft and it is to use Windows now and later Windows 2 for DOS 3.x. When OS/2 1.1 with the presentation manager becomes desirable, code can migrate to it. The LAN enables a mix DOS and OS/2 machines so this choice can be deferred. The LAN has to provide the office environment for the customer -- the files, word processing, desk-top publishing, shared authorship/coordination, calendaring, printing, etc. The actual production files should be on a LAN file server, which provides virtual DOS disks with the advantage of being able to share them between customers. By the time this

environment goes into production, I would expect to have a Windows version of MS Word as the answer to both word processing and desktop publishing sufficient for the Agency's needs. A few offices may also want Aldus Pagemaker, but only for the specialists such as in CPAS. Some standards are emerging in the field of electronic printing, and it should be possible to transmit finished copy in electronic form from its origination to publication. Windows EXCEL should also be available to provide spread sheets compatible with the rest of the Windows suite, although some use of Lotus 1-2-3 will remain, along with plenty of other
25X1 non-Windows applications that can still be used on the same equipment.

The critical new software is that which defines the precise nature of the user interface to the electronic mail backbone. The electronic mail interface has to support communication of documents and other electronic objects between people on different LANs, between AIM and the PC LANs, between departmental systems that are part of this environment at the interface level (SNADS), and between all of these and the cable systems, including the SAFE dissemination and retrospective search capabilities. The electronic mail products and interfaces on the hosts and between the hosts and departmental systems are already determined -- AIM for the VM interactive, "dumb terminal" customer, and SNADS mail services for the departmental systems, including an AIM Gateway. The missing piece to form the basis for these services in the new architecture
25X1 is an electronic mail and filing environment on the LAN.

It turns out that this requirement can largely met by just using DOS files and subdirectory structures along with conventions and a bit of software glue. A prototype of this sort of system is the "Coordinet" project implemented for
25X1 CPAS and the Intelligence Community by OIT/SAD&E. With relatively little effort (compared to most SAFE development at least), this could be expanded into a usable environment. However, there are commercially available electronic mail systems for PC LANs, and some of these merit investigation to see if they offer any functionality that customers desire. Potential candidates are such things as "The Coordinator", which offers an action tracking model of paper work flow; "3+Mail", which offers a SNADS gateway product; and "DaVinci", which offers a Windows-based presentation interface. Certainly, nothing evident in the market offers all the functionality for all customers in all of our unique environments -- especially not the overseas environment where interfaces may only be via cables, and none of these products does all that AIM does, for example. It is clear that to meet some
25X1 requirements, some integration and development will be required.

Fleshing out these interfaces is the bulk of the difficult work involved in even prototyping these systems with anything like the full-up interfaces. Due to the variety of customer interface needs and the variety in backbone transmission systems, development of a layered model for implementing the pieces independently is required. The recommended approach is to start with a simple Windows-based presentation interface, with a communications server process just picking up mail as DOS files from customers' libraries and doing the real transmission either via a commercial interface to a SNADS product or private protocols such as cable format to a communications terminal (the access
25X1 point to the cable network).

Back on the mainframe side, the software effort consists of re-casting the necessary services into the form of background electronic mail. Almost any

service can be provided on a backbone of electronic mail, including data base updates and queries based on transactions. Some applications are more difficult to design in this fashion than others, and the turn around time required for a transaction is an critical design driver. Applications which can be designed to need slow turnaround can be made available across the widest range of networks and with high fault tolerance for temporary outages, while applications that insist on using instant response designs are much more restrictive and demand high availability, high speed networks.

The most obvious service to be recast as background transactions is electronic mail itself, although OIT currently provides it as an interactive service on VM (AIM). Work is already in progress to connect the central-storage/interactive access model of electronic mail as provided by AIM to departmental computer systems with SNADS and some bridge software from a commercial vendor (Softswitch). This may well be the basis for connecting to PC LAN systems as well. But, there is a middle ground of PCs that are not on LANs but do have host connections, or small PC LANs where dedicating a communications server may not be cost effective. Thus the design should allow an alternate connection scheme wherein solitary PCs can enjoy background electronic mail transfer. This design would be prototyped as a background link from a PC task (under Windows) to VM to get mail via AIM, with the customer just being prompted for passwords when necessary but never seeing the AIM interactive screens. Basic support for this sort of transaction-oriented interface to AIM is already beginning as part of the effort to make it easier to transfer documents and use
25X1 PC-based word processors with AIM.

Concept of Operation

The following is a discussion of the concept of operation and the division of labor between the mainframes and PCs. One of the major services that has to be redesigned for this architecture is the delivery of cables, so this will be the illustration for the concept. There are actually several cable delivery environments, but the key for this discussion is that all of these environments are really amenable to treatment as electronic mail systems. The customer at the end of the process should receive and originate cables as one more form of electronic mail if this architecture is to be fully successful. The three communications and local processing environments to be discussed are overseas,
25X1 on departmental systems, and on the SAFE-like systems.

In the overseas environment, cable origination and receipt should look to the customer, to the extent possible, the same as for for all the other environments. Cables are sent through an authorization chain and eventually released by having a releasing authority "mail" them to the communications network. In practice today, that final step is usually done by printing a copy and conveying it to a communicator, although prototype direct electronic links (CRAFT to TERP) have been made. Conversely, cable traffic coming in to a station could be delivered electronically from the communications terminal to the file system in use for office automation in the station. Whether all the traffic would go to a records officer for distribution or be disseminated to a lower level automatically, at least sorted out between administrative and operational traffic, is a decision to be made by customers. The technology
25X1 allows for such processing.
25X1

within secure space. Other forms of encryption (CCEP encrypted Ethernet) are also likely to be available by the time this can be deployed, which is especially attractive given the DEC MicroVax base for ET, the next generation
25X1 of communications terminals.

For departmental computer systems, such as employed today within the DDS&T especially, another level of cable interfaces is part of the architecture. OIT/EG has in progress a project to support the DDS&T systems, specifically the new FBIS VAX systems (AFS) and some Wang VS systems. The goal is to supply cables electrically to these systems and to permit two-way exchange of electronic mail between their electronic mail networks and AIM over the same links and under the same basic architecture. This project employs the AIM SNADS gateway and a commercial store and forward mail system on MVS (Softswitch). Additional software is in progress to route incoming cables that CDS and MHF have marked as being for the DDS&T offices over to the Softswitch hub with appropriate routing indicators. Under this architecture, OIT systems have done only top level dissemination down to offices, and the departmental systems, under customer control, are responsible for any further handling and
25X1 for all local processing.

For SAFE systems, OIT systems carry the dissemination process all the way down to the personal level. Each SAFE customer can specify interest profiles to serve as a filter against all incoming cables that the particular SAFE system sees. (The DI SAFE system sees a different selection of cables than the DO SAFE due to the top level dissemination done in CDS/MHF to separate operational traffic out for DO-only consumption.) In the current Delivery 3 SAFE, cables are disseminated to customers via mail files, which are created on MVS but accessed from VM by SAFE-specific software running as a context under AIM. The cables are also indexed by words and stored for retrospective retrievals.
25X1

Regardless of what one thinks "SAFE" is or should become, under the proposed architecture, it is clear that one wants to profile and disseminate incoming cables and other intelligence source data down to individuals in their local computing environment. The simplest migration for the full cable dissemination process into the new architecture is that the MVS SAFE systems would continue to do the cable dissemination via profiling as is done today. No apparent need to re-host this process is evident, although a highly parallel processor could theoretically do it all faster. Likewise, the retrospective data base of cables is basically fine where it is today (in INQUIRE on the MVS processor), but could migrate to a back end data base machine (such as a Teradata) if the processing requirements continue beyond the cost effectiveness of the IBM architecture. The MVS processor can serve as the host for the store and
25X1 forward mail hub.

The VM processor would continue to be the "personal computers" for people with simple interactive terminals (Delta Datas or 3270 devices when Delivery 3.5 is completed). For this population, SAFE Delivery 3.x code continues as is. VM continues to be the host for the AIM system for such people, and communicates with the other AIM systems in the Agency. The bridge between the AIM systems and the LANs and all other "departmental" sorts of systems would be via the planned AIM Gateway to the MVS server, an LU6.2 SNADS link. PC customers migrating to the new architecture, however, would start to receive both AIM

mail and cables disseminated from the MVS SAFE profiling systems on the PC LAN. This mail and cable traffic will have been forwarded to the LAN and reside on the LAN file server in the PC user's mailbox on a continuous, background basis. The distinction between AIM mail and cables should be largely eliminated, although they should have different "categories" or action types associated with them so the recipient can choose which he wants to review at any one time. Once the mail or AIM file has arrived on the LAN servers, it is deleted from the host side. The decision to retain things and provide the storage for them becomes the responsibility of the customer office entirely. Only the retrospective cable file and the AIM documents actively in use by AIM customers
25X1 remain on the hosts along with other central data bases as needed.

In actual implementation, the MVS dissemination process would still produce mail files of hits to be kept for 30 days. A new process would recognize that certain mailfiles are being followed by recipients who are served on LANs rather than as direct interactive customers. The new cables added to these mail files would be "mailed" down to the individuals via their LAN communications server, along with any AIM mail addressed to them and via the same links. Some optimization for multiple people on the same LAN getting a hit on the same cable is possible, but needn't be implemented for prototyping. The process of updating profiles is already based on electronic mail under AIM and can be migrated over to PC mail in a fairly obvious fashion. PC software to create, edit and activate profiles would have to be developed, and tools to
25X1 help do so exist.

Retrospective searching of the combined document file (the set of all cables ever received from a certain date onwards), and even of the mail files (since they continue to exist on the host for 30 days) is an interesting design issue. In the interactive SAFE Delivery 3.1, search response is nearly immediate via direct connections to INQUIRE. In Delivery 2 SAFE and normal AIM, a different kind of SEARCH was was used for "SAVE" files. The AIM search process uses an "electronic mail" interface, with response coming back significantly later via a return message and a folder of hits. This interface of mailed-in queries and mailed-back responses could be the model for the proposed architecture, but there are problems to be resolved. In the new architecture, a retrospective search that produced a lot of hits would be a big problem if the hits had to come down the communications channel to be reviewed. Limiting the number of "hits" would be mandatory. An alternative is to establish a more interactive connection to a searching task and review the hits without "mailing" them down to the LAN. For example, one could have the analyst "log on" directly to an application like Delivery 1's "TEXT" that actually called INQUIRE under the covers to do retrospective search. The analyst could then request any given "hit" or list of "hits" to be be brought down to the PC for use in composing a report, for example. Choosing between these models, or finding others, is a area to be worked. Clearly for extension of the concepts into the overseas or other remote locations, the electronic mail model is adaptable where the interactive model is not. There many other data base functions that the architecture would allow to be handled as electronic mail requests, such as DO name traces if security constraints could be met. Likewise, there may be other needs to use direct interactive queries when transaction-oriented interfaces
25X1 are less useful.

Outgoing cables are another interesting area that the architecture needs to address. Presumably, all cable composition and branch-level coordination occurs on the LAN. However, the LANs and electronic mail interfaces can all be available well before all the issues of electronic cable origination can be worked out. The hardcopy channels for submitting outgoing cables should be maintained for some period, and installations of LANs shouldn't await resolution of the cable origination issues. Given the high desirability of a laser printer on the LAN anyway, one of the requirements for equipment selection of the actual printer hardware should be the ability to produce hard copy cables that can be accepted by the OIT cable systems. Even later, it should still be the case that one should never have to assume that ones mainframe interfaces are up in order to produce and get a cable out. However, if the mainframe interface is available, by the same token, one should never have to print a hard copy. The software that produces the cable locally should adapt to being able to address it out to the mail system and hence out to the cable network. The reason for caution in promising this capability in early implementations is that the process of coordinating, authenticating and releasing a cable is probably not commercially available on LAN-based mail system in a "trusted" way. Unlike AIM, sending a document through a train of people and being able to guarantee that it has gone through them is not a feature of any distributed mail system known. It may be possible to recognize safely that a single individual on the LAN is the one who actually forwarded the cable up to the host, but that is about all one can expect to get commercially. In instances where that individual has releasing authority, cables could be originated all electronically and actually sent out, but this needs to be investigated a great deal more before electronic cable origination from LANs, or any other departmental computer schemes, can be considered feasible. [redacted] 25X1

Stand-alone or Remote Use

One of the main advantages of the new architecture is that, so long as applications stay away from requiring interactive 3270 access, it does not require that the mainframe systems be constantly available. They only have to be up long enough, often enough, to get the "mail" through in a timely fashion. If the LAN mail software has alternate routing capabilities for LAN-to-LAN transfer, the availability of the mainframes is further de-emphasized. Note that for the LAN-based customer, no VM availability at all is required in the long run. The link from the LAN to the mainframe mail server can be of relatively low bandwidth if it is available most of the 24 hour day. It need only keep up with the arrival rate of mail and cables (but does have to account for the retrospective search burst arrival possibility). Statistics on how many analysts are in a physically co-located area and how many cable hits they generate in total are needed to see how much bandwidth is required, but it would be surprising if more than a 9600 baud link per LAN were needed to provide "same hour" delivery as required by SAFE for cables. Thus the architecture is not limited to headquarters environments with high bandwidths to the hosts. [redacted] 25X1

As mentioned, it is even possible to use the same architecture where there are no host links at all. The LAN, the PCs, the cable authoring software, and the office coordination tasks all function independently of any mainframe services. The same systems, subject to EMI security criteria, could be installed in

headquarters, remote outbuildings and even the foreign field. The goal of skills portability and symmetry of systems as embodied in the DO's DOLPHIN concepts is met by this architecture. The capacity of this architecture to replace CRAFT seems obvious. The installation problems are fundamentally the same for LANs as for an Alliance system, but the PCs and the LANs offer a more open architecture. This offers distinctly more possibilities for taking the next step and directly hooking the communications server to an interface to the narrative message network in the field in lieu of the MVS mail server in headquarters, but making it look basically the same to the end customer -- a mail interface. The problem of cable releasing authority still exists, but in the field environment may be more tractable where a single releasing authority, such as the Chief of Station, is more the rule. 25X1

Over time, the mail metaphor may aid the eventual migration of the narrative networks and the data networks into integrated systems so that the headquarters and field customers really do have the same interfaces. Looking at mailed transactions for retrospective cable searches leads to thinking about such transactions for other data base queries such as name traces where the query might be sent not to a data base but to a person who could access data and rapidly transform the results back into a mailed response without compromising the security of the data base itself. Likewise, the objects being mailed should not be restricted to just narrative messages. Current PC technology allows mailing of images, for example, so the capacity to use electronic mail in lieu of facsimile is present. Putting in a network of PCs doing store and forward mail rather than fax machines with dedicated circuits seems quite desirable. 25X1

Similarly, whether for headquarters or remote customers, there is no reason to assume that there is just one central server for cable searches or anything else. The distributed model makes multiple back end systems more feasible and allows for easier incorporation of new data base engines or even alternate computer sites. 25X1

Two Tiers vs. Three

The proposed architecture can be characterized as "two tier" in that the processing resides in the PCs and on the mainframe. The file server on the LAN is just another PC providing shared disk access and maintenance. It is not a general purpose timesharing service, nor need it run any data base systems or multi-user software. It can be regarded as just a smart, more securable, disk drive in place of having disks on each PC. The electronic mail system doesn't really run on the server in the sense that customers log on and use it. It is the communications task that is doing the mail work -- the rest is done by software in each PC accessing shared files on the server. This is in contrast to the "three tier" departmental computing model, where there are significant applications running on the office-level system and customers log on to the departmental machine to use it as a computer. On a LAN, customers enter a password to be able to get to their disks, but that's the extent of the log on process. 25X1

The architecture would certainly allow for a departmental computer as part of the LAN, but there appears to be no requirement for it when just considering the core services provided by OIT. If the level of office automation provided

by the combination of PCs and a mail system is not sufficient for some reason, then use of a "departmental" system as a file server plus local log on computing can be employed where necessary. However, the burden on the customer office in running a departmental system as opposed to a LAN alone is sufficiently high to design the future, commonly installed and supported OIT system to consist of only two tiers. One of the main features of the new architecture is that customer offices operate their local computing, including the LAN and its servers. A systems administrator, similar to the administrators now used for Wang Alliances, must be provided by the customer office. In the two tier model, the LAN and its servers are just more PCs and represent the minimum impact on the customer, whereas departmental computers are generally associated with higher skill levels and effort in systems administration. The philosophy in proposing a commodity architecture based on PCs and small LANs is to provide the most return with the least investment in manpower, equipment and support costs. If customer offices have multi-user applications or data bases that cannot run on PCs, then they can add departmental machines to their LANs and use them as necessary. 25X1

The proposed architecture does have the attribute that IBM compatible workstations are presumed. Other workstations that could coexist on the same LAN and use the same file server and file structures and the same LAN-based mail package could be envisioned, but they do not exist in practice. Developing any code at all on the workstation (such a creating cables) or in the communications server will mean a lock in not to a particular piece of hardware, but to a particular operating system environment, namely DOS and, later, OS/2. Implementing the architecture for multiple workstation types is not a trivial, and perhaps even an impossible, task and is not envisioned. If the Agency cannot choose a single operating system environment for workstations that are to participate in future, widely applicable, OIT-supported systems and services, then a substantial delay in implementation is required, and a reduction in function to absolutely minimal interfaces is essentially unavoidable. Although cooperative processing models and transactions all may become standard commodities, once applications are designed at the workstation level to use these standardized interfaces, then the issue is not standards but program portability. And the portability of full scale, complex applications including communications, graphic user interfaces, mail systems and data bases from IBM (Windows) to Apple (Macintosh), for example, is essentially a matter starting over at the design phase, regardless of whether the code is written here or procured commercially. There can be no half measures at this point; making a choice and living with it are required. 25X1

Data Bases

So far in the discussion, the only data bases implied were the electronic mail files on the PCs (physically on the file server, but logically appearing as files to the PC), the retrospective cable file, and 30-day mail files (the latter two on the hosts). There are many many more data base requirements. Each of these requirements has to be examined in light of the new architecture proposed to see what makes sense to do and where to do it. Clearly, the sort of private data bases held today on VM minidisks are the easiest to envision as being on the PCs and LANs instead. At the other end of the spectrum, the corporate data program will continue to represent holdings that are of interest Agency wide as central data bases. Only the customer interfaces to these

systems is open to change, starting with 3270 interactive access and perhaps moving in some instances to mailing updates and getting back reports. These are issues for the corporate customers and developers to work, not
25X1 fundamentally driven by the architecture.

In the middle ground, however, there are no easy choices. Trends in technology point to rapid growth in data base capabilities, particularly in the area of relational data bases using the SQL interface, a common standard which has been embraced by OIT as a standard. One of the promises of this technology is distributed data bases, which implies that portions of the data needed by a customer can live on different machines at different levels in the architecture and yet be used as one resource, without the customer being involved in the details. Unfortunately, much of this is hyperbole and promise. Furthermore, it generally presumes high speed real-time links employing advanced program-to-program communications protocols which are unrealistic in many environments. Systems designed with distributed data bases at this time should be regarded as research and development and are not generally applicable as a commodity architecture. Eventually, this technology will offer substantial benefits, probably in viewing host data bases using user-friendly PC systems. These front-ending approaches already exist in some cases as ad hoc products, not part of a distributed data base architecture. Thus one has to design for the moment for either data bases held locally on the PCs or on the host and take as a given that integrating the two in any fashion takes applications
25X1 development.

As has been the case in design questions discussed previously, the issue of what data lives where and how one accesses it is one that should be addressed by customers and the applications developers. The general rule of the architecture is that data to be shared by more than a group with the same LAN access (i.e. the same security-defined group) will have to be on a host. The customer's interface to this data can be either 3270 interactive or controlled by applications programs, whether commercially procured or developed, using any SNA-defined suite of protocols. (At lower levels, the SNA links may transit X.25 circuits such as provided by Mercury or go through any number of
25X1 transmission stages independent of the applications level interfaces).

Making these data base design decisions will not be easy. For example, the OIT systems on hosts provide data sharing in many ways -- particularly in the form of shared AIM folders and SAFE mail and private index files (PIFs). One of the goals of the new architecture is that users of it migrate off of the AIM system and off of VM in general, since the PCs should provide the personal computing and office automation functions. However, AIM shared folders that cross more than just an office cannot be easily mapped onto LANs since people from one office cannot generally have access to other offices' file servers where the local sharing can take place. Most commercial systems answer this problem very minimally -- sharing information with other branches is done by mailing them a copy. The only alternative is to make the AIM shared folders into a data base service that can be accessed by the PC users in some fashion. One could start by giving the PC users their mail on the PCs, but letting them access AIM interactively to peruse shared folders. A more complex development effort would allow PC users to view AIM folders and documents as extensions of their PC environment and not ever see AIM itself as an interactive service. In effect, AIM could migrate into being a file server. Over time, changes in data

base technology could allow movement from AIM to other data base systems so long as the customer's interfaces to the data were preserved. The same sort of decision has to be made in regard to SAFE PIF files, and this is an area to be worked.

25X1

Security and Records Management

Among the problems with bringing in PCs to the Agency environment has been the change in security problems and records management problems due to the storage of data in compact, distributed and essentially unmanaged forms. The security problems and records management problems are quite different, but they are caused by the same technology -- portable magnetic media with classified or official records. A complete discussion of all these problems is far beyond the scope of this paper. Opinions on these subjects vary from "there is no problem; it's up to the people to maintain the information securely and personnel security is the answer" all the way to "PCs are inherently evil and can never be secure enough for us to use without developing high technology computer security hardware and software." In truth, there are serious problems that OIT, given the mandate to protect information both by records management and computer security, has to insist on addressing. One of the jarring statistics used to emphasize the magnitude of the problem is that the OL Supply Room in Headquarters hands out over 5,000 floppy disks a month -- about 2

25X1

25X1 billion characters of data storage in a medium that is not under any official records management, accountability, or technical security control.

A paper discussing one technology for essentially eliminating most problems has been presented by OIT to the Executive Director (memo of August 12, 1987). In brief, this paper recommended eliminating the use of floppy disks as much as possible and moving in the direction of LAN file servers to provide the needed PC filing capabilities. PCs with disk drives that cannot write are not a serious problem and can be used in very limited fashion as intelligent host terminals, or in full PC fashion when connected on LANs to more securable and manageable file servers. On a LAN, even PCs without any disk drives at all are fully usable and available commercially. In vaulted areas, internal hard disks are also an option, so long as compartmentation and records management policies are not ignored. In all cases, the key to full functionality and reasonable information control is to centralize important data on a file server where the security and management of it can be implemented to whatever degree the

25X1 customers and the responsible Agency offices (OIT and OS) can agree upon.

In the past, host computers were used to perform much of this centralized, manageable, access controlled, secure environment. Many applications requiring compartmentation were not suited for this environment, and the tremendous aggregation of data in one place was a problem in its own right. Distributing this central storage outward to file servers, but not all the way to the anarchy of individual PCs, offers a compromise that should be workable. The level of security obtainable should be about the same or slightly better than that available in the Wang Alliance architecture today, which should be sufficient. Requirements for mandatory access controls and audit trails can be

met. As with all commercial systems today, additional requirements such as mandatory data labeling cannot be met in general by PC file servers and have to be put aside for future developments. Given the direction to procure and use commercial software as much as possible on the PCs and the explosion in the variety of PC software, there is simply no feasible way to add additional requirements, even simple ones such as labeling of printouts. Classifying output will be, and really always has been, up to the customer and not
25X1 something OIT can enforce through software.

A separate issue from the disk usage issues is the security of the LAN itself. There may be some confusion between the assertion that the LANs proposed increase security while previous discussions have always ruled out LANs as not secure without encryption or other largely non-commercial expensive solutions. The general attribute of a LAN is that everybody's data transits past everybody else's workstation, hence making it technically feasible to tap in at any point and capture unauthorized data. LANs are also generally touted as connecting everyone to everything, which makes compartmentation and access control highly
25X1 complicated, contradictory requirements on the LAN.

The difference is in the scope of the proposed LANs and what they are used for. In this architecture, there is not a LAN running throughout the building into which everyone plugs PCs and enjoys instant, universal access to everything via that route. Attempting to install that sort of LAN on the scale of the headquarters building was actually envisioned once but never successful. Problems have plagued and will plague every such attempt for deep, intrinsic reasons. Successful projects, on the other hand, have been to install LANs interconnecting PCs on a very local level to enhance sharing of data and resources at that level, with either no connections or controlled connections to outside resources -- hosts or other segments of LANs, via gateways. Stand alone LANs in Central Cover Staff/DO, Polygraph Division/OS, and FBIS have been quite successful, although the latter may not conform to any proposed standards and should be reviewed when such standards are adopted. The latter kind of LANs, small LANs, are what is proposed. Keeping the LAN small enough and within physically secured space, among persons of essentially equivalent clearance, eliminates the need for encryption and complex technical security for the LAN medium. File access security sufficient for privacy protection and
25X1 need-to-know compartmentation then suffices and is readily available.

Relationship of LANs to Communications

As there is no universal connectivity LAN proposed or considered feasible, terminal-to-host connectivity and point to point connections from place to place are provided by a backbone OIT network with its own security and access protections to keep customers' data separated. The current implementation of
25X1 this architecture in the Headquarters is a voice/data PBX, solving the connectivity problem for terminals and voice in one architecture. Extending this solution to as many points as it can be applied, extending over much of the metropolitan area, is the subject of important OIT initiatives in the coming years. For non-PBX equipped sites, use of communications protocols using SNA or interoperable with it (such as using Mercury for a transport mechanism when available) is the proposed architectural solution whenever host
25X1 access is required, including overseas access to systems.

There are higher speed requirements for communications than the voice/data switching can provide. In fact, between distributed PBX components themselves, high speed fiber optic links are required. The architecture chosen in these instances is to use leased/purchased fiber optic cable with Agency transmission equipment (including encryption) as needed. Unlike the telephone circuits used between buildings today, the transmission over the fiber is not from the Agency to a commercial concern's equipment, over their network and back to us at another point. OIT is actively acquiring "dark fiber", optical cables that can be put to any use, along various paths connecting Agency buildings and interests. These links will be there to support high speed connectivity requirements for decades to come. Links for video between Headquarters and

25X1 [redacted] are already in place as a service to the DDS&T. With the advent of the PC LANs as proposed will come additional requirements to build bridges between LANs and high speed Gateways across wide areas. OIT is positioning itself to

25X1 support such requirements. [redacted]

One major piece of this overall fiber optic effort should be specifically emphasized. This is an OIT initiative referred to as the "fiber LAN" in Headquarters. It should be understood from reading this paper that this is not a universal connectivity LAN designed for plug-in-and-go operation as one might think. This initiative is designed to provide the backbone network of fiber optic cables within the buildings to support any and all high speed connectivity requirements as they arise. High speed connection requirements for LANs and all other applications will come in on a case by case basis, and the backbone of fiber, fiber connection panels, fiber distribution systems and network management systems have to be in place to accommodate this in a timely

25X1 manner. [redacted]

Actions

The basic components for the new architecture are already available. OIT/EG proposes to expand its efforts to bring in, evaluate and adapt this technology
25X1 for use within the Agency.

OIT/EG and CSPO should commence design of a migration path for SAFE to utilize the new architecture. Design and prototype efforts with the SAFE customers should begin at once to see how soon the new architecture can be deployed in DI and DO. Historical SAFE requirements and current DI and DO ADP requirements should be reviewed in light of the capabilities of the new architecture and determinations made as to what is feasible in the near term, what will take development, and what might have to be foregone in order to enjoy other
25X1 benefits from the new technology.

OIT should work with IMS in the DO to see to what extent this architecture can serve as a basis for DOLPHIN. Joint effort is also required to migrate the cable creation and handling processes developed by IMS into the new environments offered by PCs and by SAFE and to consider the applicability of
25X1 this technology in DO stations world wide via OC networks.

An evolutionary migration of customers from the old systems to the new should then be planned, with investment in LANs and workstations planned as early as 1989. All OIT components have significant roles to play in such an effort, along with the ADP planners in other Agency offices. Contractual vehicles have to be put in place along with support systems for installation, maintenance, consulting, security evaluation, records management support and applications development. To be as successful as the Wang Alliance systems, which is a goal, OIT has to be able to accommodate hundreds of LAN installations a year in
25X1 the near future in order to support workstations. OIT's abilities to support PCs must expand and be able to cope with at least ten times today's volume of actions relating to PCs. Capabilities to fix PC software problems, distribute revisions and provide consulting are all required in more areas and in ten times the quantity than is possible today. OIT has to arrange that everything be done for the PCs that is done for Wangs, with levels of support and marketing expertise similar to those exercised by Wang itself directly to
25X1 customers.

OIT and OS components concerned with computer security must come to terms with the PC environment and the proposed office-level LANs. Determination of an adequate and feasible set of security constraints within the capabilities commercial PCs and software must be made. Policy on how and when to use the password authentication mechanisms of LAN file servers needs to be established. The security characteristics of the proposed architecture should be acceptable, but need to be coordinated and reviewed as necessary to be deployed. The level of trust to be accorded electronic signatures of document/transactions between systems must be established in order to pursue applications such as cable
25X1 origination.

OIT has to continue to evolve the backbone services with initiatives such as the fiber LAN network, SNA installation (part of NEWS), and the many segments of the New Building Communications Project. While LANs represent alternative forms of communications capabilities, the need for core services does not
25X1 diminish and will probably grow in new and challenging ways.

OIT/EG: 38-87

MEMORANDUM FOR: Edward J. Maloney
Director of Information Technology

STAT FROM: [redacted]
Chief, Engineering Group

SUBJECT: The "Diskless PC" Concept: Strategy and Implications

REFERENCE: Your Memo, dtd 12 Aug 87, Same Subject

1. We are developing our plans with respect to Diskless PCs on several fronts.

2. Last Friday we held the first of what we plan to be monthly coordination meetings with IMS/DO. The subject of Friday's meeting was the software environment for Diskless PCs. EG and IMS personnel are now developing plans, including alternatives, for the development and deployment of this environment. These plans will include scope of the necessary efforts to be undertaken by the EG and IMS and will be briefed to EG and IMS management prior to finalization.

3. We have also formed a LAN branch within EG/OPD, to be headed by Jim [redacted] STAT One of the first orders of business of this branch is developing a plan for the development of a standard set of Agency LAN architectures, consonant with the LAN Statement of Direction now on the table. The plan will specifically accommodate Diskless PCs, a standard user graphical interface, and the Agency's security requirements.

4. As you know, we are also in the process of acquiring a basic ordering contract for the Agency for a new family of workstations. One of the "reference configurations" in this solicitation is the Diskless PC. We anticipate being in a position to confirm that our architectural presumptions concerning the Diskless PC are valid by the middle of November.

5. We plan to have developed a complete picture of the implications of Diskless PCs and the planning for their support about 30 November, and will be prepared to brief it within the office at a convenient subsequent date.

STAT [redacted]