THE FOLLOWING DOCUMENTS
ARE ATTACHED:
(Please do not remove)

ER 4106 88
ER 4107 88
ER 4108 88
ER 4109 88
ER 4297X 88
ER 4305 88
OIT 1182 88

SUBJECT:

~~SECRET~~

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM: Edward J. Maloney Director of Information Technology [redacted] 25X1	EXTENSION	NO. OIT-1182-88	
		DATE	

TO: (Officer designation, room number, and building)	DATE		OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
	RECEIVED	FORWARDED		
1. EXDIR 7E12, Hqs.				
2.				
3. DDS&T 6E45, Hqs.				
4.				
5. D/OC [redacted] 25X1				
6.				
7. D/OS [redacted] 25X1				
8.				
9. D/OIR 2E60, Hqs.				
10.				
11. C/IMS 1D23, Hqs.				
12.				
13.				DCI EXEC REG
14.				
15.				B-209-IR

FORM 610 USE PREVIOUS EDITIONS

☆ U.S. Government Printing Office: 1985—494-834/49156

SECRET

OIT-1182-88
15 NOV 1988

MEMORANDUM FOR: ISB Members

FROM: Edward J. Maloney
Director of Information Technology

25X1 SUBJECT: Physical and Architecture Baseline Review [redacted]

1. We believe that the physical and architecture baseline diagrams that were presented at the November 3 - 4 ISB Offsite can be useful to both OIT and its customers as a common frame of reference for future planning. For this reason, OIT plans to publish, in early December, copies of our baseline report for distribution within OIT and to its customers. Before we do so, we would like to ensure the accuracy and completeness of the report. [redacted] 25X1

2. Most of the information the ATPS gathered to develop the physical and architecture baselines came from OIT databases and points-of-contact within the directorates. Sometimes available information sources conflicted, causing some of the data to be approximate rather than absolute. Since you are in the best position to know what you have, we would appreciate your review and validation. [redacted] 25X1

3. A complete copy of the report is attached. Please review the report, with particular attention to the diagrams for your directorate. Please have any requests for changes coordinated with the following directorate focal points and forward these to [redacted] C/ATPS/OIT, [redacted] 25X1 25X1

DCI
DO
DI
DS&T
DA and OC

[redacted]

Edward J. Maloney

Attachment:
Baseline Report

[redacted] 25X1

SECRET

SECRET

DRAFT

CENTRAL INTELLIGENCE AGENCY

INFORMATION SYSTEMS ARCHITECTURE BASELINE

NOVEMBER 1988

25X1

SECRET

Table of Contents

Executive Summary

This document presents the status of the Agency's information systems architecture.

The Agency is one of the most computer-intensive organizations in Government, particularly with respect to the pervasiveness of computer systems in all phases of our work. We have one of the Government's largest installations of computers and disk storage. Every day, we make extensive use of the capabilities of that installed plant in the collection, processing, analysis and production of our intelligence products.

Nevertheless, recent changes in information systems technology, particularly the trend to smaller systems that are deployed in new ways, have brought into question the way we organize our information systems activity and the way we implement our systems.

This document presents a high-level review of the present status of Agency information systems, intended as a starting point for further evolution of the Agency's information systems architecture.

The history of computing can be described by the central themes of each decade:

From 1955 to 1965 batch processing predominated, with jobs delivered to the computer for processing.

From 1965-1975 interactive computing became popular, with terminals used to provide access to mainframe computer centers.

From 1975 to 1985 distributed computing became popular, with minicomputers and personal computers providing user services and access to mainframe computers.

In the current decade, 1985 to 1995, we are observing the advent of true distributed processing.

The computer on the desktop is becoming ever more powerful, as it becomes in fact the "personal mainframe". In such an environment, the mainframe on the desktop will provide the bulk of all user services, with other computers operating as needed in the background.

From that historical perspective, many of the Agency's present information systems can be characterized as those of the 1965-1975 decade, terminaals connected to mainframes. Efforts are under way to enter the 1975-1985 decade, characterized by the connection of personal computers to minicomputers and mainframes.

The central systems planning that has been performed has been largely addressed to answering the question "how much more of the same shall we do next year?" A number of newer types of computing systems have "crept in" in some fashion, so that in some instances there can be said to be a "generation gap" between the central services and customers, with the customers employing more recent technology.

A variety of configuration management practices are employed for the central systems; they are effective at meeting the needs of the central service providers for orderly evolution of configurations. However, there is little or no configuration control for the growing body of computing equipment outside the central facility. There is also no connection between the central service configuration control and application developers outside the central service providers (for most applications), so there is no guarantee that an application will not suddenly cease operating because of a change made by central service providers.

Standards have been established for the methods for interconnecting computer systems for various purposes. However, there is no single configuration control board responsible for ensuring that those standards are followed in the implementation of Agency information systems. The only enforcement is conducted as part of OIT's review of purchase requisitions for computer equipment. This review takes place very late in the acquisition cycle, after major design decisions are made, at a time when procurement deadlines often preclude a thoughtful review. Systems that are developed under contract, or those that are implemented by staff personnel, never receive even this level of review.

The Agency's present information systems architecture shows total independence of design approaches for different systems, with some afterthought integration efforts. The central facilities have a great degree of uniformity because of the purchase of only IBM mainframes as the basis for central services. The mainframe equipment base is modern. Communications facilities to terminals and workstations support only the most primitive type of dumb terminal protocols. Network management of these facilities is very limited, with problem identification based on customer problem reports rather than continuous, automated monitoring.

Although the mainframe hardware base is modern, there are instances of obsolete technology that impede progress toward new communications approaches and the use of modern software technology: the GIMS database management system and Delta Data terminals.

The GIMS database management system, acquired in 1970, is a one-of-a-kind system supported entirely by the Agency that does not support modern terminals, communications protocols or database access standards. GIMS will not support any type of distributed database management application, or allow the use of a workstation to provide the user interface with the database system working in the background, without extensive Agency-funded development effort. Although there is a stated intent to move away from GIMS, there are no plans to move several large applications to more modern, commercial database systems.

Delta Data terminals, originally acquired in the 1970 time frame, are idiosyncratic and functionally obsolete. Support for this unusual terminal has required operating system changes that reduce the levels of availability delivered by Agency central systems. These changes cannot be carried forward into new operating systems that must be installed in order to make full utilization of the capabilities of presently-installed processors. There is a stated intent to replace Delta Data terminals; however, some Agency components have plans to continue the use of these terminals through at least 1993.

Agency computer security doctrines are based on the 1965-1975 computing approach of a dumb terminal connected to a mainframe, and are not adequate for an environment where the desktop machine is itself a powerful computer system that can store, process and transmit large amounts of information.

A particular policy question in the area of computer security deals with TEMPEST. In many cases, the Agency accepts a tremendous penalty of cost and support complexity, as well as lengthy delays in installation, because of the present TEMPEST policy. Other intelligence agencies have made changes in their TEMPEST policy that do not impose these problems.

This document is organized in five sections, with three appendices:

Section 1 is this Executive Summary.

Section 2 presents architectural baseline diagrams of present Agency information systems. These diagrams depict major Agency information systems and the principal interconnections between them.

Section 3 presents historical trends for growth of mainframe processing capacity and disk storage space, and reviews them with respect to historical trends in technology improvement.

Section 4 discusses configuration management. Present activities are presented, highlighting their strengths and shortcomings.

Section 5 reviews the Agency's position on information systems security.

The Appendices are:

A. Counts by Directorate of terminal and workstation equipment connected to central systems;

B. Counts by Office of terminal and workstation equipment connected to central systems and standalone;

C. A glossary of terms and acronyms used in this document.

Agency-Wide Information Systems Architecture Baseline

These charts depict the current status of Agency information systems. An *architectural* baseline view and a *physical* baseline view has been captured for the Office of the DCI and each directorate. The *architectural views* are high-level charts which emphasize system types and connections between systems. The *physical views* are lower-level charts, located in Appendix B, which give device counts in detail for each Directorate. In addition, charts depicting OIT's physical view, the Message Handling Architectural Baseline, and OC Worldwide Transmission Facilities have been included.

All the charts contain solid or dotted lines between the boxes at the points where connections are made. The solid lines represent existing connections. Dotted lines represent connections which are imminently planned and funded.

The first chart presents an architectural view of all Agency information systems. Subsequent charts expand views of communications, central services and directorate systems that are shown on this chart.

Each *architectural* view depicts system configurations for most standalone, clustered, and connected systems used by the directorate. The architectural view also indicates whether those systems have access to central services and if they do, how they are connected. The template explains how to read the architectural views:

o Box 1 on the left, shows most equipment types within the directorate and unless they are standalone, how they are connected to central services.

o Box 2 depicts Intelligence Community access to Agency supported systems such as CAMS, FOURC and DESIST. This box is the same for all architectural views.

o Box 3 represents communications. It contains two inner boxes; the first symbolizes communication transmission facilities, including satellite, fiber, leased lines and microwave. Further detail concerning the worldwide network is included on the OC Worldwide Transmission Facilities chart. The second inner box depicts message handling facilities, which are presented in more detail on the Message Handling Architectural Baseline chart. Box 3 is identical for all architectural views.

o Box 4 shows the CIA Computer Center to include CAMS, FOURC, SAFE and DESIST. A detail of this view is documented on the OIT Physical Baseline Chart. This box is identical for all architectural views.

Each directorate *physical* baseline view (in Appendix B) depicts the equipment resources, including equipment types and numbers for individual offices, staffs, or in the case of the DO, divisions. The "corporate level" represents general services. The "directorate level" represents large resources which are used almost exclusively by one directorate. In most cases there are at least two boxes within each component--the top box accounts for all devices connected to general services. Any boxes after the first account for equipment not connected to general services.

The *OIT physical* view lays out the numbers of mainframes, the amount of disk space, the number of COMTEN ports, and the quantity of controllers with numbers of connections available through the PBX for all Agency computer centers [redacted] 25X1

[redacted] 25X1

The communications *message handling* view depicts an expansion of the message handling boxes in both the physical and architectural views. This view depicts how message traffic is handled between headquarters and the foreign and domestic field.

25X1

Page Denied

Next 8 Page(s) In Document Denied

Capacity Planning

Our use of computing resources has grown steadily as we have exploited information systems technology to leverage the productivity of our people, so that we can deal with the explosion in the amount of information we must collect, process, analyze and deliver. There are some well-established trends in our growth in use of central processing capacity and disk storage capacity.

Central Computing Facilities

We currently have over 1400 billion characters of disk storage and 600 million instructions per second (MIPS) of general purpose computer power in our central computing facilities.

In order to visualize the amount of information stored in our central complex, consider that the average book holds about 400 characters per page, and a book about one inch thick has about 150 pages, so it holds about 60,000 characters. Thus, a conservative and rough estimate of the equivalent book storage of the amount of information in our central complex is more than 2.3 million books, or a stack of books 37 miles high, the height of more than 350 Washington Monuments!

The central processing power of 600 MIPS is more difficult to visualize. However, consider that in the early 1960's a computer with a processing capacity of .1 MIPS was considered fast and took up an entire computer room, and would rent for
25X1 roughly $500 per hour. [redacted]
25X1 [redacted]

Not shown on the chart is the growth processing power and disk storage capacity of desktop computers. Within the Headquarters compound, these machines now clearly have more aggregate processing capacity than the central complex; however, that capacity cannot be used as effectively as the capacity of the central complex, since it is not shared among a number of users.

Our mainframe computer utilization grows at a rate that is similar to those experienced in the private sector. Gartner Group reports that average annual growth in processing power for a typical Fortune 500 organization is in the 25% to 30% range and that disk space typically increases 38% to 43% annually.

The first chart shows the growth in total processing capacity of the IBM mainframe processors in the central complex, expressed in MIPS. Since the installation of SAFE, our rate of growth has been at a 34% compound annual growth rate (CAGR).

The second chart shows the total capacity of the disk storage units installed in the central complex, expressed in gigabytes (billions of bytes, where one byte is approximately one character). Our usage has grown at a 41% CAGR for some time.

The distribution of OIT central computing resources among the four directorates and the systems supported for the intelligence community is shown in the third chart. The estimates used for this chart are rough approximations, based on experience with the levels of use of various machines within the complex, rather than on detailed measurements.

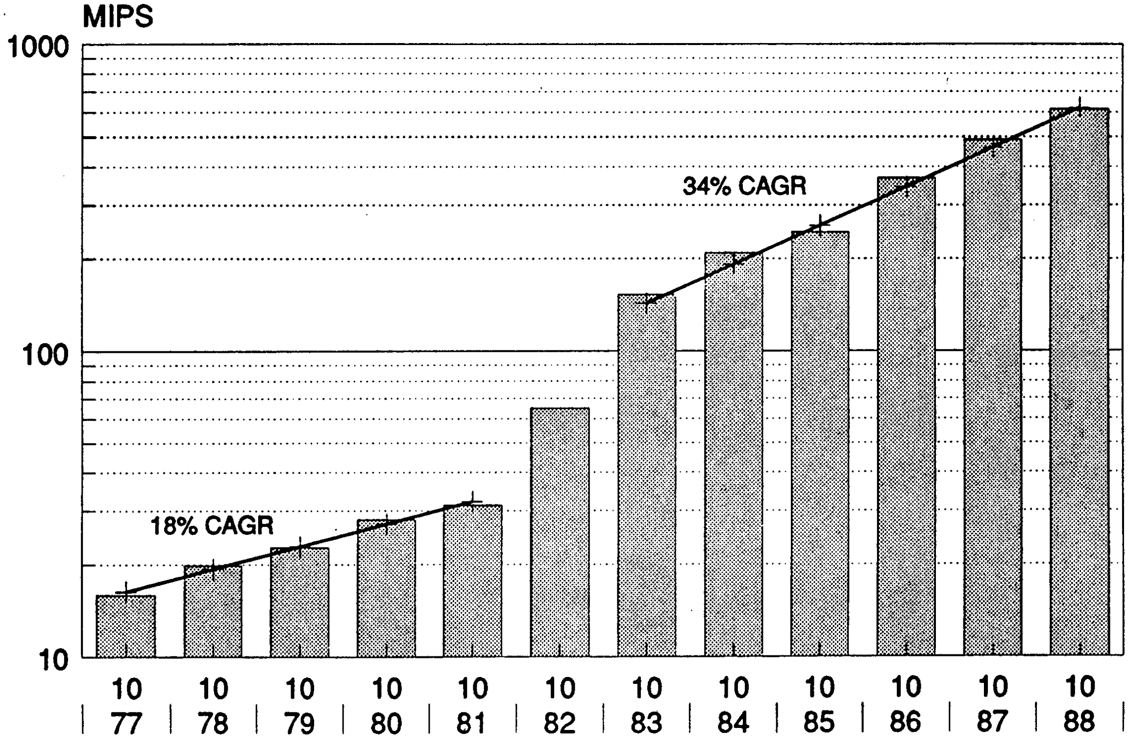
The chart of resource utilization among the directorates shows that the DI is a relatively large consumer of central processing power, even without considering the Cray system recently placed into production to support scientific computing requirements for that directorate, which is excluded from this chart. Central resource consumption by the DS&T is lower than the other directorates because most DS&T computing is performed with program specific systems, as can be seen in the architecture baseline diagrams.

Connectivity

The final chart in this section shows the availability of connections to central services for each directorate. The figures represent the number of workstations of each type which can be supported, and take into account the flexibility afforded by the new Intecom IBX compared to the previous practice of dedicating a port to each workstation. For these charts, the assumption was made that the average terminal is connected to the central systems for 60% of the work day. A higher usage rate would result in a smaller number of workstations that can be supported.

Increasing use of Systems Network Architecture to connect PCs and 3270 workstations in outbuildings is another factor improving connectivity, as Comten ports which previously connected a single workstation to the central computers will be capable of providing connectivity for eight users.

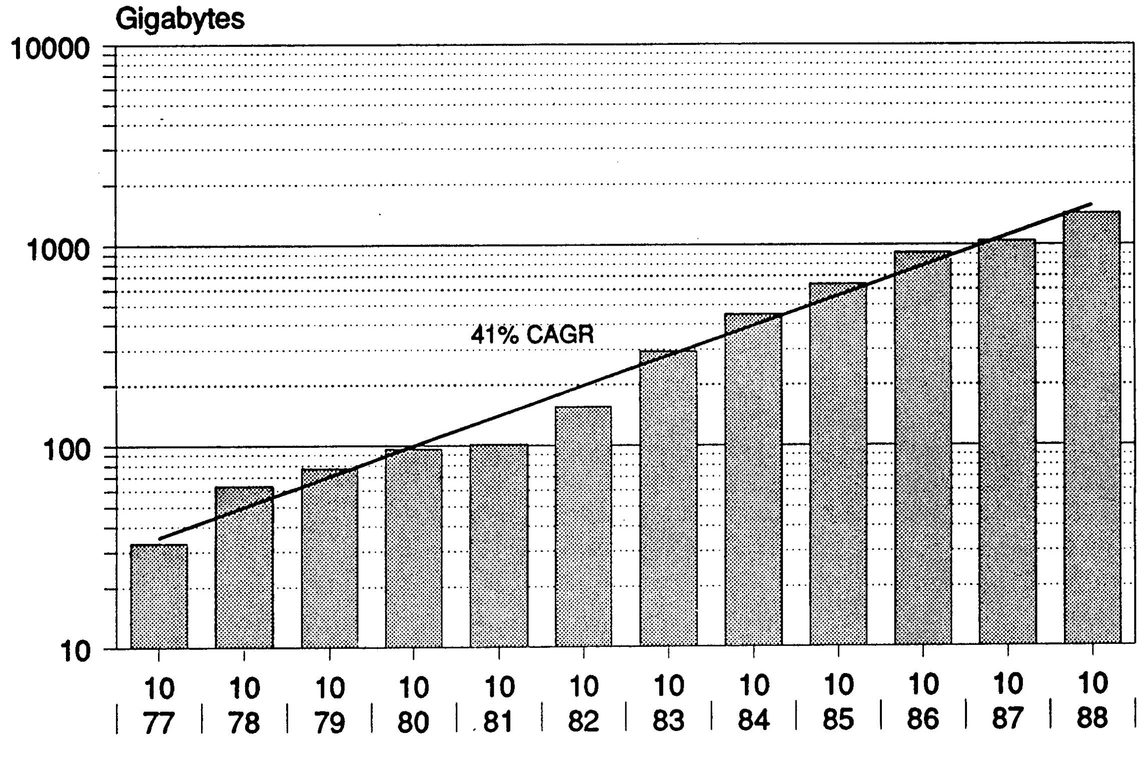
Total CPU Power (MIPS) of all OIT Mainframes



SECRET

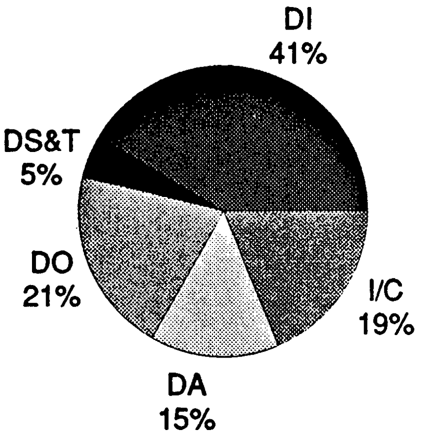
SECRET

Gigabytes of Disk Space for all OIT Mainframes

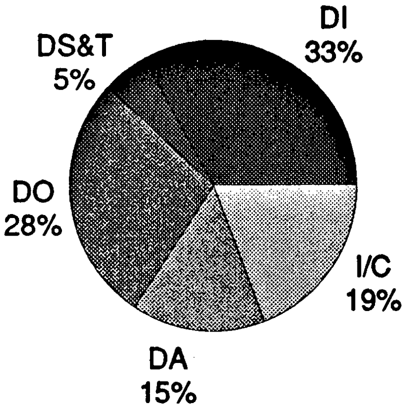


SECRET

OIT Mainframe Resource Allocation by Directorate



Processing Power (MIPS)



Disk Space (Gigabytes)

SECRET

25X1

Page Denied

Configuration Management

There are many different activities dealing with the configuration management of Agency information systems. These activities take place within OIT as the provider of central systems as well as within organizations that are the principal users of OIT central services.

Current configuration management of central services controls changes within dynamic, complex computer centers. OIT publishes a technical newsletter to announce major upcoming changes. However, users often build applications which run in the centers without being concerned about future changes to the platform. OIT does not formally inventory applications developed by users. Consequently, there is no direct communication to the user/developer about system changes that could potentially affect their applications.

Although an initial set of architectural standards has been established, the only enforcement for those standards takes place as part of OIT's review of procurement requests. This review has two limitations: the requests reach OIT very late in the procurement cycle, and many important information systems developments are not reached by that review process.

Procurement requests reach OIT as part of the review cycle before final contract award. The review package consists principally of procurement-related information, and often does not include information about the intended purpose of the acquisition, intended connections to central services or compliance with architectural standards. The reviewers thus have very little information, but are subject to tremendous time pressure because of the position of the review in the procurement cycle.

The OIT acquisition review includes only purchases of hardware and software over a value threshold, and all purchases of central processing units. However, it does not include computers that are purchased as part of a development project, nor does it cover activities such as application development that, while they may not involve sizable acquisitions, nevertheless need to be kept in conformance with architectural standards.

DA Configuration Management

OIT configuration management is controlled by the Information Technology Management Board (ITMB). The ITMB provides configuration management policy and direction to all groups within OIT. The Engineering Systems Group (ESG) is responsible for configuration management of major OIT-developed products and vendor-provided software. The Computer Operations Group (COG) is responsible for day-to-day operations and maintenance of OIT-supported computer centers. The Development Systems Group (DSG) is responsible for configuration management of OIT-developed application software such as databases. The Network Systems Group (NSG) is responsible for configuration management of the backbone communications network.

Configuration control of OIT supported computer centers is managed by the Services Management Board (SMB) within COG. The SMB meets monthly to review and approve implementation of baseline changes such as Request for Changes (RFCs) for both software and hardware for all groups in OIT.

Changes to OIT supported computer centers are scheduled by the Operations Scheduling Panel (OSP) within COG. This panel is chaired by COG, attended by ESG, other OIT components, and customer representatives from most service areas. The OSP is responsible for final coordination and scheduling of changes to system baselines.

Two management boards within Engineering Systems Group (ESG), the Engineering Services Group Management Board (ESGMB) and the Network Enhancement Work Station Management Board (NEWSMB) oversee configuration management for major OIT developed software and vendor- provided software. Individual Configuration Control Boards (CCBs) and Engineering Review Boards (ERBs) manage detailed configuration control for major activities such as VM, MVS, the Cray, AIM, SNA, MHF, IDMS/R, and SQL/DS.

In addition, ESG coordinates with Customer and Project Boards for immediate and tactical schedules, specifically for the DO Special Center, SAFE, CAMS and DESIST.

The Development Systems Group (DSG) practices consistent, formal configuration management throughout all their development projects. DSG has Configuration Control Boards (CCBs) and Engineering Review Boards (ERBs) established at the group and project level. These projects include BARS/CLAS, CAMS, DESIST, ELECTAS, FERS, HRS3, IAPS, and ICARE.

The Network Systems Group (NSG) has effective, less formal configuration management for different segments of the communications network. These segments include:

o microwave links,
o outbuilding communications equipment rooms,
o Headquarters multiplexor channel assignments,
o Headquarters Communications Operations Center Network Control Center and crypto equipment configurations,
o Headquarters Communications Operations Center Transmission Equipment.

DI Configuration Management

The Office of Information Resources, Planning and Development Division (PDD) is establishing a major configuration management effort for the Northside Computer Center, particularly the SAFE program.

DO Configuration Management

The Information Management Staff, Operations Systems Branch (OSB) has an effective configuration management program for Allstar. IMS contracts with QSI for configuration management of DI's SAFE equivalent, called MDS or Allstar Upgrade. OSB has recently been tasked to provide configuration management for other major DO programs in the Special Center.

DS&T Configuration Management

Configuration management conducted by DS&T is principally concerned with national programs. Each major program office conducts a wide variety of configuration control activities, including readiness review boards, engineering review boards and configuration control boards. Those activities are outside the scope of this document, since those systems, although they include computer systems, employ the computer systems as embedded parts of collection systems rather than as general-purpose information processing systems that are available to a wide population of users.

Computer Security

This section reviews the Agency's computer security status, with respect to the present status of computer security measures in place to protect Agency information systems and the Agency's computer security policy.

Systems

There is an National Telecommunications and Information System Security Committee (NTISSC) directive for all multiuser information systems that process classified information to meet the C2 level of certification, as defined by DOD 5200.28, "Department of Defense Trusted Computer System Evaluation Criteria" by 1992. The new DCI Directive in this area, DCID 1/16, specifies C2 as the set of criteria to be used in evaluating our system-high systems. In order to evaluate the current posture of Agency systems, in 1987 the Office of Security used the C2 criteria to evaluate a number of present Agency systems. The criteria are:

1. Discretionary Access Control--Control access to named system resources by named users, in such a way that it limits the propagation of access rights.

2. Object Reuse--When work areas are no longer in use, they are to be cleared, and all authorizations to their use are to be revoked before access is given to a different user.

3. Identification and Authentication--All users are required to identify themselves before undertaking any other actions, and a protected mechanism is to be used to authenticate user identities, with authentication data inaccessible to other users.

4. Audit--Create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to all protected system resources.

5. System Architecture--Maintain a domain for execution of the control software that is free ffrom external interference or tampering.

6. System Integrity--Hardware or software features are required that can be used to verify correct operation of the protection mechanisms.

7. Security Testing--The security mechanisms must be tested to establish that they operate as described in system documentation.

8. Security Features Users Guide--User documentation must be provided that describes the protection mechanisms, guidelines on their use and how they interact with one another.

9. Trusted Facility Manual--A manual addressed to the system administrator must present cautions about functions and privileges that should be controlled when running a secure facility, including detailed information on the use of the audit trail facility.

10. Test Documentation--The system developer must provide a document that describes the test plan and procedures used to test the security mechanisms, and the results of such testing.

11. Design Documentation--Documents must be provided that present the system developer's philosophy of protection and how it is implemented in the system.

The Office of Security surveyed major Agency information systems in 1987 with respect to these criteria. Eleven Agency systems were surveyed: General Services, [redacted] Special Center and Personal Computers. 25X1

25X1

[redacted]

Policy

There are strong reasons to increase our use of computer systems. Computers give us the opportunity to increase our ability to deal with an ever-growing volume of information data that must be collected and analyzed to deal with new intelligence requirements that we face. We also realize that expensive, manual means of doing business can be automated to save time, personnel and transportation costs, at the same time providing enhanced security. Paradoxically, we also know that some of the means for apparently enhancing security are not effective.

25X1

25X1

[redacted]

25X1

During the eighties, the Agency experienced substantial growth. One need only compare the DI of ten years ago to today's to see how the number and sophistication of Agency staff using computers has been extended. During that same period commercial, academic and industrial concerns have increased their information collection activities, so that they now provide a valuable source of open information for the intelligence analyst. Likewise, the Agency's capability to collect and analyze information and produce finished product has grown, and its product is considered vital by a wider body of Government decision-makers.

25X1

The terminal policy [redacted] is no longer adequate. Technology and our mission requirements have advanced to the point where we need to go beyond the use of dumb terminals. Computers small in size but large in capability are replacing them. These computers can connect to large, remote databases across large distances, can support distributed processing on a large scale, feature cheap reliable removable media and components, and are no longer slaves of a host computer. Easily-installed vendor products, particularly software, have become available--there are database systems costing $400 today that far exceed the capabilities of systems costing $400,000 in 1975.

The Agency is increasingly acquiring commercial off-the-shelf software products, moving from systems supported and maintained by Agency staff to commercial products built, maintained and supported by others. In many cases, products are acquired and used with little understanding of what the product actually does, how it was built, who built it, or how it is maintained. It has become very clear that whoever actually issues the command to a software package, in truth the original author of the software package is in control. This problem is now an international concern, particularly with inexpensive (and even free) personal computer software, some of which is also malicious and capable of attacking attached systems (e.g. Trojan horse, virus, worm, crab, mockingbird).

We need standards for assessment and management of computer security. Computer security professionals have become aware that much of the folklore of the past was just plain wrong. When computer systems did noot connect to one another these problems could not cause much damage; but with the advent of open system architectures, reduced software costs, increasing miniaturization, and rapidly evolving systems, the risk is real. Covert means of information extraction, communication, and penetration have been demonstrated; direct access to the operational computer is not necessary, and centralized databases render more data vulnerable. Change has become so easy that one must wonder whether anyone really knows what the Agency is connected to, what its machines are doing, and whether it has changed since the last time anyone checked. Standards for each phase of the system life cycle, with appropriate controls, are necessary.

A broad Agency information security program is needed. As information technology has advanced, the Agency's information security stance has changed little, computer security even less. A broad but practical change in the way information security is approached is needed. A practical, cost-effective overarching security policy, based on the best available security theory, practice and technology, addressing the full system life cycle, is needed. The answer to computer security problems does not lie in current agency security policy, the answer is not in magical black boxes (guards and filters--though they are useful) and other security afterthoughts, but rather in architectures, and systems implementing those architectures, engineered, structured, and operated for security from the beginning. The primary issues in such architectures and systems are access control, system assurance supported by configuration management and accountability. Addressing these issues requires, first of all, a broad training and awareness program, for technicians, managers and end users, and policy.

25X1

[redacted]

A coherent system security process is needed. The various domains of security (physical, communications, emanations, personnel, computer, technical surveillance countermeasures) are currently addressed in an independent and non-integrated fashion. Security is often in conflict with system requirements as well. The attitude needs to be established for a system life cycle view. Security specialists and generalists need to work with system developers, and need to be readily accessible during system operation and maintenance. All domains of security need to be considered together, inspections need be done together, assessment needs to be performed together, and developmental certifications need to be given as to the entire security status of systems. A formal, but not bureaucratic, process needs to be established to ensure proper management approval for information system security throughout the system life cycle.

New technology and products can help. Technology is being developed to provide assurance of correctness, accountability and compartmentation. While no technology is secure in itself, with appropriate knowledge, awareness, structure, attention and mechanism this incipient technology can be used to implement well-structured systems that can be operated at low risk. There will always be a final managerial judgment as to whether a particular technology provides adequate enhancement to operate a system with an acceptable level of risk.

Appendix A: Equipment by Directorate

The chart presented in this Appendix shows the total equipment complement by Directorate for PC's, Delta Data terminals that are connected to central services, or for Wang terminals, that may or may not be connected.

There is additional equipment in the form of Xerox 2700 printers that are connected to central services and Wang printers that may or may not have connections to central services.

Appendix B: Equipment by Office

The charts of this Appendix present the equipment complement for each Directorate, itemized by office, or in the case of the DO by division. Because of the large number of separate equipment counts that are presented, and the varying framework for each Directorate that is required because of their rather different equipment complements, this information is presented as a series of diagrams, called physical views of each directorate. The emphasis of these charts is the equipment complement, in contrast with the architectural views presented in the body of the report, that emphasized connections rather than equipment.

The *corporate level* shown on each chart represents general services. Shown as *directorate level* are substantial resources that are used almost exclusively by one directorate. For most of the charts, there are at least two boxes within each component--the top box accounts for all devices connected to general services. Any boxes below the top box account for equipment not connected to general services.

25X1

SECRET

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
MINUTES, ISB OFFSITE

25X1 FROM: [redacted] 25X1 SA/EXDIR 7E12 HQS	EXTENSION [redacted]	NO. ER 4305-88 DATE 14 November 1988

TO: (Officer designation, room number, and building)	DATE		OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
	RECEIVED	FORWARDED		
1. ER				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				DCI EXEC REG
15.				B-209-IR

SECRET

☆ U.S. Government Printing Office: 1985—494-834/49156

SECRET

ER 4305-88
14 November 1988

MEMORANDUM FOR: Information Systems Board

25X1 FROM: [redacted]
Special Assistant to the Executive Director

SUBJECT: Minutes, ISB Offsite - 3,4 Nov 1988

25X1 The ISB offsite conference was held [redacted] on 3,4 November. The focus of the conference was on Information Systems Architecture and Security with presentations by the Architecture Working Group and by the Office of Security's Information Security Group. Copies of each of the briefings are attached with the exception of the baseline architecture which has been sent under separate cover to attendees.

The Executive Director opened the session with a review of the ISB's directions and accomplishments. Discussion centered on the need for an update to the ISB charter.

25X1 [redacted] Chief of the Office of Security's Information Security Group, discussed the approach to and status of a strategic plan for information system security. The Information Security Policy Panel with membership from each Directorate, is the coordinating body for this plan. The plan is scheduled to be completed in February '89.

25X1 [redacted] Deputy Director of the Office of Communications, presented a current view of the overseas communications architecture and a summary of future challenges.

Mr. Ed Maloney, Director of the Office of Information and Technology, reviewed recent accomplishments by the Office and discussed the technical and management challenges OIT faces from a near term, intermediate and long range perspective.

25X1 [redacted], Chief of OIT's Architecture and Technology Planning Staff presented a well received view of the Agency and Directorate baseline architectures. This effort represents the first step in the development of an 1993 Agency information systems architecture.

25X1 [redacted] member of the Electronic Processes Study Group, presented the results of the team's examination of the Agency's movement toward an all-electronic office environment. The group pointed out that the process is underway in an unstructured way and is gaining momentum. The essence of their recommendation is that we must insure that this process is accomplished in a controlled and consistent way and in a way which assures accessibility by all employees.

The list of actions resulting from the conference is attached.

25X1 [redacted]

25X1 [redacted]

SECRET

Attachments:

1. Agenda
2. EXDIR charts
3. Security Briefing
4. OC Briefing
5. OIT Briefing
6. EPSG Briefing
7. Action Items

25X1

[redacted]

[redacted]

25X1 DCI/EXDIR [redacted] (10 Nov 88)

Distribution:

1 - EXDIR, 7D55 HQS
1 - ADDS&T, 6E56 HQS
1 - Comptroller, 7C21 HQS
1 - C/IMS, 1D4109 HQS
25X1 1 - D/OIT [redacted]
1 - D/OC,
1 - D/OIR, 2E60
25X1 1 - D/OS, [redacted]
1 - DDA, 7D24 HQS
25X1 1 [redacted]
1
1
1
25X1 1 [redacted] 6E56 HQS
1 - Executive Registry
1 - ISB File

25X1 [redacted]

[redacted]

ISB OFFSITE
NOVEMBER 3-4, 1988

AGENDA

Thursday, 3 November 1988

	1830 - 1845	Opening Remarks.	Jim Taylor
25X1	1845 - 1930	Information Security Strategy.	[redacted]
	1930 - 2000	Discussion	

Friday, 4 November 1988

25X1	0800 - 0845	Communications Directions.	[redacted]
	0845 - 0945	Information Technology Directions.	Ed Maloney
	0945 - 1000	Break	
25X1	1000 - 1200	Agency Information Systems Architecture.	[redacted]
	1200 - 1300	Lunch	
	1300 - 1345	Electronic Processes Study Group.	
	1345 - 1445	Executive Discussion and Closing Remarks	Jim Taylor

25X1 [redacted]

Attachment 1

Executive Director

Opening Remarks

Attachment 2

25X1

25X1

25X1

Page Denied

25X1

25X1

25X1

25X1

ISSUES ISB HAS GRAPPLED WITH	ACTIONS	RESULTS
SENSE OF VISION AND LEADERSHIP	INFORMATION SYSTEM POLICY	REASONABLY SUCCESSFUL
MORE EFFECTIVE PLANNING PROCESS	INITIATED STRATEGIC PLANS	GOOD START, WHAT NOW?
MORE EFFECTIVE DECISION MAKING	DISCUSSIONS (WORKSTATIONS)	MOSTLY INEFFECTIVE
CLEARER ROLES; ACCOUNTABILITY	DISCUSSED AT LEAST ONCE	NO IMPACT
ARCHITECTURAL STRATEGY	FOCUSED ATTENTION ON AWG	BABY STEPS
STANDARDS	AWG	EASY ONES APPROVED
INVESTMENT STRATEGY	SOME DISCUSSION	BETTER, STILL LIMITED UNDERSTANDING
SECURITY	REQUESTED SECURITY STRATEGY	SLOW, BUT PROGRESSING
EFFECTIVE NETWORK MANAGEMENT	CONCERN, BUT NO FOCUS	
CONFIGURATION MANAGEMENT	CONCERN, BUT NO FOCUS	
ENFORCEMENT OF STANDARDS	SOME DISCUSSION	LOOSE UNDERSTANDING OF PROCESS
EFFECTIVE USE OF CRITICAL SKILLS	SUGGESTED IS CAREER SERVICE	FOUNDERED
EFFECTIVE USE OF ELECTRONIC MEDIA	EPSG CHARTERED	REPORTING TOMORROW
COMMUNICATIONS	PROPOSED WORKING GROUP	
CORPORATE DATA BASE	SOME DISCUSSION	DIRECTORATE ISSUE?

INFORMATION TECHNOLOGY

. Direction and pace of technology, complexity of our decision making process, need to assure capability to accomplish work at the component level, and ability to adapt rapidly to customer needs, all argue for:

- overall strategy which includes emphasis on support for work groups
- more desktop computing power as customers need it
- effective and accountable network management

. Such a decentralized strategy has much to recommend it, but we need to ensure that:

- component-acquired systems will talk to other component-acquired systems and to our mainframes
- we can guarantee adequate end-to-end system performance
- nobody can unilaterally take an action adversely affecting the performance of the whole system
- we don't spend more on maintenance and training than we need to
- we achieve reasonable balance in our component investment programs
- we don't support one component's needlessly expensive approach at the expense of others
- our security environment is understood and our security interests are protected

. To accomplish our mission then we need:

- improved overall central management attention and direction
- effective planning process
- effective investment review and financial control
- participative development of selected standards, and rigorous enforcement
- effective network management and control
- effective security policy and rigorous implementation of this policy
- thoughtful maintenance arrangements

ISB CHARTER UPDATE

EMPHASIZE RESPONSIBILITY FOR ENSURING:

o DEFINITION OF AGENCY INFORMATION SYSTEM NETWORK

.. BASELINE ARCHITECTURE

.. FUTURE ARCHITECTURE

o EFFECTIVE SUPPORTING PROCESSES AND PROGRAMS

.. SECURITY STRATEGY AND POLICY

.. DIRECTORATE AND AGENCY PLANNING PROCESS

.. INVESTMENT STRATEGY

.. CONFIGURATION CONTROL

.. CHANGE MANAGEMENT

JHT
11/3/88

Office of Security

Strategic Information Security Plan

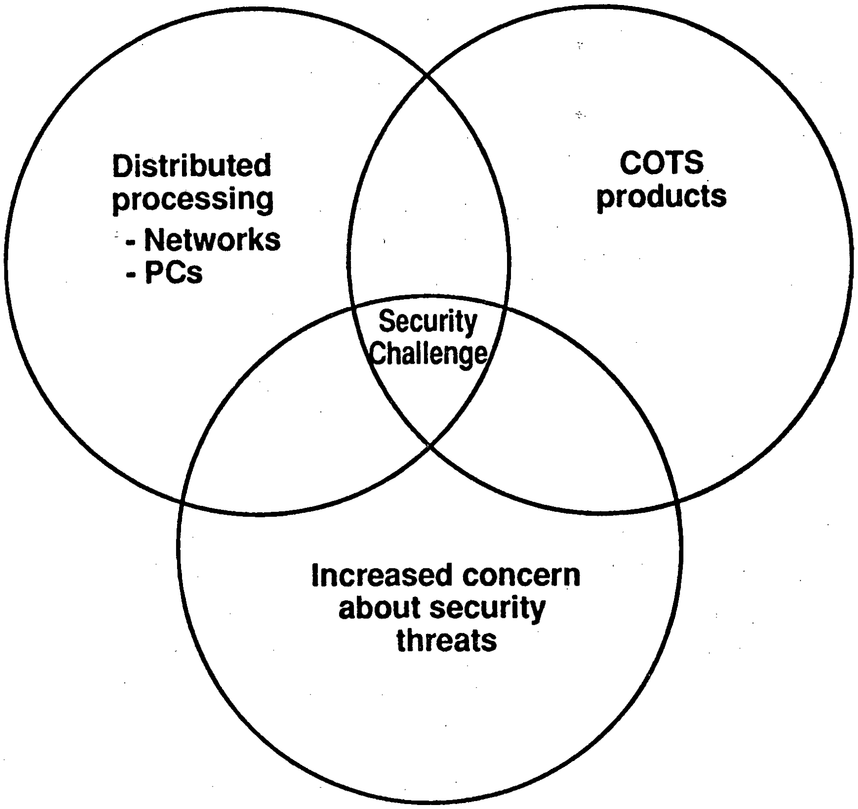
Attachment 3

AGENCY INFORMATION SECURITY STRATEGIC PLAN

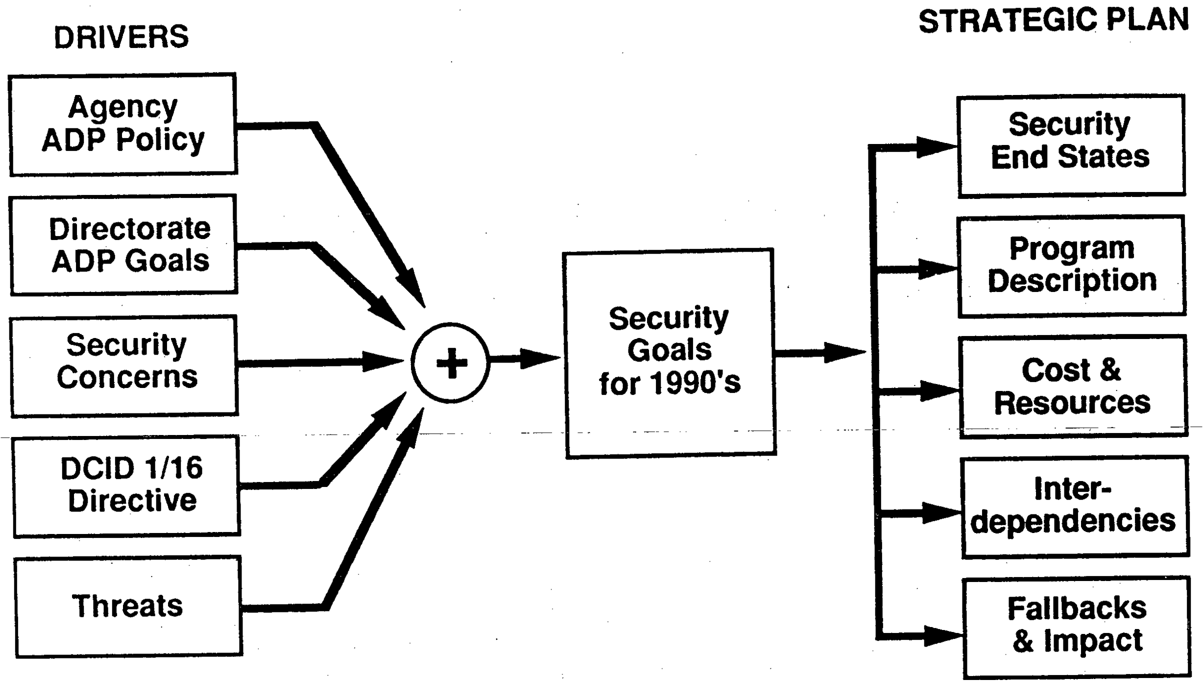
Status and Security Goals

3 November 1988

Major Trends



Information Security Strategic Plan



DRIVERS

Agency ADP Policy

Directorate ADP Goals

Security Concerns

DCID 1/16 Directive

Threats

+

Security Goals for 1990's

STRATEGIC PLAN

Security End States

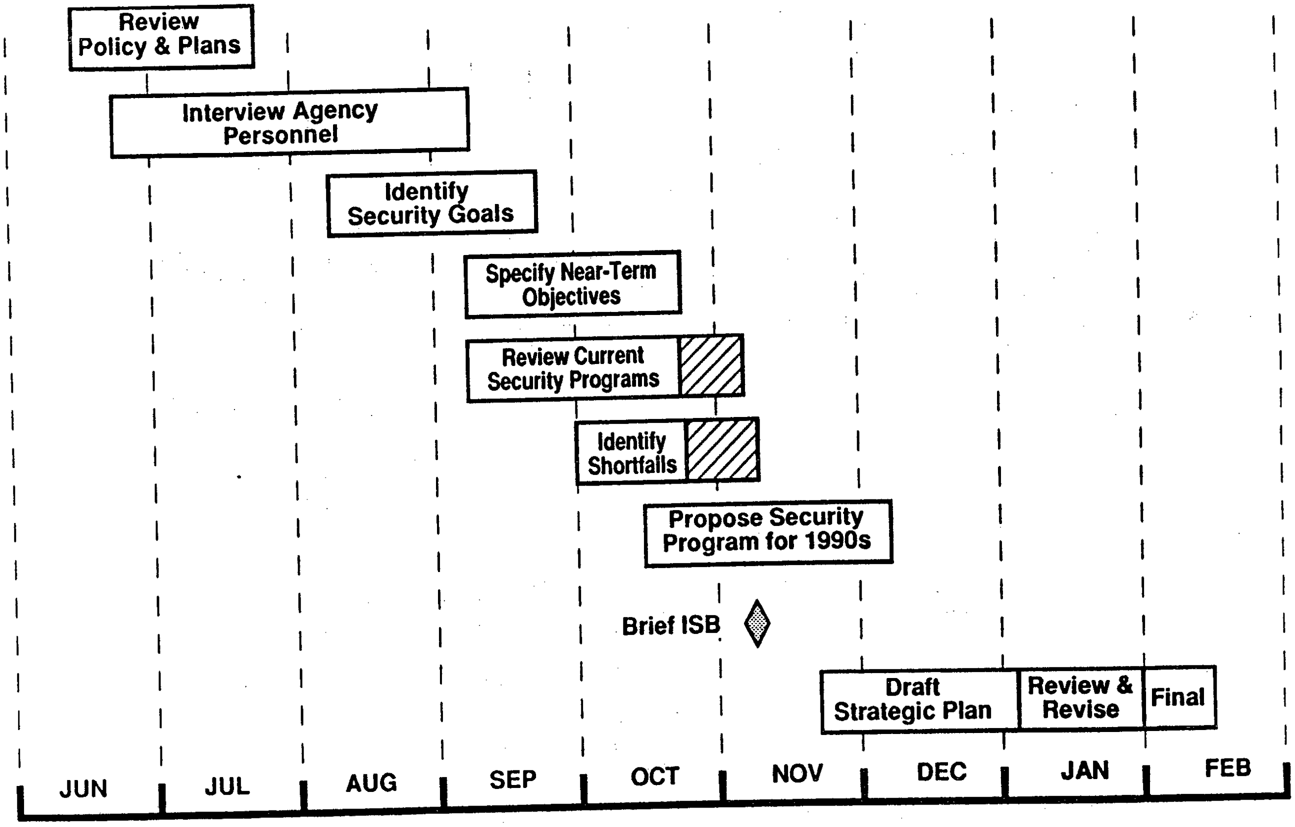
Program Description

Cost & Resources

Inter-dependencies

Fallbacks & Impact

Security Plan Activity Schedule



Review Policy & Plans

Interview Agency Personnel

Identify Security Goals

Specify Near-Term Objectives

Review Current Security Programs

Identify Shortfalls

Propose Security Program for 1990s

Brief ISB

Draft Strategic Plan

Review & Revise

Final

ANALYSIS OF SPECIFIC SECURITY NEEDS AND CONCERNS

- Interviews (32)
  - Senior Managers -- EXDIR, ISB, ISPP, senior staff (17)
    - Emphasis: Threats, issues, needs, goals
  - OS -- Deputy directors, group & division chiefs, ISG staff (15)
    - Emphasis: Current information security activities, roles, responsibilities
- Reviewed directorate strategic plans and related documents
  - 1984 Computer Security Investment Strategy report
  - DCID 1/16 computer security directive
  - Threat 88

STAT

Page Denied

Next 1 Page(s) In Document Denied

SECURITY PROGRAM NEEDS (CONCLUDED)

- In-house computer security technical support
- Awareness and training
- Secure multi-level systems (downstream demands)
- Keep up with security impact of new ADP technology

AGENCY INFORMATION SYSTEM SECURITY GOALS

1 - Robust access controls on media, systems and networks

2 - Effective audit trails on media, systems and networks

3 - Enhanced computer security awareness program

4 - Information security standards and rules promulgated

5 - Systems life-cycle security program across the directorates

6 - Professional cadre of trained computer security specialists

Access Control Objectives

Immediate	Near Term	Downstream
• Strengthen security controls on insertion & removal of magnetic & other media • Devise more effective means for monitoring hardware & software maintenance • Establish approval procedures for unclassified external connections • Provide for encryption of data on magnetic & other media (limited test environment)	• Provide access control mechanisms that implement compartmentation & need to know • Provide secure maintenance facility for critical systems • Provide access control mechanisms for classified external connections e.g., guards • Implement test bed to address network security & connectivity issues • Provide for encryption on selected PCs & departmental systems • Protect Agency systems from virus & other denial of service threats	• Implement AIS controls for multiple compartments • Provide modern, secure maintenance tools • Improve user authentication e.g., electronic/ biometric devices • Develop & test multi-level controls • Implement universal file encryption • Implement end-to-end encryption capability over PBX & other networks - Terminal to terminal - Terminal to mainframe

Key: **Fully met** ▨ Partially met by an existing program

Audit Objectives

Immediate	Near Term	Downstream
• Evaluate & install tools for automated analysis of audit trails	• Implement enhanced audit trail analysis tools	• Develop & implement near real-time monitoring & analysis of system activities
• Define core system audit requirements for mainframe and departmental systems	• Implement comprehensive corporate audit requirements	
• Define network audit requirements	• Develop & implement network audit	
• Strengthen accountability for magnetic & other media		

Key: **Fully met** Partially met by an existing program

Security Awareness Objectives

Immediate	Near Term	Downstream
• Develop program for increasing awareness of security technical issues among systems development personnel • Expand & increase the frequency of computer security awareness briefings for managers, system users, and system support personnel; include new topics such as viruses	• Implement awareness program for systems developers	

Key: **Fully met** Partially met by an existing program

Security Standards Objectives

STAT

Immediate	Near Term	Downstream
• Update security policy [redacted] • Develop system security handbooks for user operations & maintenance - headquarters - field - contractor sites • Develop system security engineering guidelines	• Define minimum security technical requirements for connections of: - Agency users to Agency networks - External users (contractors, IC members) to Agency systems & networks - Agency users to external systems, networks	• Define a policy & minimum requirements for processing multiple compartments
	• Define a standard on classification markings (labeling) of information in Agency systems	

Key: Fully met Partially met by an existing program

System Life Cycle Objective

Immediate	Near Term	Downstream
• Define computer security roles & responsibilities within the Agency	• Develop security plan for every AIS	• Verify & accredit every Agency AIS per DCID 1/16
• Designate a system security officer for every production system	• Include computer security requirements in every Agency AIS acquisition	• Implement year 2000 DCID 1/16 requirements
• Implement special personnel security screening for sensitive AIS positions	• Define a method for uniform risk assessment	
• Provide security product assessment and consultative services to Agency system designers & operators		
• Assess the impact of emerging AIS technology on security		

Key: **Fully met** Partially met by an existing program

Professional Cadre Objectives

Immediate	Near Term	Downstream
• Recruit experienced computer scientists	• Recruit experienced computer scientists	• Recruit experienced computer scientists
• Define categories of computer security specialists	• Train & deploy OS computer security officers to key components	
• Initiate basic training program & certification of operational system security officers	• Implement advanced training program	
• Define advanced training requirements for technical computer security specialists		

Key: Fully met Partially met by an existing program

25X1

NECESSARY FOLLOW-ON ACTIVITIES

- Write operational plans in accordance with Agency Computer Security Strategic Plan
  - Audit program plan (OS)
  - Data encryption program plan (OC)
  - Wang network program plan (OS)
  - Various Directorate program plans (as appropriate)

STAT

Page Denied

Office of Communications

Directions and Issues

Attachment 4

SECRET

OFFICE OF COMMUNICATIONS

COMMUNICATIONS DIRECTIONS

ISB Off – Site, 4 November 1988

NETWORK STATUS

CHALLENGES

"FORECAST 2000" PREDICTIONS

SECRET

OC – DCO – 826 – 11/88

MERCURY SERVICES

- MESSAGE SWITCHING SUPPORT
- DATA SUPPORT
  - FACSIMILE
  - VOICE FORWARDING
  - GRAPHICS
  - IMAGERY
  - INTERACTIVE TERMINAL

25X1

SECRET

MESSAGE RELAY SYSTEM

STATUS

CURRENT:

CODE & TEST	
INTEGRATION W/PSS & ENS	DEC 88
HQS INSTALL	SEP 88
25X1 [redacted] INSTALL	FEB 89
OPERATIONAL CUTOVER	
HEADQUARTERS	3rd QTR FY–89
25X1 [redacted]	1st QTR FY–90 FY–90

SECRET

CONFIDENTIAL

CRISIS COMMUNICATIONS

- **RETAIN PRESENT UHF CAPABILITIES**
- **PARTICIPATE IN DoD "FOLLOW – ON" EFFORT**
- **MORE EFFICIENT USE OF PRESENT SYSTEMS**
- **IMPROVE LINK ROBUSTNESS**
- **EXPLOIT COMMERCIAL SYSTEMS**
- **EXPLOIT ALTERNATE SYSTEMS**

CONFIDENTIAL

CONFIDENTIAL

NMSDB OBJECTIVES

- DOCUMENT NETWORK USERS, NODES, AND EQUIPMENT
- DOCUMENT NETWORK SERVICES AND CIRCUITS
- DEFINE PRIMARY, ALTERNATE, AND CONTINGENCY CIRCUITRY
- ENABLE MANAGERS TO OBTAIN TIMELY AND ACCURATE CONFIGURATION REPORTS
- PROVIDE BASIS FOR FUTURE REAL–TIME MONITORING AND REPORTS ON NETWORK FACILITIES
- PROVIDE BASIS FOR GRAPHIC NETWORK DISPLAYS

CONFIDENTIAL

OC – ED – 1024 – 10/88

CONFIDENTIAL

NMS DATABASE – STATUS/PLAN

- PROTOTYPE SOFTWARE AND DOCUMENTATION DELIVERED – AUG 88
- DEPLOYMENT
  - BEGIN TEST NETWORK [redacted] – DEC 88
  - BEGIN OPERATIONAL DEPLOYMENT – JUN 89
- OUTYEAR PROGRAM PLAN – JAN 89
- CEMS INTERFACE SPEC – JAN 89

25X1

CONFIDENTIAL

SECRET

CHALLENGES

- **SUSTAINING CAPITALIZATION**
- **COMMUNITY RELATIONSHIPS**

25X1

[redacted]

- **IMPROVED SECURITY**
  - **Key Management**
  - **End – to – End Encryption**
- **CUSTOMER DEMAND**
- **TRANSITION TO NEW SERVICES**
- **MAINTAINING AND IMPROVING OUR SKILLS BASE**
  - **Agency Backbone Network**
  - **Special Programs Support**

SECRET

Page Denied

Next 1 Page(s) In Document Denied

Office of Information and Technology

Directions and Issues

Attachment 5

CONFIDENTIAL

Office of
Information
Technology

1988 Achievements

- Computer Center Moves
- CRAY
- Desist

25X1 [redacted]

- Video Conferencing
- Link-1 Network Mgmt System

(Continued)

MG-197-11/88

CONFIDENTIAL

CONFIDENTIAL

Office of
Information
Technology

1988 Achievements
(Continued)

- O Non-Text SVC Center
- O ELECTAS
- O Applicant Processing
- O Claims Processing
- O PBX
- O Adaptive Technology Awareness Day

CONFIDENTIAL

Office of
Information
Technology

Short-Term

(1-2 Years)

○ Management/Organizational

○ Information Management

○ communication

○ Computing

CONFIDENTIAL

Office of Information Technology

Short-Term Organization/Management

Return to Basics

- O communication (c)
- O Training
- O Resume Hiring
- O Develop A Strong Rqmt/Plan/Budget Function
- O Strengthen Career SVC (Occup. Panels)
- O Build Long Range Plan to Provide Customer Services Locally
- O Review Lines of Command

MG-199-11/88

CONFIDENTIAL

Office of
Information
Technology

Short-Term Organization/Management (Continued)

Network View

- O Availability
- O Connectivity
- O Simplicity
- O Strengthen CM
- o STANdARds

CONFIDENTIAL

Office of
Information
Technology

Short-Term
Information Management

- Expand Training for MZIers
- Develop Proposals for Archiving Policy
- Electronic Records
- Develop & Begin Plans for Improved Registry Support

CONFIDENTIAL

CONFIDENTIAL

Office of
Information
Technology

Short-Term Communication

○ Move & Upgrade Comm. Center

○ Continue to Integrate PBX Technology

○ Introduce Additional Voice Function

25X1

[redacted]

○ Develop Wash. Area Integrated Voice/Data Net

CONFIDENTIAL

Office of
Information
Technology

Short-Term Computing

○ Training

○ Availability

○ VM-XA

○ Develop Plan Against Architecture

Office of
Information
Technology

Mid-Term
1993

○ Communication

○ Information Management

○ Computing

CONFIDENTIAL

Office of
Information
Technology

Long Term
(~~1988+~~) 1998+

- ○ Architecture Baseline Controls
- ○ Network Management
- ○ Communication Backbone
- ○ C~~o~~entral Data Warehouse
- ○ C~~o~~entral Mainframe Operations For Data and Special Processing
- ○ Use of U.S. Facilities to Deploy Data Storage and Office Processing
- ○ Different Organization Structure

CONFIDENTIAL

Electronic Processes Study Group

Report

Attachment 6

Electronic Processes Study Group

Using Electronic Processes For Everyday Activities

Briefing to ISB
4 November 1988

[redacted]

STAT

Page Denied

Background

Problem Statement

Draft Policy

Risks of Implementation

Recommendations

EPSG Future

Background

Primary Focus

- Electronic processes today
- Records management requirements

Related Issues

- Architecture
- Automating specific forms
- Managing electronic documents

Problem

Agency resources cannot keep pace with growth in information

- Focus has been on solving substantive problems with technology
- Lack of management focus on everyday processes
- We need to develop a policy for automating these processes

Draft Policy

The Agency will promote electronic systems for everyday processes by:

- Providing connectivity for each employee to any other employee
- Providing an electronic inbox and outbox for each employee
- Providing every employee access to a consistent set of of electronic tools and services at their workstation
- Encouraging all employees to use electonic documents for communicating and conducting Agency business

Risks of Implementation

- Information stored electrically can be more difficult to retrieve
- "Management by Walking Around" could become a lost art
- Inadequate records management could result in loss of information
- We could exceed our capacity for storage, transmission, or processing of everyday information
- Changing technology could make older electronic records inaccessible
- Electronic information may not be admissible as evidence
- The security risks may be perceived to be greater than with paper

These risks are not new
They can be overcome

Recommendations for the ISB

- Publish Policy as a Headquarters Notice
- Establish a goal that the architecture will support the policy
- Set a date when connectivity will be accomplished

General Recommendations

- Promote the continuing development of Agency standards for electronic connectivity. New systems must include the "hooks" needed to connect with other Agency systems.

- Every employee should be provided with an electronic inbox and outbox which are connected both within and outside the local work group to send and receive the information needed to perform their everyday processes.

2058-89

Recommendations

- Each directorate should provide a node (electronic address) that is the entry point to their architecture, such as exists in the DCI and DDS&T areas.

- Each directorate should provide an electronic registry that is the default recipient for all electronic messages not specifically addressed to an individual.

Recommendations

- The Agency should provide a standard set of electronic tools for requesting services
- The services providers must process requests received through the network regardless of originating system
- Service components should give priority to processing requests submitted by electronic means. All correspondence between the service provider and requester should be via electronic means.

Recommendation

- Broaden the interpretation of the term "Official Business" to include computer activities which promote interpersonal communications and are not prohibited by law (e.g., no use for personal gain or for illegal activities).

Recommendation

The Agency should not wait to resolve the connectivity problem before developing an aggressive schedule/plan to start automating everyday processes, beginning with memos, cables, and common Agency forms.

EPSG Future

- Propose policy for managing electronic records
- Re-formulate recommendations so that Directorates can capture them in their ADP strategic plans

2063-89

STAT

Page Denied

Actions

Attachment 7

14 Nov 88

Actions:

1. The Executive Director will draft an updated ISB charter for presentation at a future meeting of the ISB.

2. The Executive Director will attach the ISB, as a subcommittee, to the Agency Executive Committee.

3. The Comptroller will initiate an ADP/Communications investment review. The review will also address requirements for sustaining investment in the future. This will be the focus of the May ISB offsite.

4. The Office of Information and Technology will ensure the completion of the baseline architecture document and will ensure that this baseline is captured in a CAD-like system for ease of updating.

5. The Architecture Working Group will define the Agency information systems architecture for 1993 and will brief this architecture at the next offsite. Each Directorate will actively participate in this definition to ensure that its requirements are captured. The architecture will define the network model and set of central services and network standards required to meet agency and directorate needs in the 1993 time frame. The architecture will specifically include Agency communications, both domestic and foreign. The question of how configuration control of this architecture should logically be partitioned to ensure that Agency, Directorate and Office interests are protected will be addressed.

6. The Office of Security will take action on the most urgent of the tasks described in the preliminary information systems security plan. The status of these efforts and a presentation of the final plan will be briefed to the ISB at the next offsite. The Office will take steps to ensure that the planning for the security of our systems remains in step with the Agency information system architecture.

7. With regard to the EPSG recommendations:

a. The Executive Director will package the recommendations of the EPSG for senior Agency management review.

b. The AWG will ensure that the information systems architecture supports the recommendations of the EPSG.

c. The Directorate of Administration will review and respond to the EPSG recommendations regarding the standardization of user interfaces across applications and the accessibility of these applications by all employees.

d. The EPSG will take a closer look at the Records Management concerns and present to the ISB at the next offsite a list of prioritized actions that the Agency must take to move us forward on this issue.

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
ACTION ITEMS, ISB OFFSITE

STAT
STAT

FROM: [redacted]
SA/EXDIR
7E12 HQS

EXTENSION [redacted]

NO. ER 4297-88

DATE 10 November 1988

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. ER				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				DCI EXEC REG
14.				
15.				B-209-IR

FORM 1-79 610 USE PREVIOUS EDITIONS

☆ U.S. Government Printing Office: 1985—494-834/49156

ER 4297-88
10 November 1988

MEMORANDUM FOR: Information Systems Board

STAT

FROM: [redacted]
Special Assistant to the Executive Director

SUBJECT: Action Items, ISB offsite - 3,4 Nov 1988

The following is the set of actions resulting from the recent ISB offsite. The formal meeting minutes with a complete set of the briefing charts will be distributed early next week. The next offsite referred to below is tentatively scheduled for the end of February.

Actions:

1. The Executive Director will draft an updated ISB charter for presentation at a future meeting of the ISB.

2. The Executive Director will attach the ISB, as a subcommittee, to the Agency Executive Committee.

3. The Comptroller will initiate an ADP/Communications investment review. The review will also address requirements for sustaining investment in the future. This will be the focus of the May ISB offsite.

4. The Office of Information and Technology will ensure the completion of the baseline architecture document and will ensure that this baseline is captured in a CAD-like system for ease of updating.

5. The Architecture Working Group will define the Agency information systems architecture for 1993 and will brief this architecture at the next offsite. Each Directorate will actively participate in this definition to ensure that its requirements are captured. The architecture will define the network model and set of central services and network standards required to meet agency and directorate needs in the 1993 time frame. The architecture will specifically include Agency communications, both domestic and foreign. The question of how configuration control of this architecture should logically be partitioned to ensure that Agency, Directorate and Office interests are protected will be addressed.

6. The Office of Security will take action on the most urgent of the tasks described in the preliminary information systems security plan. The status of these efforts and a presentation of the final plan will be briefed to the ISB at the next offsite. The Office will take steps to ensure that the planning for the security of our systems remains in step with the Agency information system architecture.

7. With regard to the EPSG recommendations:

a. The Executive Director will package the recommendations of the EPSG for senior Agency management review.

b. The AWG will ensure that the information systems architecture supports the recommendations of the EPSG.

c. The Directorate of Administration will review and respond to the EPSG recommendations regarding the standardization of user interfaces across applications and the accessibility of these applications by all employees.

d. The EPSG will take a closer look at the Records Management concerns and present to the ISB at the next offsite a list of prioritized actions that the Agency must take to move us forward on this issue.

STAT

[redacted]

STAT DCI/EXDIR,[redacted]10 Nov 88)

Distribution:

1 - EXDIR, 7D55 HQS
1 - ADDS&T, 6E56 HQS
1 - Comptroller, 7C21 HQS
1 - C/IMS, 1D4109 HQS
STAT 1 - D/OIT,[redacted]
1 - D/OC,
1 - D/OIR, 2E60
STAT 1 - D/OS,[redacted]
1 - DDA, 7D24 HQS
STAT 1 -[redacted]
1 -
1 -
1 -
1 -
1 -
1 - Executive Registry
1 - ISB File

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

ISB OFFSITE CONFERENCE

STAT
STAT

FROM: [redacted] SA/EXDIR 7E12 HQS	EXTENSION [redacted]	NO. ER 4109-88	DATE 25 October 1988

TO: (Officer designation, room number, and building)	DATE		OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
	RECEIVED	FORWARDED		
1. Executive Registry				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				DCI EXEC REG
15.				

FORM 610 USE PREVIOUS EDITIONS
1-79

☆ U.S. Government Printing Office: 1985—494-834/49156

Q-2-9-1C

ER 4109-88
25 October 1988

MEMORANDUM FOR: Information Systems Board

STAT FROM: [redacted]
Special Assistant to the Executive Director

SUBJECT: ISB Offsite - 3,4 Nov 1988

STAT The Information Systems Board will be meeting [redacted] 3,4 November. An agenda for the meeting is attached. The agenda has been abbreviated by the exclusion of the Strategic Plans presentations. The Executive Director has tentatively scheduled an offsite in February and the Directorate Strategic Plans will be included in that agenda.

STAT [redacted]

Attachment

STAT DCI/EXDIR/[redacted](25 Oct 88)

Distribution:
Orig - Addressee
1 - DCI Admin
1 - ER
1 - ISB File

Subject ISB Offsite - 3,4 November 1988 (cont'd)

Addressees:

EXDIR,7D55 HQS
ADDS&T,6E56 HQS
Comptr,7C21
C/IMS,1D4109 HQS
STAT D/OIT [redacted]
D/OC,
D/OIR,2E60
STAT D/OS [redacted]
DDA,7D24 HQS
STAT [redacted]

INFORMATION SYSTEMS BOARD

Thursday, 3 November 1988
[redacted]

STAT

Agenda

STAT [redacted]

1630 - 1730 Social Hour

1730 - 1830 Dinner

1830 - 1845 Opening Remarks. The Executive Director will review recent progress towards improved management of information technology within the Agency.

STAT 1845 - 1930 Information Security Strategy. [redacted], Chief of Information Security Group within the Office of Security, will present a strategic plan for dealing with the challenges of maintaining the security of Agency information systems.

1930 - 2000 Discussion

Friday, 4 November 1988

STAT 0800 - 0845 Communications Directions. [redacted] Deputy Director of the Office of Communications, will discuss challenges and directions for Agency world-wide communications.

0845 - 0945 Information Technology Directions. Mr. Edward Maloney, Director of the Office of Information and Technology, will discuss OIT's challenges and directions for managing the Agency's information system in today's rapidly changing information technology environment.

0945 - 1000 Break

STAT 1000 - 1200 Agency Information Systems Architecture. [redacted] Chief, Architecture and Plans Staff, Office of Information Technology will review with the Board the status of the activities of the Architecture Working Group. Emphasis for this first report will be on the information system baseline, capacity planning, and configuration management.

1200 - 1300 Lunch

STAT 1300 - 1345 Electronic Processes Study Group. [redacted] member of the Electronic Processes Study Group, will present the results of the group's four month study into the state of the Agency's electronic processes and will present recommendations which would allow the Agency to make more effective use of electronic processes in the conduct of daily business.

1345 - 1445 Executive Discussion and Closing Remarks

STAT [redacted]

STAT

Page Denied

Next 6 Page(s) In Document Denied