

CONFIDENTIAL

ROUTING AND RECORD SHEET



SUBJECT: (Optional)

OIT Missions and Functions Revision

FROM: Edward J. Maloney
Director of Information Technology

EXTENSION

NO.

OIT-1033-88

DATE

28 October 1988

TO: [redacted] 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. DDA
7D18 Hqs

13 NOV 1988

[Handwritten initials]

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

04M-6

CONFIDENTIAL

CONFIDENTIAL

OIT-1033-88
28 October 1988

MEMORANDUM FOR: Deputy Director for Administration
FROM: Edward J. Maloney
Director of Information Technology
SUBJECT: OIT Missions and Functions Revision
REFERENCE: Your Memorandum, dtd 20 September 1988, Same Subject,
DDA 88-1962

Rae,

1. This is in response to your request for a revised missions and functions statement for each of our OIT components reflecting our recent organizational adjustments.

2. At Tab A I have provided a copy of our revised missions and functions statement. In addition, through discussions with my group chiefs, I have prepared in graphic format the overall organization of OIT (see Tab B), as well as the group organization by branch and by functional responsibility (see Tab C). I have directed my group chiefs to continue this dialogue with their division chiefs, branch chiefs, and line officers. It is my intent that all employees in OIT will understand how they relate to the organization and their functional responsibilities.

3. Moreover, in an on-going series of discussions with my managers (e.g. our forthcoming OIT Division Chiefs' offsite), I am communicating my view of our office objectives, both short and long term. We are now translating these goals into specific taskings for each of our organizational elements.

4. To date, I am pleased with our progress as evidenced by the improvements in the availability of the General Services and the Special Centers. We still have many challenges ahead of us but, with your assistance and the cooperation of the other offices, we will be prepared to meet them.

[Redacted Signature Box]

Edward J. Maloney

25X1

25X1

This Document becomes UNCLASSIFIED
when separated from attachment.

CONFIDENTIAL

[Redacted Box]

Page Denied

CONFIDENTIAL

SUBJECT: OIT Missions and Functions Revision

25X1 OIT/MSD [redacted] (28 Oct. 88)

Distribution:

{Orig + 1 - DDA }

- 2 - OIT/FO
- 3 - ISC/OIT
- 1 - MSD Chrono
- 1 - MSD Subject

CONFIDENTIAL

CONFIDENTIAL

OFFICE OF THE DIRECTOR (O/DIR)

MISSION

The Director of Information Technology (D/OIT) is responsible for setting OIT policy and managing all OIT functions. Those functions include operating the Agency's 24-hour data and communications services; maintaining data and communications equipment and software; managing the domestic communications network; directing the Agency Freedom of Information Act, Executive Order 12356, and Historical Review programs; directing the Agency Information Management Program; providing oversight of classification and declassification functions; and managing the MZ career sub-groups. The D/OIT and his staff also conduct liaison with such organizations as the Information Security Oversight Office, the National Archives and Records Administration, the Office of the Federal Register, and the General Services Administration's Office of Information Resources Management.

In addition to the Director and Deputy Director, OIT, other key staff components in the Office of the Director include: the Requirements and Plans Staff, the Architecture and Technology Planning Staff, and a Special Assistant for Development and Engineering. Management of OIT is coordinated through the Office's five groups: Network Services Group, Management Services Group, Computer Operations Group, Engineering Services Group, and Development Services Group.

CONFIDENTIAL

CONFIDENTIAL

REQUIREMENTS & PLANS STAFF (R&PS)

R&PS manages and tasks all OIT customer requirements other than the routine operational maintenance of OIT-supported equipment. C/R&PS also manages the OIT system integration effort.

ARCHITECTURE AND TECHNOLOGY PLANNING STAFF (A&TPS)

A&TPS develops OIT's long-range technical plan in support of information systems, office automation, and communications. The staff also formulates the information architecture to support the requirements of OIT's customers, including interoperability between customer equipment and OIT computer and communications systems. C/A&TPS serves as the executive secretary for the Customer/Standards Committee and the Information Technology Management Board.

SPECIAL ASSISTANT FOR DEVELOPMENT AND ENGINEERING (SA/D&E)

The SA/D&E conducts special studies, analyses, and research for the Director of Information Technology and provides technical consultation to the Director and his staff.

CONFIDENTIAL

NETWORK SERVICES GROUP (NSG)

MISSION

Network Services Group (NSG) develops and executes the OIT client service strategy. In fulfilling this responsibility, NSG provides customer voice and data connectivity, ensures the reliability and availability of equipment on customer premises, assists clients in the effective use of OIT systems and problem resolution, and provides standards for the control of Agency information.

CONFIDENTIAL

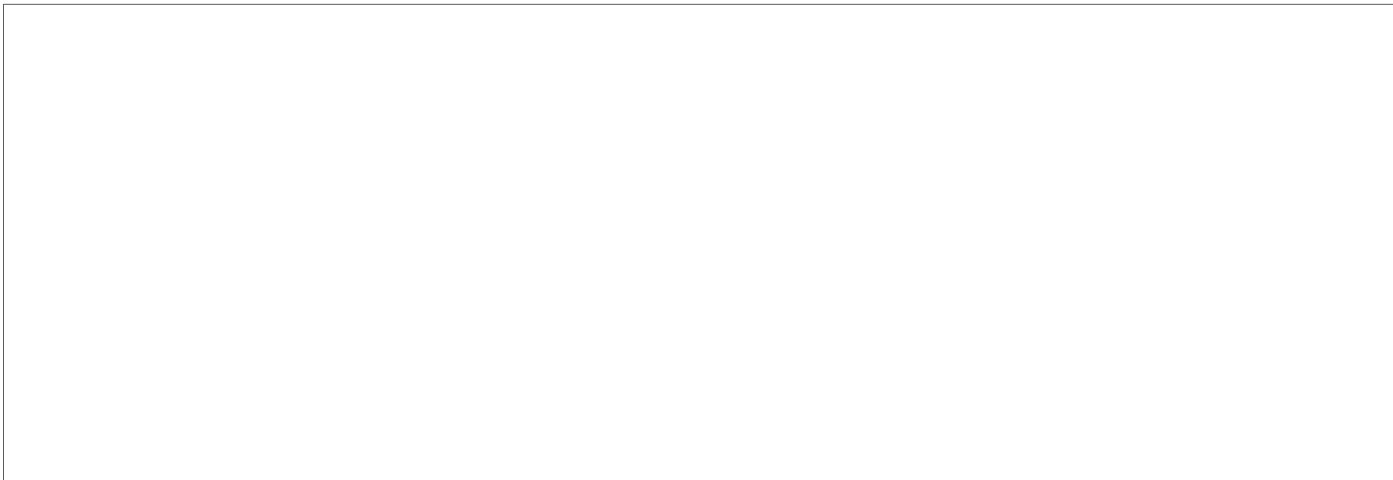
UNITED STATES NETWORKS DIVISION (OIT/NSG/USND)

USND provides secure communications (crypto, secure voice, data and video, facsimile, and terminal equipment) for the Agency. The division is responsible for all systems that provide carrier support to the headquarters area from Agency facilities within the continental United States.

COMMUNICATIONS ENGINEERING DIVISION (OIT/NSG/CED)

CED provides telecommunications services at Reston and effects the major realignment and upgrade of all telecommunications services for the New and Original Headquarters Buildings. The division also provides for the strategic planning and systems engineering for Metropolitan Area Communications (MAC) and engineering support to operational elements in all matters pertaining to communications.

25X1



COORDINATOR DIGITAL NETWORK SERVICES (OIT/NSG/C/DNS)

C/DNS coordinates all functions associated with the non-secure and secure voice networks, as well as the integrated data/voice network. This includes the operation and maintenance of PBX and IBX equipment, their attached stations, and integrated terminals; moves, adds, and changes (MACs) as they relate to the integrated voice/data and voice only networks; trunk and traffic management; and the billing process.

MAINTENANCE MANAGEMENT DIVISION (OIT/NSG/MMD)

MMD manages the maintenance of all customer premise data processing and communications equipment to ensure quality service.

CUSTOMER ASSISTANCE DIVISION (OIT/NSG/CAD)

CAD provides consulting assistance in the use of computer mainframes, personal computer hardware and software, workstations, and telephone equipment. The division manages the VM and AIM systems, assigns passwords, provides commercial software through the PC Software Store, and provides customer information through seminars and briefings.

DATA AND VOICE SERVICES DIVISION (OIT/NSG/DVSD)

DVSD effects the distribution of computer-generated output in remote sites such as OIT registries and data access centers. It also provides telephone support (such as telephone information and assistance with long distance calls) for the Agency.

INFORMATION MANAGEMENT DIVISION (OIT/NSG/IMD)

IMD administers the Agency Information Management Program, the Top Secret and Collateral Control Program, and the Information Security Program. IMD also prepares the Agency National Security Classification Guide and manages the Agency's component registries, information services centers, and the Archives and Records Center at Warrenton.

INSTALLATIONS DIVISION (OIT/NSG/ID)

ID installs and relocates all ADP and communications equipment such as personal computers, word processors, local printers, secure and non-secure telephones, and associated peripheral equipment located at customer sites.

~~SERVICE DESK (OIT/NSG/SD)~~

~~The OIT Service Desk provides a single point of contact for information, general assistance, and problem reporting concerning OIT operational services. It acts as the customer interface for trouble calls concerning computer equipment, secure and non-secure telephones, and the telecommunications network.~~

CONFIDENTIAL

MANAGEMENT SERVICES GROUP (MSG)

MISSION

Management Services Group (MSG) supports the Director of Information Technology in such areas as policy formulation; planning, programming, and budgeting; business communications; ADP contracting; human resource development; FOIA/Privacy Act/Executive Order 12356 requests; classification/declassification review; historical review; administrative support services; and computer, communications, and information security.

CONFIDENTIAL

MANAGEMENT SERVICES DIVISION (OIT/MSG/MSD)

MSD provides OIT financial management and coordinates a wide range of Agency and OIT policies, procedures, and regulations. MSD plans OIT's business communications and designs and prepares office publications and visual aids. The division also provides ad hoc management support to the D/OIT, develops coordinated OIT positions, and prepares OIT briefings and presentations. In addition, MSD reviews ADP procurements Agency-wide as required by Headquarters Regulation 7-15, develops and distributes computer-related documentation to Agency customers, and operates a library of specialized computer manuals, textbooks, and other instructional materials.

INFORMATION SERVICES DIVISION (OIT/MSG/ISD)

ISD manages the Agency's response to requests from the public for information under the Freedom of Information and Privacy Acts and Executive Order 12356. The division handles declassification review of documents, prepublication review of manuscripts submitted by current and former employees, and review of employment summaries prepared by Agency employees. ISD also manages for the Director of Central Intelligence the CIA Historical Review Program.

SUPPORT STAFF (OIT/MSG/SS)

Support Staff provides OIT administrative and management support. In fulfilling its responsibilities, the staff provides personnel, logistics, ADP document control, personal and physical security, and travel support.

TECHNICAL SECURITY DIVISION (OIT/MSG/TSD)

TSD coordinates and supports the OIT information and technical security programs. The division also provides information security risk management and assessment services for the Director of Information Technology, OIT managers, and operating components. TSD implements overall Agency computer security policy, prepares procedures and guidelines, and develops computer security techniques. TSD also audits OIT information systems for abuse and unauthorized access and assists the Office of Security in investigations involving information systems. Moreover, the division is responsible for interpreting and applying policies and standards, managing cryptographic clearances, conducting COMSEC audits and surveys, providing COMSEC/TEMPEST guidance and accreditation, investigating and reporting COMSEC compromises and violations, and preparing risk and damage assessment reports.

CONFIDENTIAL

HUMAN RESOURCE PROGRAM (OIT/MSG/HRP)

HRP ensures that OIT has a highly motivated and professional workforce. In fulfilling this responsibility, HRP recruits, selects, and places applicants for OIT employment and manages employee training, development, and rotations. HRP provides career development and grievance counseling. In coordination with the Office of Training and Education, HRP also develops and provides courses and seminars for OIT personnel.

CONTRACTS DIVISION (OIT/MSG/CD)

CD procures information technology equipment, software, and services for OIT and its customers. The division operates under authority delegated from the Director of Logistics and follows applicable federal and Agency regulations in performing its procurement functions.

CONFIDENTIAL

COMPUTER OPERATIONS GROUP (COG)

MISSION

The Computer Operations Group (COG) effects the management, facilities engineering, operation, maintenance, and production of the 24-hour, 7-day-a-week data and communications centers. This includes hardware and software maintenance for OIT communications operating systems and message processing systems. Additionally, COG provides a Senior Operations Duty Officer (ODO) in support of the OIT mission.

CONFIDENTIAL

OPERATIONS DUTY OFFICER (OIT/COG/ODO)

The ODO serves as the Senior OIT representative performing liaison between the customer and all OIT service managers with primary emphasis after normal duty hours. The ODO also maintains contact with other Agency Duty Officers and coordinates with appropriate OIT service elements as needed to resolve customer problems. The ODO monitors the worldwide communications network and keeps managers and supervisors informed of situations that may impact on CIA communications and data center operations.

OPERATIONS INTEGRATION AND PLANNING STAFF (OIT/COG/OIPS)

OIPS performs COG's COTR functions and serves as the focal point for establishing priorities and for planning and coordinating COG office moves to the New Headquarters Building. It oversees changes impacting upon data/communications systems and monitors requested changes. OIPS also reviews overall performance results and operational problems to ensure that service standards are met. Maintaining the COG special project tracking system also is a responsibility of OIPS. It is responsible for identifying critical service needs in the event of a disaster or extended outage, and for identifying the alternative temporary or interim processing capability required. OIPS is responsible for processing all procurement actions and contract renewals for COG and NSG.

OPERATIONS DIVISION (OIT/COG/OD)

OD operates the Agency's data processing and communications systems and certifies the readiness and acceptance of these systems. This includes the Second Phase Automated Relay System (SPARS) and the Data Transmission Exchange (DATEX) (both to be replaced by the Message Relay Switch (MRS)), the Domestic Message Switch (DMS), the Cable Dissemination System (CDS), the Message Handling Facility (MHF), and the Automated Printing and Reproduction System (APARS). OD also operates the Crisis Communications Center (CCC), with control over the Agency UHF SATCOM Crisis Communications network, and acts as the hub terminal for VIP and critical communications. OD conducts the ADP operations in the Agency's two computer centers, the CAMSW2 Development Center, and the Data Base Control Center. In addition, OD provides operational guidance and direction for the NPIC Communications Center and 15 communications facilities that support narrative traffic requirements for a variety of Agency and other Intelligence Community members in the Washington Metropolitan Area.

CONFIDENTIAL

~~PRODUCTION DIVISION (OIT/COG/PD)~~

~~PD implements new applications, data base management, and message handling systems. PD also provides the resources for entering and verifying data from coded source documents into readable machine language. PD also implements customer requirements for message dissemination, corrects errors in the dissemination of message traffic, and maintains responsibility for OIT-supported data base management systems to ensure data integrity and security.~~

TECHNICAL SERVICES DIVISION (OIT/COG/TSD)

TSD coordinates all activities concerning the installation of OIT computer systems, including the relocation of systems and services to the New Headquarters Building. TSD also functions as the COTR for all contractors supporting the relocation of data facilities. TSD plans all computer system configuration changes, designs automated switch networks for data systems, and manages the hardware modifications to the telecommunications systems. In addition to analyzing all mainframe hardware failures and ensuring proper corrective action, the division coordinates vendor engineering changes to ensure that modifications are necessary, pretested, scheduled, and installed. Ensuring the development of new software systems and releases to meet operational requirements also is a TSD responsibility.

CONFIDENTIAL

ENGINEERING SERVICES GROUP (ESG)

MISSION

The Engineering Services Group provides the data communications networks, computer systems software, message handling systems, office systems, data base systems, and engineering and analysis services in support of the OIT and Agency missions.

CONFIDENTIAL

CONFIDENTIAL

OPERATING SYSTEMS DIVISION (OIT/ESG/OSD)

OSD provides installation and support of operating systems, program products, and other related system software. The division keeps abreast of hardware and software technology, provides systems consulting, and participates with vendors in early support programs and joint studies to provide needed system services.

DATA BASE SYSTEMS DIVISION (OIT/ESG/DBSD)

DBSD provides installation and support of data base systems, applications enabling products, and other related system software. DBSD also ensures the integration of these systems and products into the OIT architecture.

OFFICE PRODUCTS DIVISION (OIT/ESG/OPD)

OPD develops and maintains the Agency's unique host-based office automation software (Automated Information Management--AIM) and workstation system software. OPD also provides planning and systems engineering for future office automation systems, workstations, workstation/host communications, and related software.

DATA COMMUNICATIONS DIVISION (OIT/ESG/DCD)

DCD provides development and engineering support for domestic communications facilities, including local area networks, specialized message handling systems, integrated electronic mail systems, and specialized printing and graphics devices. DCD also develops and maintains communications software to support the OIT host/workstation network.

SYSTEMS PLANNING AND EVALUATION DIVISION (OIT/ESG/SPED)

SPED measures and reports on resource utilization for computer processing and domestic communications systems and networks, and develops long range capacity plans for these systems. The division evaluates new requirements for impact on domestic communications and computer processing capacity and performance, and analyzes the impact of new technologies on system capacity and performance.

CONFIDENTIAL

CONSOLIDATED SAFE PROGRAM OFFICE (OIT/ESG/CSPO)

CSPO coordinates the development, deployment, and operation of the Support for the Analysts' File Environment (SAFE) project within OIT and provides liaison on SAFE matters with the Office of Information Resources and the Defense Intelligence Agency.

DEVELOPMENT SERVICES GROUP (DSG)

MISSION

The Development Services Group (DSG) designs, develops, and enhances information systems and other special-purpose computer systems for a wide variety of customer applications. DSG provides similar services for Intelligence Community (IC) information systems, including the COMIREX Automated Management System (CAMS), the Decision Support and Information System for Terrorism (DESIST), and the Community-wide Computer-assisted Compartmentation Control (4C) System. DSG also acts as a consultant to other development activities in the Agency and performs feasibility studies and requirements analyses.

CONFIDENTIAL

CONFIDENTIAL

ARTIFICIAL INTELLIGENCE STAFF (OIT/DSG/AIS)

AIS develops applications that require technology based on artificial intelligence and expert systems. AIS also consults with other OIT and Agency managers on the use of AI technology.

SYSTEMS ENGINEERING STAFF (OIT/DSG/SES)

SES provides systems engineering support to group projects, acts as the point of contact for technical standards and policy matters, and assists in obtaining services and support from other OIT components.

CONFIGURATION MANAGEMENT CENTER (OIT/DSG/CMC)

CMC provides for the control, management, and security of all baselined software and documentation produced in support of applications developed and maintained by the Development Services Group. CMC also administers automated management and security systems used to store and control such software and documentation, and provides guidance and training on the use of these systems to DSG programmers.

CONTRACTS ADMINISTRATION STAFF (OIT/DSG/CAS)

CAS assists software development personnel in ADP contract activities, and acts as the COTR for a large multivendor contract for development services. CAS provides support for this contract to group personnel and several other Agency components.

CAREER MANAGEMENT STAFF (OIT/DSG/CMS)

CMS coordinates the career management plans and activities for Development Services Group personnel, including those on rotational assignment to various Agency components.

CONFIDENTIAL

CORPORATE SYSTEMS DEVELOPMENT DIVISION (OIT/DSG/CSDD)

CSDD provides the design, development, and implementation of corporate data systems. In addition, CSDD provides data and data base administration to corporate systems developers and investigates and implements new technologies for the development and support of corporate data systems.

DEVELOPMENT SERVICES DIVISION (OIT/DSG/DSD)

DSD develops and supports applications for a variety of Agency customers, such as an insurance claims processing system for the Office of Personnel and an AIM-based course registration system for the Office of Training and Education. Additionally, it supports PC-based information retrieval systems for overseas deployment by the Office of Technical Service, a PC-based message encryption system. DSD maintains a Local Area Network (LAN)-based information retrieval application for the Directorate of Operations and several systems that support the Counter Terrorist Center.

CAMS PROGRAM OFFICE (OIT/DSG/CAMS)

The CAMS Program Office provides definition, design, development, enhancement, and maintenance of the Processing Segment (P/S) of the Intelligence Community's COMIREX Automated Management System (CAMS). Additional functions in support of CAMS include feasibility studies and consulting services to CAMS P/S users.

CONFIDENTIAL



B

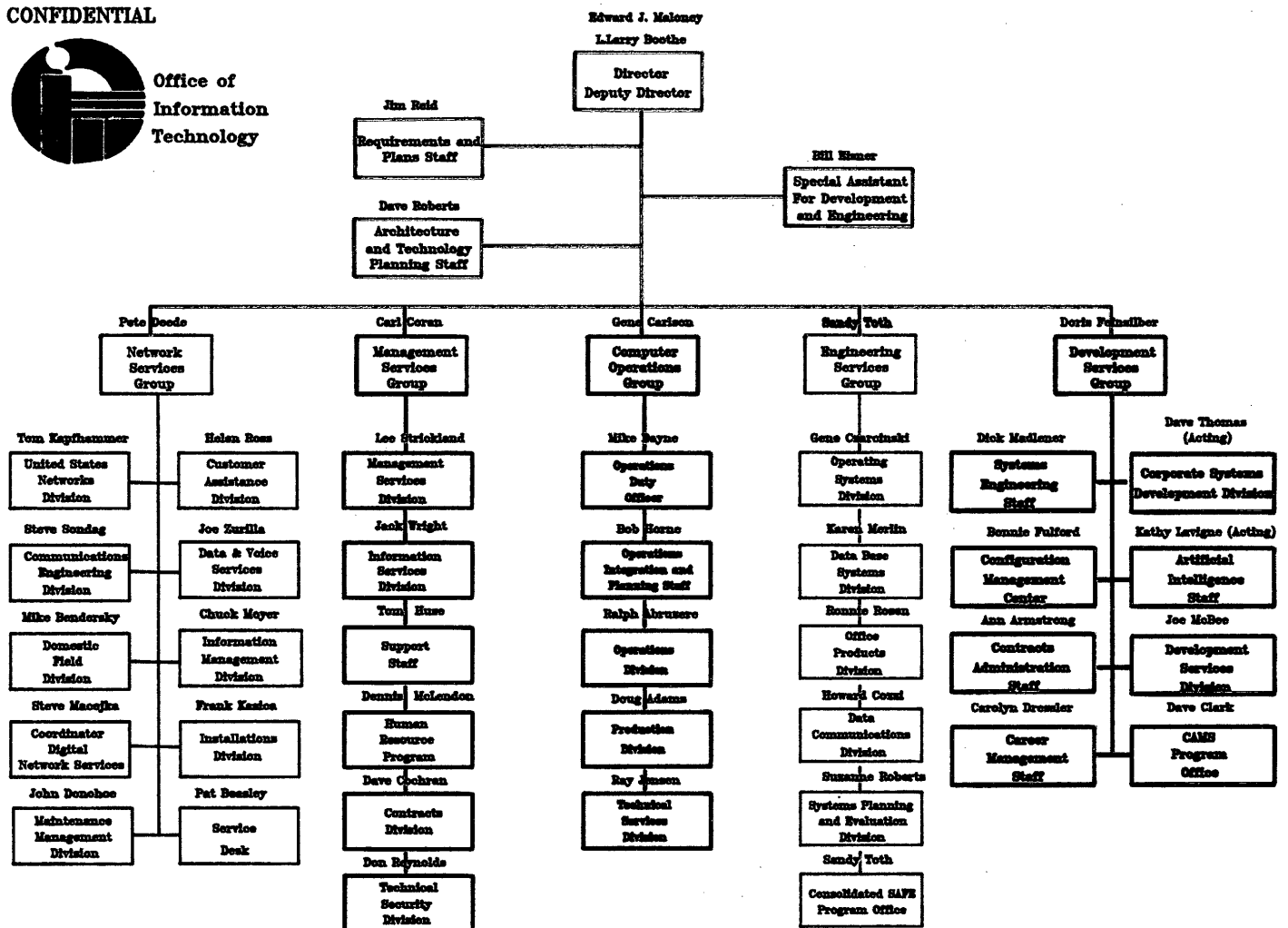


Office of Information Technology

CONFIDENTIAL



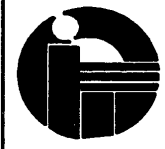
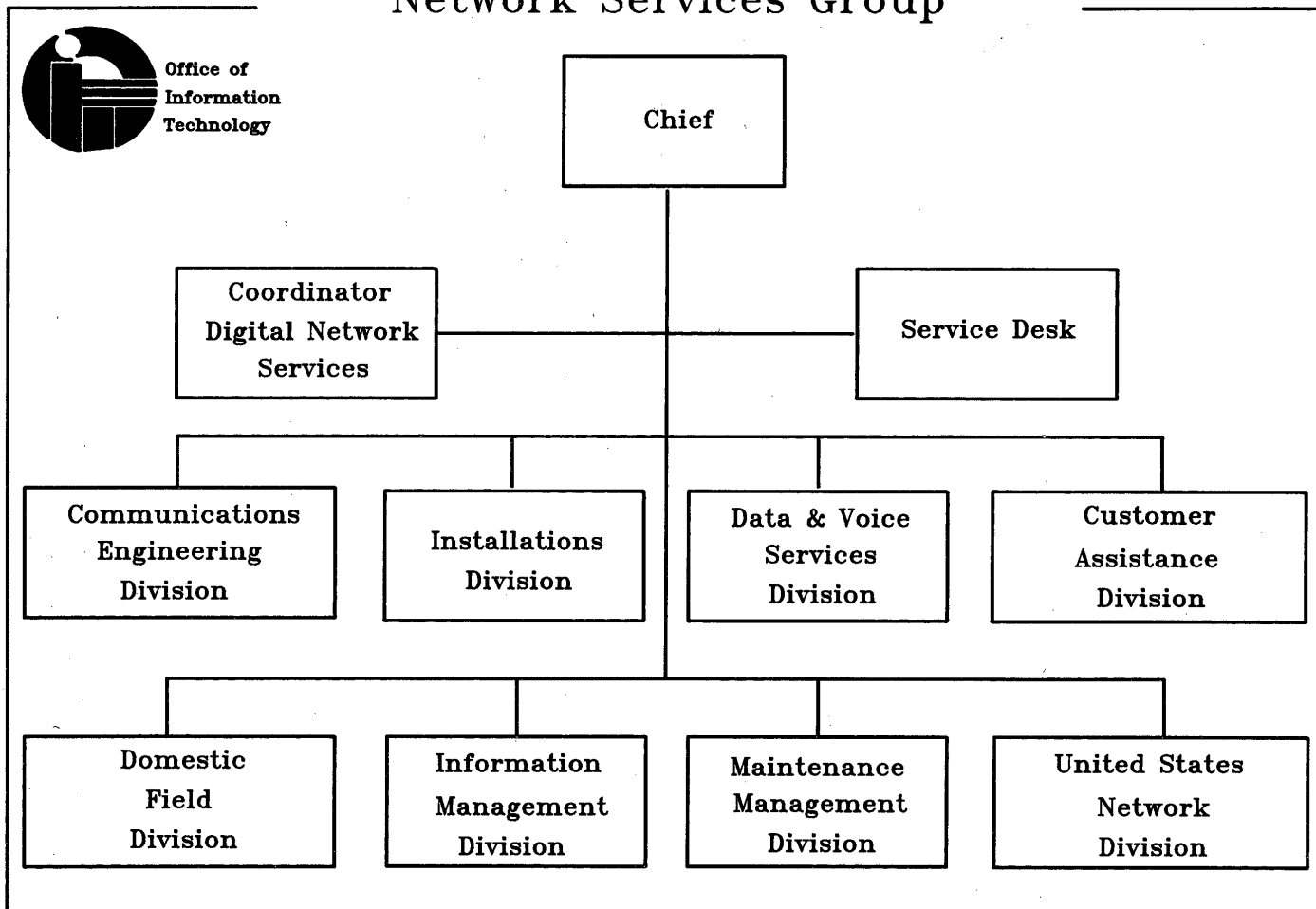
Office of Information Technology



c

ADMINISTRATIVE-INTERNAL USE ONLY

Network Services Group

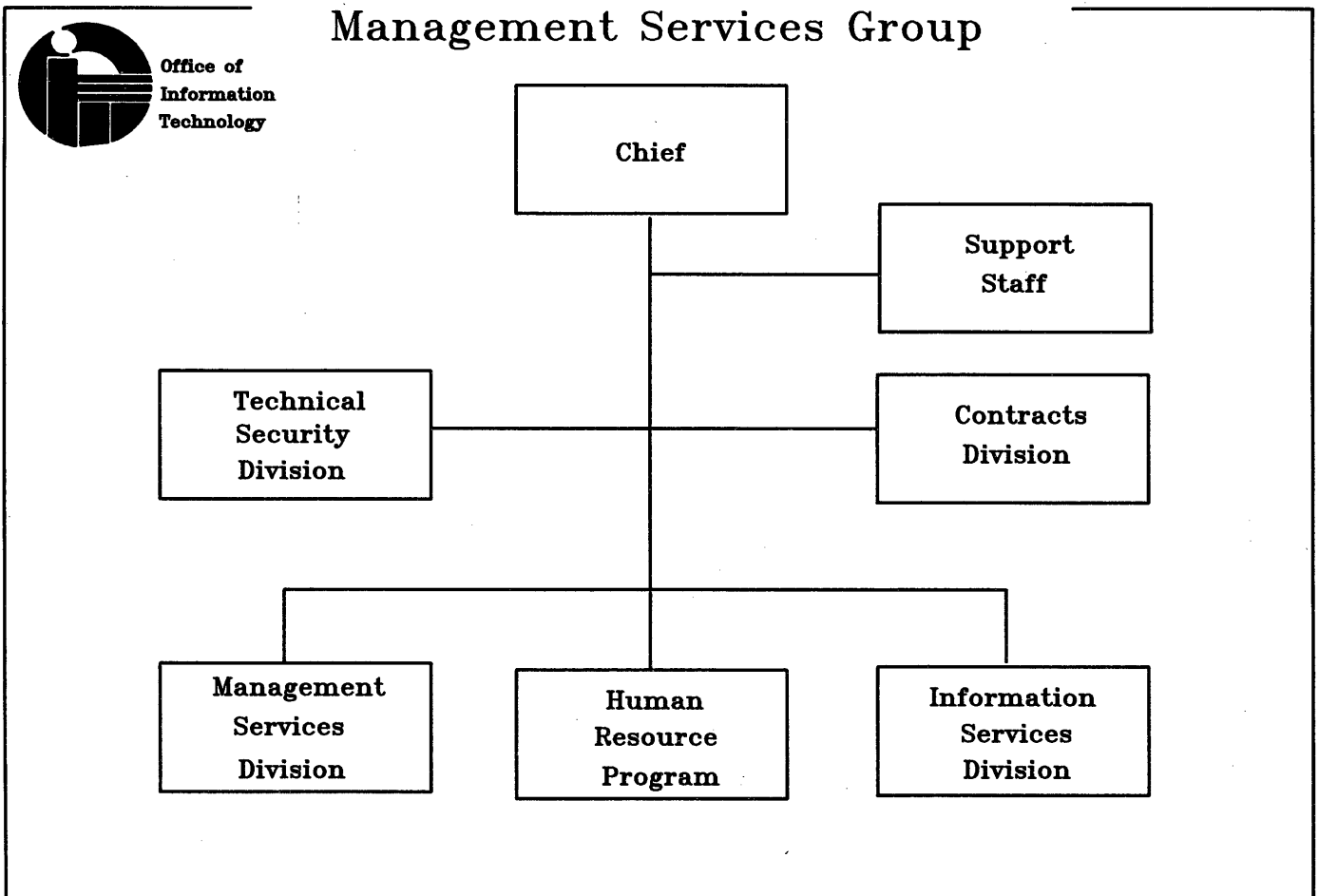


Office of
Information
Technology

Page Denied

Next 1 Page(s) In Document Denied

ADMINISTRATIVE-INTERNAL USE ONLY



Page Denied

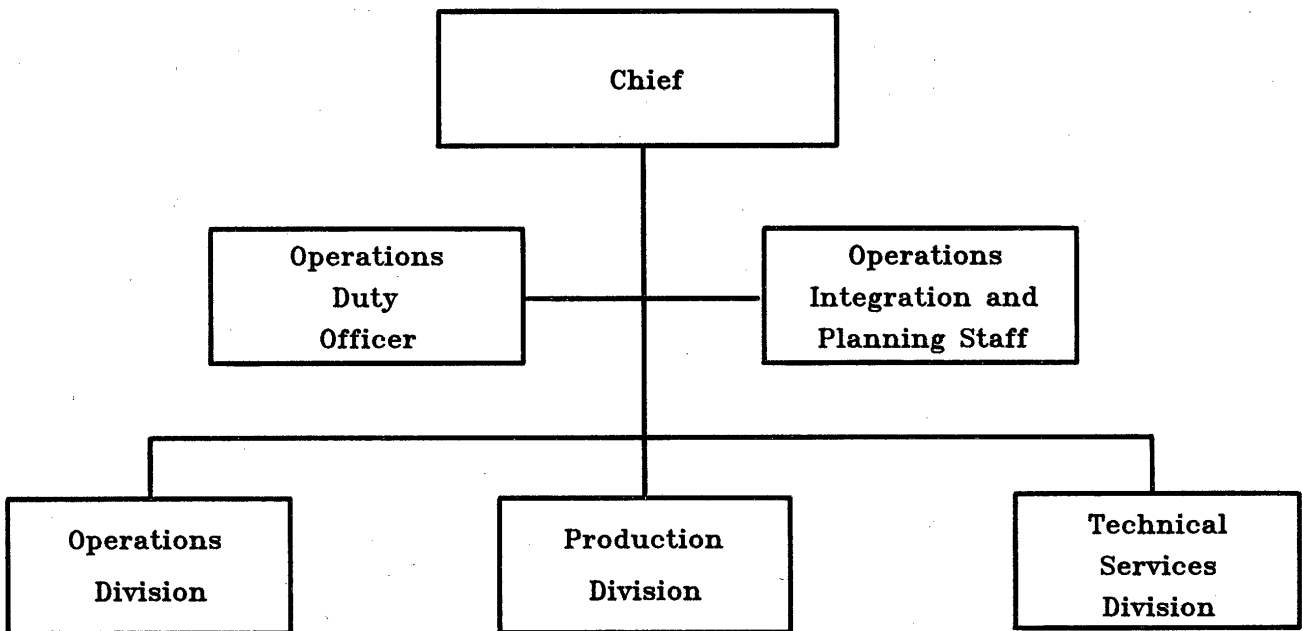
Next 1 Page(s) In Document Denied

ADMINISTRATIVE-INTERNAL USE ONLY



Office of
Information
Technology

Computer Operations Group



ADMINISTRATIVE-INTERNAL USE ONLY

Page Denied

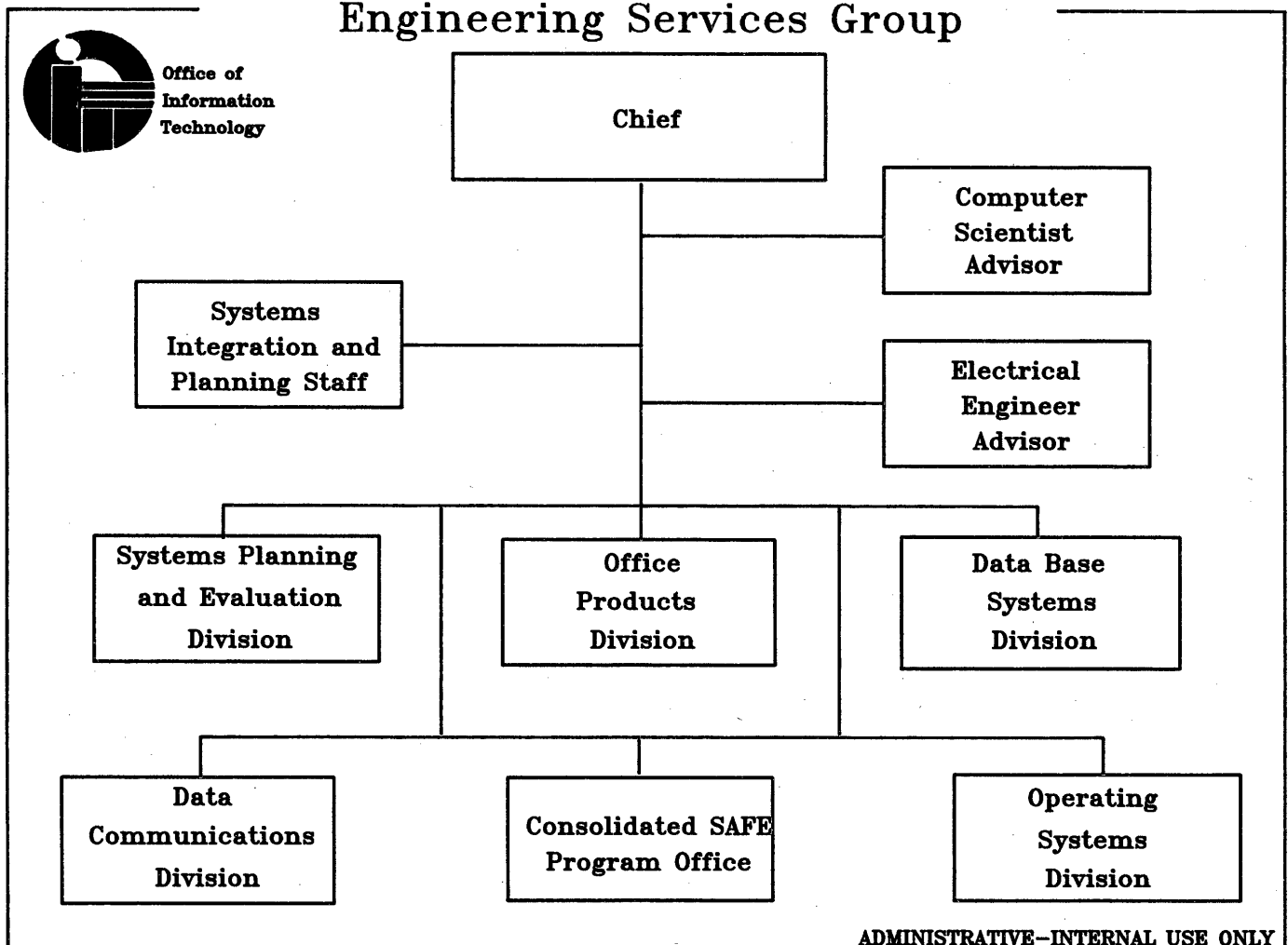
Next 1 Page(s) In Document Denied

ADMINISTRATIVE-INTERNAL USE ONLY

Engineering Services Group



Office of
Information
Technology



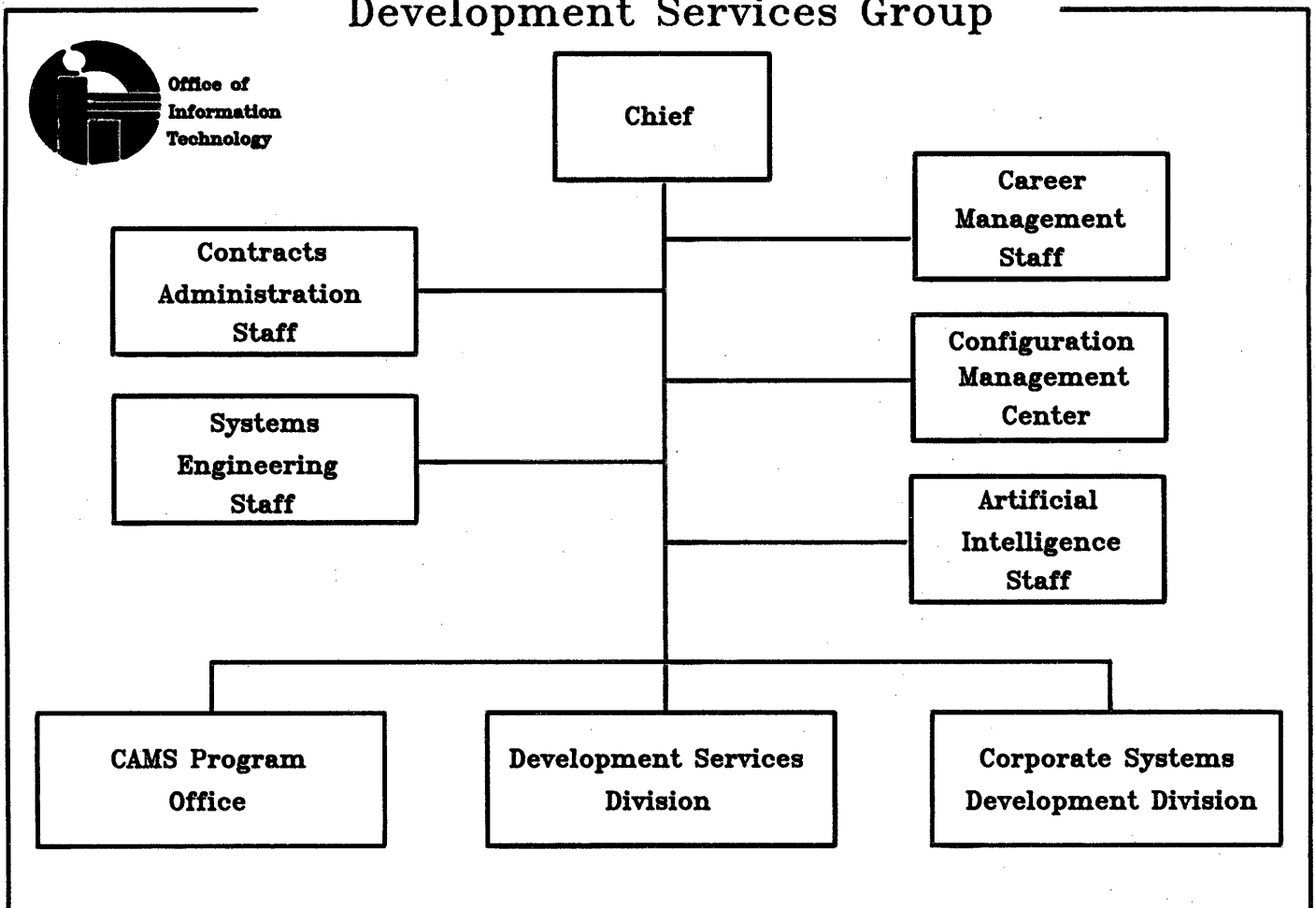
ADMINISTRATIVE-INTERNAL USE ONLY

Page Denied

Next 1 Page(s) In Document Denied

ADMINISTRATIVE-INTERNAL USE ONLY

Development Services Group



Page Denied

Next 1 Page(s) In Document Denied



ADMINISTRATIVE - INTERNAL USE ONLY

DDA 88-1962
20 September 1988

MEMORANDUM FOR: Director of Information Technology
FROM: R. M. Huffstutler
Deputy Director for Administration
SUBJECT: Missions and Functions Revision

Please prepare a new missions and functions statement for each of the components in OIT commensurate with their new duties following the organizational adjustments. These statements should clearly identify who is responsible for what and should be well understood by all members of OIT.

I would like this by 31 October 1988.



R. M. Huffstutler

STAT

ADMINISTRATIVE - INTERNAL USE ONLY



DDA 88-1962
20 September 1988

MEMORANDUM FOR: Director of Information Technology
FROM: R. M. Huffstutler
Deputy Director for Administration
SUBJECT: Missions and Functions Revision

Please prepare a new missions and functions statement for each of the components in OIT commensurate with their new duties following the organizational adjustments. These statements should clearly identify who is responsible for what and should be well understood by all members of OIT.

I would like this by 31 October 1988.



R. M. Huffstutler

ORIG:DDA:RMHuffstutler:jal
DISTRIBUTION:

Original - Addressee

- 1 - DDA Subject
- 1 - DDA Chrono
- 1 - RMH Chrono

Handwritten signature/initials: D + M - 4

ADMINISTRATIVE - INTERNAL USE ONLY