1 FAM 270
BUREAU OF INFORMATION RESOURCE MANAGEMENT (IRM)

(CT:ORG-209; 03-24-2009)
(Office of Origin: IRM/BPC/EAP)

1 FAM 271 CHIEF INFORMATION OFFICER (CIO)

1 FAM 271.1 Policy

(CT:ORG-198; 10-15-2008)

The Chief Information Officer:

(1) Establishes effective information resource management planning and policies;

(2) Ensures availability of information technology systems and operations, including information technology (IT) contingency planning, to capably support the Department's diplomatic, consular, and management operations;

(3) Exercises management responsibility for ensuring that the Department's information resources meet the business requirements of the Department's business practitioners and provide an effective basis for knowledge sharing and collaboration within the Department and with other foreign affairs agencies and partners; and

(4) Exercises delegated approving authority (DAA) for development and administration of the Department's computer and information security programs and policies. The Bureau of Diplomatic Security (DS) is the DAA for State systems that fall under the requirements of the DCI Directive for Protecting Sensitive Compartmented Information (SCI) Within Information Systems (DCI Directive dated 6/3).

1 FAM 271.2 Responsibilities

(CT:ORG-198; 10-15-2008)

a. The Chief Information Officer (CIO) holds a rank equivalent to that of an *A*ssistant *S*ecretary.

b. The CIO fulfills the responsibilities of the Chief Information Officer pursuant to section 5125 of the Clinger-Cohen Act (40 U.S.C. 1425), Chapter 35 of 44 U.S.C., the e-Government Act of 2002 (Public Law 107-347), and other applicable law, regulations, and directives.

c. The CIO serves as the principal adviser to the Secretary of State, the Under Secretary for Management (M), and other senior officials on matters pertaining to developing, implementing, and as necessary, revising policies, plans, and programs to facilitate and strengthen the cost-effective, efficient, and timely application of information systems, knowledge management, and technology resources to comply with applicable requirements and achieve strategic Department missions.

d. The CIO, in performing his or her responsibilities, exercises functional authority on behalf of the Under Secretary for Management (M). Pursuant to 44 U.S.C. 3506(a)(2)(A), in carrying out his or her statutory responsibilities, the CIO reports directly to the Secretary of State.

e. With respect to the subject matter described in subparagraph e(6) of this section, and taking into account applicable statutes, executive branch instructions, and Department policies, the CIO:

(1) Manages and coordinates the Department’s information resources and technology infrastructure and provides core information, knowledge management, and technology (IT) services;

(2) Co-chairs the Department’s e-Government Program Board with the Chief Financial Officer and coordinates on IT capital planning matters regarding enterprise-wide information resource management and establishes IT program priorities;

(3) Ensures that user requirements and business practices, as well as knowledge management objectives, are reflected in information resource management decisions;

(4) Represents the Department in the Federal CIO Council and other organizations;

(5) Assures that Department information resource policies and

programs fulfill Federal Enterprise Architecture and e-Government objectives;

(6) Establishes policies, plans, and programs and oversees specific operations to ensure that the Department's information resource management, information systems, and information technology is designed, acquired, operated, maintained, monitored, and evaluated so as to comply with all applicable requirements and support the efficient, cost-effective, and timely achievement of strategic Department missions to include, but not be limited to:

(a) Security, in coordination with DS;

(b) Configuration management, in coordination with DS;

(c) Workforce planning;

(d) Knowledge management;

(e) Modernization of the Department's information systems;

(f) Development, implementation, and maintenance of a sound and integrated information technology architecture for the Department;

(g) Establishment and promulgation of technical and operating standards for application to Department information systems; and

(h) Analysis, prior to significant information technology investments, of the Department's mission-related and administrative processes, with due consideration to restructuring and outsourcing, as appropriate;

(7) Is the designated approving authority (DAA) for development and administration of the Department's computer and information security programs and policies. The Bureau of Diplomatic Security (DS) is the DAA for State systems that fall under the requirements of the DCI Directive for Protecting Sensitive Compartmented Information (SCI) Within Information Systems (DCI Directive dated 6/3);

(8) Provides advice, guidance, and direction to Department elements responsible for preparing information resource management plans required by statutes, executive branch instructions, and Department policies;

(9) Recommends funding priorities with respect to the acquisition, operation, maintenance, and improvement of Department information resource, programs, and projects, including the discontinuance or termination of such programs and projects;

(10) Initiates the development, implementation, and evaluation of training plans, in coordination with affected bureaus, to ensure that Department personnel acquire skills needed to manage and use existing and planned information resources;

(11) Establishes, or otherwise ensures, that a process is in place to evaluate fairly whether proposed collections of information should be approved, and to certify such proposed collections of information to OMB for review and approval;

(12) Maintains liaison, in coordination with affected Department elements, with members and staffs of Congressional committees having oversight responsibilities for the Department's information resources and information resources management;

(13) Exercises substantive responsibility for following the Department's regulatory publications: Foreign Affairs Manual Volume 5, Information Management, and its related Foreign Affairs Handbooks in their entirety; and

(14) Performs such other functions as may be delegated by the Secretary of State or Under Secretary for Management (M).

1 FAM 271.3 Organization

(CT:ORG-171; 08-24-2007)

See 1 FAM 271 Exhibit 271.3 for an organization chart of the Bureau of Information Resource Management(IRM).

1 FAM 271.4 Definitions

(TL:ORG-130; 04-30-2004)

Access Control Facility, Version 2 (ACF2): A National Security Agency (NSA)-approved, C-2 rated software product. It provides security for data stored on computer systems using the IBM Multiple Virtual System/Enhanced Services Architecture (MVS/ESA) operating system.

Alternate communications site: Established by the Department of State's Critical Infrastructure Committee, this site serves as the alternate

communications and command and control center in the event of a major interruption of service, due to such things as a terrorist attack, fire, natural disaster, or catastrophic failure of the Department's primary facilities in Washington, DC and Beltsville, Maryland. These services include networking for all ClassNet, OpenNet, and Telegraphic Communications.

Call accounting: The process by which call detail records for specific or groups of telephone extensions are collected and recorded for billing and traffic-monitoring purposes.

Capital planning: An integrated management process that provides for the continuous identification, selection, control, life-cycle management, and evaluation of an information technology investment program designed to achieve a desired business outcome.

Central office of record (COR): The office of a Federal department or agency that keeps records of accountable communications security (COMSEC) material held by elements subject to its oversight.

Combined bureau processing centers: The combined bureau processing centers (CBPCs) are classified network centers that provide a centralized infrastructure to support bureau foreign affairs information systems (FAIS) requirements. These systems provide electronic telegram capabilities and classified electronic e-mail capabilities for the bureaus. The AF, PM, EAP, EB, NEA, and EUR bureaus have information-processing equipment located in the CBPC.

Communications security (COMSEC) account: An administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

Computer technologies: The technology employed in developing and using computers, computer peripherals, operating systems, software, and communications systems.

Configuration management (CM): The process of identifying and defining the configuration items in a system; controlling the release and change of these items throughout the system life cycle; recording and reporting the status of configuration items and change requests; and verifying the completeness and correctness of configuration items.

Data administration: The organization responsible for the definition, management, organization, and supervision of data within an enterprise or organization. A business function responsible for identifying, documenting, and modeling business information requirements, and for maintaining the business's set of data definitions and standards.

Database administration (DBA): Technical support and configuration management of a data base management system. Functions include system maintenance, user access control, review of new data base designs, data base change control, data base replication, and security issues and procedures.

Data replication: The process of, or facilities for, maintaining multiple copies, subsets, or versions of data (copy management). This process is normally managed by the data base administrator and can be primary-site (single location) or multi-site (multiple locations) in nature.

Department of State publications (DOSPUB): A list of routing indicators and security levels for every post.

Desktop browser: A suite of programs located in a desktop PC that allows both viewing and navigation from one node on the Internet or OpenNet, to another.

Desktop systems: Typically, personal computer hardware, software, and other peripheral devices, that users have on their desks.

e-Government: The use by the government of Web-based Internet applications and other information technologies, combined with processes that implement these technologies.

Enterprise architecture (EA): Enterprise architecture is defined by three unique groups:

(1) The Department level business function and information flow;

(2) The supporting technologies; and

(3) The crosscutting security architecture.

The business is defined through the functions performed and supporting information flows; the technology by the data, application, and technical infrastructure layers; and the security architecture that affects all layers. In the architecture, the existing state is the "as is" or current architecture, whereas anticipated changes to meet the Department's future needs are represented in the "to be" or target architecture. A transition plan is included in the Enterprise Architecture to identify how the gap between the "as is" and the "to be" states will be closed. Finally, a Technical Reference Model and Standards Profile are included to provide the supporting technology with appropriate technical standards.

Field surety: A full life-cycle approach to verification of the integrity of post classified information-processing equipment.

Graphical user interface (GUI): An interactive screen display by which the user can move a mouse to point the screen cursor at symbols representing data or instructions to the machine, reducing the need for keyboard typing.

Hardware assurance: Hardware assurance is provided through investigatory procedures that review the technology safeguards applied to classified information-processing equipment for signs of tampering.

Information resources: Information and related resources, such as personnel, equipment, funds, and information technology (IT).

Information security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information.

Information system security officer program (corporate): Designed to plan, implement, and coordinate the Department's information system security program for corporate applications and networks and to provide support for the worldwide information system security officer's activities.

Information technology architecture: An integrated framework for evolving or maintaining existing, and acquiring new, information technology to achieve the Department's strategic and information resource management goals.

Infrastructure: (Also reference network infrastructure, telecommunications infrastructure, telecommunications systems.) Hardware, software, and cabling that provides high-speed data and voice services to all users within the Department, connectivity among the Department's domestic locations and access to the Diplomatic Telecommunications Service Program Office (DTS-PO) international gateway or other communications connectivity.

Key management: Key management is the supervision and control of the process whereby encryption-keying material, to include fortezza-type certificate, is generated, stored, protected, transferred, loaded, used, and destroyed.

Life-cycle management: Life-cycle management is the ordered sequential process of planning, applying, and controlling the use of funds, human

resources and physical resources from the inception of a project throughout the operational life of the program. This includes defining user requirements, concepts, and systems specifications; acquisition planning, source selection, system implementation, deployment, operations and maintenance, and deactivation.

Local area networks (LANs): A user-owned and operated data transmission facility connecting a number of communicating devices such as computers, terminals, printers, and storage devices within a single building or a campus of buildings to provide a capability to share files and other resources among several users.

Message broker—A middleware product to support program-to program communication between existing heterogeneous (i.e., not designed to work together) applications. Message brokers are based on three principles:

(1) Program-to-program connections are more manageable, effective, and durable than database-sharing strategies;

(2) Many applications must exchange data every few seconds, minutes, or hours, rather than waiting for a nightly batch run; and

(3) Connections cost less if arranged on a many-to-many basis, so messages and the development effort required to fit interfaces into application programs can be reused.

Messaging: The electronic transfer of official and unofficial correspondence including telegrams and e-mail.

Metadata: Literally, "data about data." Information relating to business processes, data sources, and ownership, helping users to navigate through the data.

Middleware: The set of software facilities that resides between a client's application software and the server. Middleware enables the application software to communicate with the server software. Middleware includes remote procedure calls, message queuing, object request brokers, inter-process communications, remote file access, remote database access, message routing services, directory services, conversational services, time service, terminal services, and security services.

Mission essential infrastructure (MEI): This infrastructure consists of the Department's core network communication array designed to share data with posts and annexes around the world. This array or backbone includes the networking and telecommunication systems within Main State, the Beltsville Communications Center, and all other facilities, annexes, and posts that relay or bridge communications directly between two or more facilities.

The MEI within the Department serves to support the Department's mission-essential business processes that consist of telecommunications (i.e., OpenNet, ClassNet, voice systems), mainframe operations and access controls, and official and unofficial messaging.

OpenNet: OpenNet is a physical and logical Internet Protocol (IP)-based global network that links the Department of State's Local Area Networks (LANs) domestically and abroad. The physical aspect of the network uses DTS circuits for posts abroad, FTS-2001-provided circuits, leased lines, and dial-up public switch networks. This includes interconnected hubs, routers, bridges, switches, and cables. The logical aspect of the network uses Integrated Enterprise Management System (NMS) and TCP/IP software, and other operational network applications. OpenNet is a Sensitive But Unclassified (SBU) network, which supports e-mail and data applications.

PBX: Abbreviation for private branch exchange. A private telephone exchange that provides on-premises dial service and may provide connections to local and trunked communications networks.

Premise distribution system: Cabling and associated equipment installed in a facility, including the main distribution frame (MDF), intermediate distribution frames (IDFs), and telecommunications closets (TCs). Protectors and grounding systems are included.

Repository: A specialized type of database containing metadata.

Standards: An established basis of performance used to determine quality and acceptability. As applied to information technology, standards characteristically address the implementation of technical and operating functions, and interfaces between equipment, between software packages, and between equipment and software packages. Standards become rules when an appropriate authority so determines.

Systems assurance: Ensuring availability, currency, and responsiveness over the system life cycle, it incorporates the disciplines of:

(1) Change management;

(2) Quality assurance;

(3) Configuration management; and

(4) Disaster recovery and contingency planning.

Systems integrity: Systems integrity applies and provides resources and procedures to prevent unauthorized access to Department information and to ensure data integrity.

Technology safeguards: Technology safeguards include the defensive counterintelligence methods and techniques that are applied to equipment to counter potential hostile threats.

Web technology: The software and services including Telnet, file Transfer Protocol (FTP) and Web servers used to build applications, other than e-mail, that work on the Internet or OpenNet.

Wide area network (WAN): A data transmission facility that connects geographically dispersed sites using long-haul networking facilities.

Wireless communications: Radio, cellular telephone, and satellite communications, including Tactical Satellite (TACSAT), and International Maritime Satellite (INMARSAT).

1 FAM 271.5 Authorities

(TL:ORG-130; 04-30-2004)

Authorities include:

(1) Annual authorization and appropriation acts, including the Budget Enforcement Act;

(2) Freedom of Information Act of 1966, Public Law 89-554 (5 U.S.C. 552);

(3) Privacy Act of 1974, Public Law 93-579 (5 U.S.C. 552a);

(4) Federal Managers' Financial Integrity Act of 1982, Public Law 97-255;

(5) Omnibus Diplomatic Security and Antiterrorism Act of 1986, Public Law 99-399;

(6) Computer Security Act of 1987, Public Law 100-235;

(7) Computer Matching and Privacy Protection Act of 1988, Public Law 100-503;

(8) Chief Financial Officers (CFO) Act of 1990, Public Law 101-576;

(9) Government Performance and Results Act of 1993, Public Law 103-62;

(10) Federal Acquisition Streamlining Act of 1994 (FASA), Public Law 103-355;

(11) Government Management Reform Act of 1994, Public Law 103-356;

(12) Paperwork Reduction Act of 1995, Public Law 104-13;

(13) Information Technology Management Reform Act of 1996 Division E, (ITMRA) (Clinger-Cohen Act of 1996), Public Law 104-106;

(14) Federal Financial Management Improvement Act of 1996, Public Law 104-208;

(15) Electronic Freedom of Information Act Amendments of 1996, Public Law 104-231;

(16) Workforce Investment Partnership Act of 1998, Public Law 105-220;

(17) Title XVII, Government Paperwork Elimination Act of 1998, Public Law 105-277;

(18) e-Government Act of 2002, including the Federal Information Systems Management Act of 2002 (Public Law 107-347, amending 44 U.S.C. Chapter 35);

(19) Declassification of State Department Records, 22 U.S.C. 4354;

(20) Fees and Charges for Government Services and Things of Value, 31 U.S.C. 9701;

(21) Architectural and Transportation Barriers Compliance Board, Electronic and Information Technology Accessibility Standards, 36 CFR Part 1194;

(22) Federal Property Management Regulations, 41 CFR Chapter 101;

(23) Federal Management Regulation System, 41 CFR Chapter 102;

(24) Federal Acquisition Regulations, 48 CFR Chapter 1, Subpart 39.2, Electronic and Information Technology;

(25) Department of State Acquisition Regulation (DOSAR), 48 CFR Chapter 6;

(26) Executive Order (E.O.) 10346, Preparation by Federal Agencies of Civil Defense Emergency Plans;

(27) E.O. 12472, Assignment of National Security and Emergency Preparedness Telecommunication Functions;

(28) E.O. 12656, Assignment of Emergency Preparedness Responsibilities, E.O. 12656;

(29) E.O. 12862, Setting Customer Service Standards;

(30) E.O. 12931, Federal Procurement Reform;

(31) E.O. 12958, Classified National Security Information (as amended by E.O. 13292);

(32) E.O. 12999, Educational Technology: Ensuring Opportunity for all Children in the Next Century;

(33) E.O. 13010, Critical Infrastructure Protection;

(34) E.O. 13011, Federal Information Technology;

(35) E.O. 13048, Improving Administrative Management in the Executive Branch,

(36) E.O. 13101, Greening the Government Through Leadership in Environmental Management;

(37) E.O. 13103, Computer Software Piracy;

(38) Capital Programming Guide, Version 1.0, Supplement to OMB Circular A-11, Part 3: Planning Budgeting, Acquisition and Management of Capital Assets;

(39) OMB Circular A-76, Performance of Commercial Activities;

(40) OMB Circular A-109, Acquisition of Major Systems;

(41) OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards;

(42) OMB Circular A-123, Management Accountability and Control;

(43) OMB Circular A-127, Financial Management Systems;

(44) OMB Circular A-130, Management of Federal Information Resources;

(45) OMB Circular A-131, Value Engineering;

(46) OMB Memorandum 96-22, Implementation of the Government Performance and Results Act of 1993;

(47) National Security Decision Directive 145;

(48) PDD 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas;

(49) PDD 63, Critical Infrastructure Protection;

(50) PDD 67, Enduring Constitutional Government and Continuity of Government Operations;

(51) Federal Preparedness Circular 60, Continuity of the Executive Branch of the Federal Government at the Headquarters Level During National Security Emergencies;

(52) Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations;

(53) SECY-00-0088, National Plan for Information Systems Protection; and,

(54) Other guidance and authorities, as appropriate.

1 FAM 272 OFFICE OF INFORMATION ASSURANCE/CHIEF INFORMATION SECURITY OFFICER (IRM/IA) (CISO)

(CT:ORG-198; 10-15-2008)

The Office of Information Assurance/Chief Information Security Officer (IRM/IA) (CISO):

(1) Serves as Chief Information Security Officer (CISO) for the Department;

(2) Serves as the Chief Information Officer's (CIO) primary adviser concerning Department information security issues. Serves as the CIO's representative on intra- and inter-agency issues regarding information security;

(3) Serves as designated senior agency information security official as specified in the Federal Information Security Management Act (FISMA) 2002 (44 U.S.C. Chapter 35) or other applicable law;

(4) Serves under the supervision of the CIO, carrying out the CIO's responsibilities under 44 U.S.C. 3544;

(5) Heads the Office of Information Assurance (IRM/IA) with the mission and resources to assist in ensuring agency compliance with FISMA 2002 and other applicable national requirements and mandates;

(6) Develops and maintains an agency-wide information security program as required by 44 U.S.C. 3544(b);

(7) Coordinates the design and implementation of processes and practices that assess and quantify risk with respect to information resources;

(8) Develops and maintains information security policies, procedures, and control techniques to address all applicable information security requirements, including those issued under 44 U.S.C. 3543 and 40 U.S.C. 11331;

(9) Trains and oversees personnel with significant responsibilities for information security with respect to those responsibilities and provides liaison with information systems security officers domestically and abroad;

(10) Advises and assists Department senior management with their information security responsibilities;

(11) Reports Department compliance status with program-related Federal mandates to Department leadership, OMB, and Congress; and

(12) Serves as co-chair of the Department's Information Security Steering Committee.

1 FAM 273 STATE MESSAGING AND ARCHIVE RETRIEVAL TOOLSET PROGRAM MANAGEMENT OFFICE (IRM/SMART)

(CT:ORG-198; 10-15-2008)

The State Messaging and Archive Retrieval Toolset Program Management Office (IRM/SMART):

(1) Re-engineers, consolidates, and modernizes Department corporate messaging, collaboration and archiving processes and systems to satisfy business needs and legal requirements;

(2) Provides ability to search, manage, archive, and retrieve the information and knowledge contained in Working and Archival messages;

(3) Plans and manages critical special programs related to IRM-wide missions;

(4) Manages SMART strategic project activities including planning, budget, and coordination with Department long-range vision priorities, and legal requirements;

(5) Manages SMART tactical program including finance, schedule, personnel, acquisition, risk, and quality;

(6) Determines requirements for Command and Control Messaging and designs solutions to meet Department business and legal requirements. Develops and integrates SMART core messaging solutions with other Department and external systems. Ensures that solutions meet configuration, security, and statutory requirements;

(7) Defines SMART architecture and ensures performance, integration and interoperability with related IT investments;

(8) Manages test and quality control for the SMART system;

(9) Develops and operates the SMART system laboratories; and,

(10) Deploys SMART worldwide and provides technical support and training.

1 FAM 274 DEPUTY CHIEF INFORMATION OFFICER FOR BUSINESS, PLANNING AND CUSTOMER SERVICE/CHIEF KNOWLEDGE OFFICER (IRM/BPC)

(CT:ORG-198; 10-15-2008)

The Deputy Chief Information Officer for Business, Planning and Customer Service/Chief Knowledge Officer (IRM/BPC):

(1) The DCIO/CKO assists and advises the Chief Information Officer (CIO) in the execution of his or her responsibilities;

(2) Ensures that the Department's information resource management

decisions reflect the needs of the Department's business practitioners. Anticipates changes in both technology and the business practices of the Department to ensure that the Department's information resources programs fully meet information, e-Government, and knowledge management objectives;

(3) Manages overall liaison, interface, and outreach functions within the bureau and Department to provide information resource management policies and programs that best support the Department's business practitioners and business practices;

(4) Exercises leadership and provides management guidance to deliver IRM products and services to the bureau's internal and external customers;

(5) Exercises leadership on IT architecture, engineering and planning, and e-Government. Ensures that IT architectures and plans provided by IRM are effective and consistent with Federal IT architecture programs and requirements;

(6) Exercises strategic responsibility in the Department for developing and implementing improvements in information technology infrastructure, systems, and programs to improve communication and collaboration among U.S. foreign affairs agencies domestically and at posts and missions abroad;

(7) As Chief Knowledge Officer, provides strategic direction and advocacy to manage knowledge assets and programs throughout the Department; and guides and supports knowledge management initiatives within State and between State and other agencies and foreign affairs partners;

(8) Provides liaison and fosters cooperation with other Federal agencies, educational institutions, non-governmental, not-for-profit, and private-sector organizations regarding knowledge management initiatives, practices, and standards;

(9) Provides overall leadership of the Department's e-Government initiatives and programs; and

(10) Represents the Business Practices and Programs office in the e-Government Program Board.

1 FAM 274.1 Customer Service Office (IRM/BPC/CST)

(CT:ORG-198; 10-15-2008)

The Customer Service Office (IRM/BPC/CST):

(1) Reports to the Chief Knowledge Officer, Deputy Chief Information Officer for Business, Planning and Customer Service (IRM/BPC) on IRM's compliance with guidelines prescribed in accordance with applicable laws and regulations pertaining to customer service standards;

(2) Oversees IRM liaison and support activities to ensure that customer service issues are resolved;

(3) Maintains liaison with functional and regional bureaus, the Diplomatic Telecommunications Service Program Office (DTS-PO), other U.S. Government agencies, and foreign governments to ensure appropriate customer support;

(4) Manages technical briefings, seminars, and conferences to encourage the Department at home and abroad to facilitate the transfer of information related to information technology;

(5) Oversees IRM Business Center activities to support Department and IRM Bureau e-Government and e-Diplomacy strategic objectives and performance goals through research, advice, consultation, development, and implementation of enterprise-wide, Web-based technology solutions; and

(6) Provides oversight for support services including the InfoCenter Service Desk for the IRM Bureau and the Department.

1 FAM 274.1-1 Business Center Division (IRM/BPC/CST/BC)

(CT:ORG-198; 10-15-2008)

The Business Center Division (IRM/BPC/CST/BC):

(1) Manages the activities of the Business Center Division to ensure that the technology-based services provided are fully, effectively, and successfully integrated in support of Department and IRM Bureau strategic objectives and performance goals;

(2) Coordinates and advises on enterprise level Web-based solutions and technology adoption issues;

(3) Coordinates enterprise-level Intranet and Extranet activities to ensure conformance with Department-wide IT architectures and plans;

(4) Researches and develops information technology solutions to meet the enterprise business needs;

(5) Provides consultation services on applying information technology to mission requirements;

(6) In support of e-Diplomacy:

(a) Provides project development support for e-Diplomacy and other related program initiatives designed to enable effective collaboration between foreign affairs agencies;

(b) Develops Web-based solutions to support Department efforts to organize, communicate, and provide ready access to information both internally and externally;

(c) Researches and evaluates new and emerging technologies for potential application to Department mission requirements; and

(d) Promotes strategies and practices to enhance the management of the Department’s information assets.

(7) With regard to enterprise solutions:

(a) Develops and implements enterprise-level, Internet-based solutions to enhance IRM Bureau mission accomplishment;

(b) Provides Web and portal development services in response to customer requirements from throughout the Department and the foreign affairs community;

(c) Provides graphics and design support for IRM marketing and information dissemination projects;

(d) Researches, develops, and implements efforts to integrate business processes and new information management technologies; and

(e) Leads effort to expand Department use of SIPRNET, ClassNet,

OSIS, and OpenNet to exchange data securely among Department users and with other agencies.

(8) With regard to business operations:

(a) Provides a wide variety of technical services in support of the bureau's IT infrastructure, including information security, data base administration, and systems/network administration;

(b) Manages a rigorous configuration management and quality assurance process for all IRM Bureau products and services produced;

(c) Provides Web hosting and domain name administration services in support of Department Web sites and portals; and

(d) Develops and manages budgets for reimbursable services accounts.

(9) With regard to business development solutions:

(a) Promotes IRM Bureau IT products and services to the Department and other agencies through marketing and information dissemination efforts;

(b) Provides business process reengineering, change management, and related IT consulting services to promote best practices and continuous improvement of Department IT products and services; and

(c) Plans and manages briefings, seminars, conferences, and other events to promote interaction among information technology professionals and to facilitate information exchange throughout the Department.

1 FAM 274.1-1(A) Systems Accessibility Staff (IRM/BPC/CST/BC/SAS)

(CT:ORG-198; 10-15-2008)

The Systems Accessibility Staff (IRM/BPC/CST/BC/SAS):

(1) Promotes universal accessibility to Department technology, information, services, and programs through efforts such as the Information Resources Management Program for Accessible Computer/Communication Technology (IMPACT); and

(2) Provides advice and guidance to systems planners, developers, and administrators to ensure compliance with Section 508 of the Rehabilitation Act and related regulatory requirements.

1 FAM 274.1-2(B) Liaison Division (IRM/BPC/CST/LD)

(CT:ORG-198; 10-15-2008)

The Liaison Division (IRM/BPC/CST/LD):

(1) Provides liaison with functional and regional bureaus, the Diplomatic Telecommunications Service—Program Office (DTS-PO), other U.S. Government agencies, and foreign governments, to ensure that all IRM Bureau customer issues are resolved;

(2) Provides assistance to customers with ordering and delivery of IRM Bureau products and services;

(3) Oversees negotiation, coordination, and monitoring of agreements with Department bureaus and foreign affairs agencies about information resources; and

(4) Coordinates the preparation of all service-level agreements between the IRM Bureau and its internal and external customers.

1 FAM 274.1-2(B)(1) Overseas Branch (IRM/BPC/CST/LD/OB)

(CT:ORG-198; 10-15-2008)

The Overseas Branch (IRM/BPC/CST/LD/OB):

(1) Provides liaison with regional bureaus and posts to ensure that all IRM Bureau customer issues are resolved;

(2) Oversees negotiation, coordination, and monitoring of agreements with regional bureaus covering the terms and conditions under which the IRM Bureau will provide information services. Ensures that such agreements are consistent with the Department’s information resources management policies, goals, and objectives; and

(3) Prepares and coordinates responses from posts abroad pertaining to OIG issues.

1 FAM 274.1-2(B)(2) Domestic Branch (IRM/BPC/CST/LD/DB)

(CT:ORG-198; 10-15-2008)

The Domestic Branch (IRM/BPC/CST/LD/DB):

(1) Provides liaison with functional bureaus regarding domestic information technology issues;

(2) Oversees negotiation, coordination, and monitoring of agreements with functional bureaus covering the terms and conditions under which the IRM Bureau will provide information services. Ensures that such agreements are consistent with the Department's information resources management policies, goals, and objectives;

(3) Provides liaison with the School of Applied Information Technology (SAIT) and the Bureau of Diplomatic Security (DS) on IRM Bureau projects and issues;

(4) Serves as the IRM Bureau and Chief Information Officer's vendor liaison. Plans and hosts briefings by vendors and information technology (IT) industry experts concerning topics of interest within the IRM Bureau; and

(5) Promotes professional interaction among information technology professionals throughout the Department by managing technical briefings, seminars, and conference abroad.

1 FAM 274.1-2(B)(3) External Affairs Branch (IRM/BPC/CST/LD/EA)

(CT:ORG-198; 10-15-2008)

The External Affairs Branch (IRM/BPC/CST/LD/EA):

(1) Provides liaison with DTS-PO and other foreign affairs agencies to ensure that all IRM Bureau customer issues are resolved;

(2) Oversees negotiation, coordination, and monitoring of agreements with other Department bureaus and foreign affairs agencies, covering the terms and conditions under which the Department will provide information services to the representatives of such bureaus domestically, as well as other agencies located at diplomatic missions and consular posts abroad. Ensures that such agreements are consistent with the Department's foreign affairs and information

management policies, goals, and objectives;

(3) Consults, coordinates, and negotiates agreements with foreign governments, foreign telecommunications service providers, and international organizations encompassing the full range of the Department's international information resources management requirements, including, as appropriate, reciprocal arrangements;

(4) Oversees the Department's representation to the National Communications System (NCS) and NATO's Civil Communications Planning Committee, and ensures that the Department is represented on interagency committees addressing IRM matters as directed by senior management; and

(5) Provides guidance and support with respect to the negotiation, implementation, monitoring, and further improvement of the U.S.–Russian Federation and Newly Independent States direct communications link (DCL), the Nuclear Risk Reduction Center (NRRC), the government-to-government communications link (GGCL), and such other initiatives.

1 FAM 274.1-3 Support Services Division (IRM/BPC/CST/SPS)

(CT:ORG-198; 10-15-2008)

The Support Services Division (IRM/BPC/CST/SPS):

(1) Provides Department employees worldwide with a single point of contact for information or assistance on IRM Bureau products and services and standard commercial off-the-shelf (COTS) products;

(2) Provides IRM management and other Department bureaus with reports relating to incident management, from preparing initial requests for services and records management to performing monitoring and closure; and

(3) Operates and manages a variety of information technology (IT) hardware, software, and peripherals for the bureau, division, and Department, supporting customers worldwide.

1 FAM 274.1-3(A) InfoCenter Branch (IRM/BPC/CST/SPS/IS)

(CT:ORG-198; 10-15-2008)

The InfoCenter Branch (IRM/BPC/CST/SPS/IS):

(1) Manages the centralized IRM InfoCenter Service Desk for the IRM Bureau and Department. Provides domestic and Department employees abroad with a single point of contact for information or assistance on IRM Bureau products and services and standard commercial off-the-shelf products;

(2) Provides complete incident recording, tracking, and follow-up for all service requests received at the IRM InfoCenter Service Desk from Department employees;

(3) Provides first-level support (Tier-1) to Department employees, and, when required, transfers and monitors completion of service requests to other IRM Bureau service providers (Tier-2 and Tier-3) and Department technical support functions for resolution;

(4) Manages problem escalation, when necessary;

(5) Provides "early warning" and other notifications of core outages and other events, when necessary; and

(6) Provides on site domestic Tier-2 service for offices or bureaus requesting second-level support.

1 FAM 274.1-3(B) Operations Support Branch (IRM/BPC/CST/SPS/OS)

(CT:ORG-198; 10-15-2008)

The Operations Support Branch (IRM/BPC/CST/SPS/OS):

(1) Is the office responsible for valid, reliable, and timely information by providing systems and network administration, research and analysis, and training support to our external and internal customers of the Support Services Division;

(2) Consists of two teams:

(a) Systems Team—responsible for all systems design,

integration, account administration, and network administration for this division, as well as selected customers; and

(b) Research and Analysis Team—responsible for all statistical analysis and reporting, data management, training division personnel, quality assurance, service-level agreements, and outreach for the division.

(3) OS provides:

(a) IRM management and other Department bureaus with research and analysis relating to incidents reported to the Support Services Division;

(b) Ensures that the information technology hardware, software, and communications systems in the division are operational and meet the configuration standards of the Department;

(c) Ensures that all Division information technology resources are maintained at a desired level of availability and reliability to support a 24x7 operation and enable the division to provide Tier-1 and Tier-2 Helpdesk support;

(d) Provides backup systems administration support to other bureaus within the Department of State;

(e) Negotiates and documents service level agreements between the Support Services Division (SPS) and functional and regional bureaus and between SPS and offices within IRM;

(f) Measures, analyzes, and reports performance as specified in service level agreements developed for the information technology service management (ITSM) initiative;

(g) Monitors IRM news groups and conferences on the intranet, and posts solutions from the InfoCenter knowledge base;

(h) Conducts quality assurance and quality control (QA/QC); solicits and reviews IRM InfoCenter customer satisfaction; interprets feedback; and provides reports with recommendations for quality-of service-improvements;

(i) Participates in developing documentation to support various IRM products and services for the IRM InfoCenter and customers worldwide, and works with other IRM organizations to develop training materials;

(j) Collaborates with other IRM service providers and systems experts on technical evaluations and special projects;

(k) Provides as-needed on-site support for the Under Secretary for Management, Chief of Protocol, and the Chief Information Officer regarding general network issues, user access, and Web and e-mail operations;

(l) Manages the operation of all information technology (IT) systems currently in place in the division, and ensures adherence to all Department of State, Diplomatic Security, IRM, and Division policies;

(m) Manages non-technical seminars on a variety of information technology subject areas of interest to the Department;

(n) Updates and maintains all hardware, software, peripherals, and allied equipment to ensure continued and uninterrupted operational capability;

(o) Maintains the IRM incident-reporting database, ensuring its availability, reliability, and security regardless of hardware or software platform, and maintains links to all Department information technology network monitoring platforms to ensure timely awareness of any disruptions in service;

(p) Performs property accounting for the division;

(q) Evaluates, tests, and integrates state-of-the-art technology in support of our global technical support mission and installs and maintains multiple enterprise-wide application servers. The applications servers provide numerous capabilities to the Support Services Division, such as access to information for Department employees worldwide;

(r) Develops, enhances, and maintains the suite of IT tools used by the on-line technical information; and

(s) Develops, documents, and maintains standard operating procedures for performing customer support functions within the division and between the division and customer offices worldwide.

1 FAM 274.2 Enterprise Architecture and Planning Office (IRM/BPC/EAP)

(CT:ORG-198; 10-15-2008)

The Enterprise Architecture and Planning Office (IRM/BPC/EAP):

(1) As the e-Government (e-Gov) Program Management Office under the direction of the CIO, manages the entire IT Capital Planning Process as the agent of the e-Gov Planning Board (e-GovPB), an advisory entity to the Under Secretary for Management, which is the highest-level organization that addresses the full range of the Department's e-Gov and IT Capital Planning activities. The e-GovPB's associated organizations include the e-Gov Advisory Group and e-Gov Working Group;

(2) Manages the activities of the Enterprise Architecture Division and Planning Division to ensure that IT architectures and plans produced by IRM/BPC/EAP are fully, effectively, and successfully integrated to meet the Department's business needs;

(3) Acts as the Department of State's senior authority on IT architecture, engineering, and planning issues. Ensures that the Department's IRM architecture, engineering, and planning initiatives are conducted in accordance with government requirements and industry's best practices; and

(4) Leads efforts to coordinate IT architecture and planning activities that take place in bureaus throughout the Department, to ensure that these decentralized activities conform with and support the Enterprise Architecture, and e-Government Strategic plans.

1 FAM 274.2-1 Enterprise Architecture and Engineering Division (IRM/BPC/EAP/EA)

(CT:ORG-198; 10-15-2008)

The Enterprise Architecture and Engineering Division (IRM/BPC/EAP/EA):

(1) Develops and maintains the Department's Enterprise Architecture, which is based on the Department's Federal Enterprise Architecture, including baselines, transitions, and targets;

(2) Develops and maintains principles, processes, standards, and product standardization for all elements of the Enterprise

Architecture; and

(3) For the IRM Bureau, and other bureaus and offices throughout the Department:

(a) Reviews information technology plans and programs, including applications, data, networks, and platforms, for conformance with Department Enterprise Architecture;

(b) Supports business process reengineering initiatives;

(c) Investigates the implications of emerging technologies for supporting business requirements and analyzes the possible effects of such technologies on business requirements; and

(d) Assists in ensuring engineering compatibility of specific applications, data, networks, and platforms, with the Enterprise Architecture.

1 FAM 274.2-2 Planning Division (IRM/BPC/EAP/PL)

(CT:ORG-198; 10-15-2008)

The Planning Division (IRM/BPC/EAP/PL) serves under the direction of the Department's Deputy Chief Information Officer and through the Director of the Enterprise Architecture and Planning Office as the e-Government Program Office (e-Gov PMO), established under the Department's e-Government Program Board (e-GovPB) process. It:

(1) Implements the Department's Information Technology strategic planning activities by developing the Information Technology and e-Government Strategic Plans and coordinating them with the Department's strategic planning activities;

(2) Implements the control and evaluation function of the Department's capital planning and investment control (CPIC) process by reviewing status reports from project managers on performance measures and cost and schedule goals, seeking to identify at-risk projects and acting to mitigate risks or correct problems. Manages all phases of the IV and V processes. Conducts performance reviews of major projects in the Department's current fiscal year IT capital asset plan;

(3) Supports the e-Government Program Board by coordinating the Department's IT Capital Planning activities:

(a) Manages the formulation, preparation, and dissemination of the Department's IT Capital Asset Plans, including preparing the OMB Exhibit 53 and Exhibit 300s for the Department's e-Gov/IT projects;

(b) Manages the operation, maintenance, and enhancement of the Investment Portfolio Project Tracking System (I-TIPS), which is a Web-based project tracking system that collects information on IT initiatives; and

(c) Develops procedures for the e-GovPB to use for selecting, monitoring, and evaluating Department Information Technology projects.

(4) Provides staff and administrative support for the meetings of the e-GovPB and associated organizations:

(a) Develops and coordinates the Department's e-Gov/IT Project Management Support Program by establishing a comprehensive project management curriculum to prepare project managers. Serves as technology, infrastructure, interoperability, and security advocate. *It* is assisted in this responsibility by the Enterprise Architecture Division and the Information Assurance Office of the Bureau of Information Resource Management;

(b) Serves as the Department's point of contact (POC) for implementing the e-Government (e-Gov) initiative of the President's Management Agenda (PMA) and e-Gov legislation (the e-Government Act of 2002, the Government Paperwork Elimination Act, and other related statutes). Coordinates Department-wide responses to OMB, Federal CIO Council, and other interagency e-Gov tasks, directives, and guidance. Coordinates Department representation at inter-agency meetings, working groups, conferences, and other forums on the e-Gov initiative of the PMA and e-Government generally.

1 FAM 274.3 e-Diplomacy Office (IRM/BPC/EDIP)

(CT:ORG-198; 10-15-2008)

The e-Diplomacy Office (IRM/BPC/EDIP):

(1) Has primary responsibility under the Deputy CIO/Chief Knowledge Officer for ensuring that user needs and business practices are fully reflected in the Department's information resource decisions; for

improving interagency communication and collaboration; and for developing and implementing the Department's knowledge management strategy;

(2) Serves as liaison with interagency working groups on communication and collaboration;

(3) Provides advocacy and advice in its areas of responsibility as a member of the e-Government Program Board;

(4) Promotes programs to build the knowledge-sharing culture and infrastructure to achieve the Department's knowledge management goals with regard to technology, knowledge-sharing, and decision-making;

(5) Ensures that enterprise solutions support business practices that maximize and leverage the Department's knowledge resources in the following ways:

(a) Encourages and enables individuals and organizations to draw from and add to the Department's knowledge base and to share their expertise and experience;

(b) Ensures consistent, visible executive support for knowledge-sharing and knowledge-resource development;

(c) Promotes and develops technology-enabled communities and other forms of knowledge-management activities that meet the business needs and enhance the business practices of Department users;

(d) Factors knowledge management considerations into recruitment, training, and rewards and recognition programs; promotes a new training model that educates personnel on the importance and potential of knowledge management for the Department as well as individuals; and links training on knowledge tools to everyday user needs and business practices;

(e) Promotes content management procedures that identify, collect, categorize, and refresh knowledge using common frameworks across the Department;

(f) Promotes security practices that reflect changing business needs while providing adequate security for information resources and business users;

(g) Develops or adapts work processes to include knowledge management tools and practices as an integral part of the daily workflow;

(h) Develops and implements knowledge management programs to managers at all levels with accurate, relevant, and timely information; and

(i) Promotes high-quality services and technology that foster collaboration and reduce the time, costs, and efforts of transactions and that enable the Department's users and foreign affairs partners to exchange or receive appropriate information whenever and wherever they need it.

(6) Promotes innovative knowledge management and e-Government solutions throughout the Department and with other foreign affairs agencies and partners. Provides leadership, support, and facilitative and consulting services for bureaus and posts in these areas; and

(7) Initiates and supports e-Government cross-cutting projects that meet business requirements and user and customer needs. In coordination with the e-Government Program Office, assists bureaus and posts to conceive, design, estimate cost, implement, and manage such initiatives.

1 FAM 274.4 Information Resource Policy and Regulations Office (IRM/BPC/PRG)

(CT:ORG-198; 10-15-2008)

The Information Resource Policy and Regulations Office (IRM/BPC/PRG):

(1) Is the office responsible for the content of volume 5 of the Foreign Affairs Manual (5 FAM) and its associated Foreign Affairs Handbooks (5 FAHs). Ensures that 5 FAM is accurate, complete, and timely. Addresses cross-cutting Department policies, regulations, and procedures concerning Department-wide information resources management in 5 FAM. Coordinates for publication 5 FAM subjects, ensuring that all relevant stakeholders are included in the clearance process;

(2) Serves as a repository for all Department-wide information *resource* management-related statutes, executive orders, legal mandates, regulations, guidelines, etc;

(3) Reviews proposed new Federal information resource management statutes and regulations. Provides comments and interpretations, as appropriate, to IRM Bureau managers and other information resource managers throughout the Department. Ensures dissemination of these materials throughout the IRM Bureau and the Department;

(4) Serves on interagency committees, as directed, by senior management;

(5) Conducts reviews of information management processes in the Department to assess the effectiveness of policies. Recommends changes in policies. Works with operational offices to identify any operational issues; and

(6) In coordination with the Bureau of Resource Management (RM), serves as the Department's liaison to the U.S. Government Accountability Office (GAO) regarding Information Technology (IT) audits. Initiates, coordinates, and reviews Department-wide input and prepares the official response for CIO approval and final RM clearance.

1 FAM 275 DEPUTY CHIEF INFORMATION OFFICER FOR OPERATIONS/CHIEF TECHNOLOGY OFFICER (IRM/OPS)

(CT:ORG-198; 10-15-2008)

The Deputy Chief Information Officer for Operations/Chief Technology Officer (IRM/OPS):

(1) Provides overall liaison, interface, and outreach functions within the Department to supply the information resources management operations that best support the Department's mission and functions;

(2) Provides direction and policy guidance on substantive operational activities in the IRM Bureau to ensure that the Department and other foreign affairs agencies receive the full range of worldwide rapid, reliable, responsive, secure, classified, and unclassified voice and data information management operating systems, networks, programs, and support services in a cost-effective, customer service-oriented manner. Ensures that people with disabilities have access to information technology;

(3) Provides enterprise-wide business systems, system integration, mainframes, and client/server operations, consistent with the principles embodied in the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act);

(4) Implements U.S. Government information management directives. Directs IRM's providing of operational products and support services to the Department and to other foreign affairs agencies as information resource management operating programs are implemented under Department inter-bureau and U.S. Government interagency agreements, as appropriate;

(5) Provides leadership and technical experts for the U.S.-Russian Federation and Newly Independent States Direct Communications Link (DCL), the Nuclear Risk Reduction Center (NRRC), and the Government-to-Government Communications Link (GGCL), and such other similar systems, as may be established;

(6) Provides technical guidance, consistent with the "Department of State Enterprise Architecture and Information Technology Strategic and Performance Measurement Plan" to bureaus and offices so that they can implement appropriate information technology operations;

(7) Accounts for the management and overall security of the classified and unclassified mainframe systems; and

(8) Oversees the Defense Liaison Office reporting to the IRM Bureau.

1 FAM 275.1 Enterprise Network Management Office (IRM/OPS/ENM)

(CT:ORG-198; 10-15-2008)

The Enterprise Network Management Office (IRM/OPS/ENM), in conjunction with other IRM offices and DTS/PO, the ENM directorate is responsible for managing and overseeing the design, operation, and life-cycle management of the Department's worldwide networks. The office is comprised of three divisions and one staff office.

1 FAM 275.1-1 Network Engineering and Design Division (IRM/OPS/ENM/NED)

(CT:ORG-198; 10-15-2008)

The Network Engineering and Design Division (IRM/OPS/ENM/NED):

(1) Provides technical guidance and support for the design, development, and engineering of the Department's enterprise network;

(2) Provides technical guidance and support for the design, development, and engineering of the Department's server and client operating systems;

(3) Validates applications to run on the Department's network, as appropriate;

(4) Performs capacity planning and ensures optimum performance of the Department's networks;

(5) Supports the IRM Customer Center in consolidating wide-area network and operating system requirements; and

(6) Oversees the development, implementation, and maintenance of the Integrated Enterprise Management System (IEMS), which includes proactive network monitoring, problem resolutions, escalation, troubleshooting, and trouble-ticketing.

1 FAM 275.1-2 Operations Division (IRM/OPS/ENM/OPS)

(CT:ORG-198; 10-15-2008)

The Operations Division (IRM/OPS/ENM/OPS):

(1) Oversees and provides 24-hour management and administrative support for the Department's networks;

(2) Ensures the reliable operations and performance of classified/unclassified internet-working systems and network services;

(3) Provides operational, administrative, and management support for the worldwide internet protocol (IP) network through the Department's Enterprise Network Management Operations Center (ENMOC);

(4) Provides operational support for the Department's server and client operating systems; and

(5) Provides technical support and coordination for detecting and correcting IT security vulnerabilities.

1 FAM 275.1-3 Networks Life-Cycle Management Division (IRM/OPS/ENM/NLM)

(CT:ORG-198; 10-15-2008)

The Networks Life-Cycle Management Division (IRM/OPS/ENM/NLM):

(1) Provides oversight and management responsibility for developing and maintaining technical baselines for the network infrastructure;

(2) Provides technical assistance in the form of testing, evaluating, and reviewing the enterprise network equipment, systems, services, and technical support for the Department's Configuration Control Board (CCB);

(3) Establishes and maintains a network configuration management plan (CMP) to monitor, track, and approve engineering changes, upgrades, modifications, procedures, precepts, and criteria. Maintains an accurate database of hardware, firmware, software, and documentation for the Department's networking assets;

(4) Conducts integration testing and evaluation for new or modified hardware or software for the enterprise network; coordinates software distribution, new releases, updates, fixes, and version controls;

(5) Provides enterprise patch management support. Provides patch support to mitigate vulnerabilities or provide alternate patch solutions for the DOS environment;

(6) Provides asset management services (i.e., life-cycle replacement schedules) for Department IT Infrastructure; and

(7) Provides acquisition and procurement support for products, labor, and services required for enterprise-wide IT management, operations, and maintenance responsibilities.

1 FAM 275.2 Information Technology Infrastructure Office (IRM/OPS/ITI)

(CT:ORG-198; 10-15-2008)

The Information Technology Infrastructure Office (IRM/OPS/ITI):

(1) Advises the Deputy Chief Information Officer for Information Resource Management Operations and other high-level officials in the Department regarding infrastructure issues;

(2) Directs and manages the development, maintenance, installation, and operations of the Department's telephone, radio, and wireless communications programs. Provides for systems integrity and technology safeguards in conformance with established Bureau of Diplomatic Security standards and policies;

(3) Implements policies, standards, and procedures to conform with established Department of State architecture standards and policies to ensure effective and efficient infrastructure; and

(4) Evaluates the utilization of new technology as it applies to the Department's infrastructure.

1 FAM 275.2-1 LAN and WAN Service Division (IRM/OPS/ITI/LWS)

(CT:ORG-198; 10-15-2008)

The LAN and WAN Service Division (IRM/OPS/ITI/LWS):

(1) Advises the Director for Information Technology Infrastructure on all matters concerning the installation and maintenance of local and wide-area network (LAN/WAN) infrastructure;

(2) Administers policy, standards, and procedures to conform with established Department enterprise architecture, and in regards to maintaining and installing LAN/WAN infrastructure;

(3) Maintains the Department's LAN/WAN infrastructure and associated supporting technologies;

(4) Provides LAN/WAN infrastructure security to conform with Department security standards;

(5) Develops acquisition plans for new requirements; serves as contracting officer representative; and performs contract administration for all existing contacts for labor, equipment, maintenance, and spare parts in support of LAN/WAN services; and

(6) Provides oversight and management for the Department's Radio Program, Foreign Posts Telephone Program, and the Liaison Office to the Bureau of Overseas Buildings Operations (OBO).

1 FAM 275.2-1(A) Liaison Branch/OBO (IRM/OPS/ITI/LWS/LT-OBO)

(CT:ORG-198; 10-15-2008)

The Liaison Branch/OBO (IRM/OPS/ITI/LWS/LT-OBO):

(1) Provides OBO with IRM's IT requirements for space, environmental systems, cabling, and information security systems at new office buildings, (NECs), interim office buildings (IOBs), and temporary office buildings (TOBs) at posts abroad;

(2) Continuously reviews architectural, mechanical, and electrical drawings for NECs to ensure that IT facilities and environmental systems are adequate to accommodate IRM's information, communications systems, and personnel; and

(3) Tracks the progress of all NEC, IOB, and TOB projects and coordinates all of IRM's technical plans for acquisitions and installations and informs the appropriate program office of all project changes, schedule delays, and engineering changes.

1 FAM 275.2-1(B) Installation Branch (IRM/OPS/ITI/LWS/ITL)

(CT:ORG-198; 10-15-2008)

The Installation Branch (IRM/OPS/ITI/LWS/ITL):

(1) Implements policy standards and procedures regarding the installation of LAN/WAN infrastructure;

(2) Plans, designs, installs, and documents installation of LAN/WAN infrastructure and related technologies;

(3) Provides enterprise integrity and remediation for the Department's installed information technology infrastructure; and

(4) Provides technical training and oversight for Information Management Technical Specialist to develop a core base of Communications Specialists (COMPSPECS).

1 FAM 275.2-1(C) Maintenance Branch (IRM/OPS/ITI/LWS/MNT)

(CT:ORG-198; 10-15-2008)

The Maintenance Branch (IRM/OPS/ITI/LWS/MNT):

(1) Implements policies, standards, and procedures as they apply to maintaining the classified LAN/MAN/WAN infrastructure abroad;

(2) Provides onsite preventative and remedial services for the continued operations or restoration of classified IT systems at posts abroad;

(3) Establishes and administers service contracts for repairing and returning failed IT hardware, firmware, or software, including INMARSATS, and for procuring new requirements;

(4) Manages the Department's International Maritime Satellite communications contingency program (INMARSATS);

(5) Conducts regular visits to posts abroad to troubleshoot and repair defective equipment and software for unclassified IT systems;

(6) Conducts regular visits to posts abroad to provide operations and maintenance support for unclassified IT systems in accordance with manufacturer's recommendations, IRM, and DS guidance and policies; and

(7) Performs depot-level maintenance and testing on failed IT equipment for posts abroad.

1 FAM 275.2-1(D) Foreign Posts Telephone Branch (IRM/OPS/ITI/LWS/FPT)

(CT:ORG-198; 10-15-2008)

The Foreign Posts Telephone Branch (IRM/OPS/ITI/LWS/FPT):

(1) Implements policies, standards, and procedures for maintaining and operating PBX telecommunications systems at all foreign posts;

(2) Plans, installs, and maintains PBX systems at foreign posts; *and,*

(3) Establishes and administers service contracts for repairing and returning failed telephone hardware, firmware, or software and for procuring telephone systems.

1 FAM 275.2-1(E) Radio Programs Branch (IRM/OPS/ITI/LWS/RPB)

(CT:ORG-198; 10-15-2008)

The Radio Programs Branch (IRM/OPS/ITI/LWS/RPB):

(1) Implements policies, standards, and procedures for maintaining and installing HF, UHF, and VHF radio systems, including TACSATS;

(2) Engineers, designs, plans, installs, and maintains radio systems;

(3) Provides emergency communications systems to posts in crisis situations and communications support for special operations;

(4) Manages the Department's Tactical Satellite Communications contingency program (TACSATS); and

(5) Supports the Coordinator for Counter-terrorism (S/CT) in deploying, operating, and maintaining the Foreign Emergency Support Team's (FEST) deployment packages for exercises and missions abroad.

1 FAM 275.2-2 Telecommunications, Wireless and Data Services Division (IRM/OPS/ITI/TWD)

(CT:ORG-198; 10-15-2008)

The Telecommunications, Wireless and Data Services Division (IRM/OPS/ITI/TWD):

(1) Advises the Director of Information Technology Infrastructure regarding all matters concerning voice, video-conferencing, voice/data, wireless services, and telecommunications infrastructure;

(2) Develops and administers policy, standards, and procedures to conform with established Department architecture regarding voice, video-conferencing, voice/data, wireless services, and telecommunications infrastructure;

(3) Maintains the Department's voice, video-conferencing, voice/data, wireless services, and telecommunication services infrastructure, and associated support telecommunications systems;

(4) Provides voice, video-conferencing, voice/data, wireless, data, and telecommunications services support to the Office of the Secretary for special infrastructure requirements; and

(5) Serves as program manager for the Department's Enterprise Network Program (E-Net), which is modernizing State's data networking in the metropolitan area. Program management includes responsibility for designing, developing, operating, and network managing premise networks (LANs), and for the metropolitan area network interconnecting the main state Department building and the annexes (MAN).

1 FAM 275.2-2(A) Business Operations Management Branch (IRM/OPS/ITI/TWD/BOM)

(CT:ORG-198; 10-15-2008)

The Business Operations Management Branch (IRM/OPS/ITI/TWD/BOM):

(1) Develops and implements policies, standards, and procedures regarding domestic telecommunications service to include call accounting, private branch exchanges (PBXs), domestic circuit acquisitions, and charge-back programs;

(2) Administers acquisition of telecommunications service to include PBXs, domestic circuits, and premise distribution systems; and

(3) Manages programs that provide for detailed call-accounting information, including long-distance calling activity.

1 FAM 275.2-2(B) Domestic Telephone and Data Services Branch (IRM/OPS/ITI/TWD/DTD)

(CT:ORG-198; 10-15-2008)

The Domestic Telephone and Data Services Branch (IRM/OPS/ITI/TWD/DTD):

(1) Develops and implements policies, standards, and procedures regarding domestic circuits, PBX operations, enterprise network (E-Net) operations, and telecommunications infrastructure; and

(2) Plans, installs, and maintains the Department's domestic circuits, PBXs, telecommunications infrastructure, and associated supporting telecommunications systems.

1 FAM 275.2-2(C) Domestic Technical Services Branch (IRM/OPS/ITI/TWD/DTS)

(CT:ORG-198; 10-15-2008)

The Domestic Technical Services Branch (IRM/OPS/ITI/TWD/DTS):

(1) Implements policies, standards, and procedures for maintaining Domestic LAN/WAN infrastructure;

(2) Provides technical services support for the Department's command and control systems, which includes the fifth floor Communications Center, the Operations Center, the Secure Voice Center, and classified data networks;

(3) Provides 7x24-hour operations and maintenance services for the Secure Voice Center and the red switch telephones systems;

(4) Provides Tier III engineering and maintenance support for the continuous operations and rapid restoration of classified networks in the fifth floor Communications Center;

(5) Provides installation, configuration, and maintenance support for the Department's classified networks cryptographic systems/equipment; and

(6) Provides installation and maintenance support for the activation and mobilization of the Department's contingency operations at alternate sites.

1 FAM 275.2-3 Systems Integrity Division (IRM/OPS/ITI/SI)

(CT:ORG-198; 10-15-2008)

The Systems Integrity Division (IRM/OPS/ITI/SI):

(1) Advises the Director of Information Technology Infrastructure on all key management infrastructure (KMI) matters; secure voice; PKI/biometric; and anti-virus programs used to implement and maintain information assurance and systems integrity;

(2) Administers KMI policy, standards, and procedures regarding cryptography, information assurance, and systems integrity to conform with national and Department policy and regulations;

(3) Provides comment(s) concerning the development of related national policy;

(4) Provides technical security oversight and management for mainframe security, cryptographic services, and Information Integrity for the Department's PKI/biometric and anti-virus programs; and

(5) Coordinates IRM integration, verification, and interoperability (IV&V) testing for the Department's IT assets using or supported by anti-virus, cryptographic, mainframe, PKI, and biometric security systems.

1 FAM 275.2-3(A) Cryptographic Services Branch (IRM/OPS/ITI/SI/CSB)

(CT:ORG-198; 10-15-2008)

The Cryptographic Services Branch (IRM/OPS/ITI/SI/CSB):

(1) Advises all Department bureaus of encryption devices and technology necessary to comply with national and Department information assurance (IA) practices;

(2) Implements key management infrastructure (KMI) policies, standards, and procedures as they apply to Type I, II, III encryption devices to include symmetrical and asymmetrical algorithms;

(3) Manages the Department's communications security (COMSEC) programs (i.e., COMSEC material control system (CMCS) and central office of record (COR)) to meet national cryptographic management and audit policy requirements;

(4) Manages the Department's cryptographic clearance (access) office and procedures and associated services to include maintaining 5 FAH-6, Communications Security Handbook; and

(5) Manages the Department's secure voice program.

1 FAM 275.2-3(B) Information Integrity Branch (IRM/OPS/ITI/SI/IIB)

(CT:ORG-198; 10-15-2008)

The Information Integrity Branch (IRM/OPS/ITI/SI/IIB):

(1) Implements policies, standards, and procedures regarding information systems security to conform with Department regulations;

(2) Manages the Department's Mainframe Security Program to ensure compliance with Department security policies and industry best practices. Develops, implements, and administers, policies, standards, and procedures regarding mainframe security, with specific emphasis on amplifying and correlating workstation and network-centric Department policies to the mainframe environment. Installs, tailors, configures, and operates all software packages designed to establish, facilitate, augment, and/or control:

(a) User identification and authorization;

(b) Data and resource access control;

(c) Security event monitoring and auditing; and

(d) Cryptographic services support on mainframe hardware platforms regardless of the operating system.

(3) Serves as COMSEC custodian for mainframe based cryptographic service systems. Monitors and advises on, as appropriate, the installation and operation of mainframe interfaces with the OpenNet, Internet, or dedicated interagency communication links to ensure compliance with Department security guidelines; provides procedural safeguards for data transiting these boundaries;

(4) In a custodial capacity, implements technical security controls on behalf of all mainframe system and application owners; advises on the secure design, installation, and operation of systems and applications; serves as a voting member on the SIO/EOC CCB on suitability of mainframe hardware and software selection and configuration; and monitors and advises on security matters for IT/CCB Change Records relevant to, or concerning interfaces with, the mainframes. The Information Integrity Branch conducts internal system security reviews and renders internal audit reports to all Department mainframe systems and applications owners;

conducts real-time security event monitoring and mainframe network intrusion detection; and serves as a first-level CIRT for security incidents originating on any mainframe platform or at its boundary interfaces;

(5) Manages and coordinates the Mainframe Application ISSO program, in cooperation with CIO/IA and DS; advises on all mainframe security relevant policies; coordinates intra- and inter-agency computer security issues; and supports certification and accreditation of mainframe resident applications or general support systems. Works with the PKI Program and IRM/OPS/ENM to facilitate and integrate PKI with the mainframe as a single sign-on methodology;

(6) Implements anti-virus policies, standards, and procedures to conform with established DOS architecture to ensure effective and efficient operations that protect critical automated information systems (AIS) against the threat of virus infection. Through these safeguards, computer and communications resources, including the data they store, are available and free of malicious code virus infection. The Information Integrity Branch manages a Virus Incident Response Team (VIRT) capable of responding to virus alerts Department-wide and provides 7X24 on-call assistance and an 8-hour, 5-day Help Desk in support of anti-virus software products. It maintains an anti-virus intranet Web site (accessible via the OpenNet) where the user community may obtain the latest versions of anti-virus software, virus signature files, virus alert information, and policy guidance 7X24. Also, develops policy that mandates reporting virus discoveries to this office;

(7) Administers and implements policies, standards, and procedures regarding Public Key Infrastructure (PKI), including digital signature and asymmetric public key encryption technology, to conform with Department regulations. Manages the Department's PKI program, including establishing and operating the PKI Root Certificate Authority (CA) and all subordinate certificate authorities on all Department classified and unclassified networks, domestic and overseas;

(8) Coordinates and manages the Department's cross-certification with the Federal PKI Steering Committee Federal Bridge Certification Authority (FBCA) for classified and unclassified automated information systems digital signature and public key encryption interfaces to other Federal agencies, state and local governments, foreign governments, and the public, domestic and overseas. Represents the IRM Bureau in all department-level and the

Department of State in all Federal-level forums, working groups, standing committees, and boards relative to using public key technology and infrastructure, and acts as the PKI technical advisor to all such groups within the Department. Coordinates IRM integration, verification, and interoperability testing for the Department; and

(9) Manages the Department's Biometric Logical Access program, including the integration with the Department and Federal PKI programs, for all Department classified and unclassified networks, domestic and overseas. Represents IRM Bureau in all department-level and the Department of State in all Federal-level forums, working groups, standing committees, and boards relative to using biometrics for logical access control, and acts as the technical advisor to all such groups within the Department.

1 FAM 275.2-4 Technical Security and Safeguards Division (IRM/OPS/ITI/TSS)

(CT:ORG-198; 10-15-2008)

The Technical Security and Standards Division (IRM/OPS/ITI/TSS):

(1) Advises the Director of Information Technology Infrastructure about all matters concerning hardware assurance and field surety program operations; and

(2) Administers policy, standards, and procedures regarding hardware assurance and field surety programs to conform with Department regulations.

1 FAM 275.2-4(A) Hardware Assurance Team (IRM/OPS/ITI/TSS/HAT)

(CT:ORG-198; 10-15-2008)

The Hardware Assurance Team (IRM/OPS/ITI/TSS/HAT):

(1) Implements policies, standards, and procedures regarding hardware assurance to conform with Department regulations;

(2) Investigates new hardware assurance technologies; and

(3) Performs assurance procedures on newly acquired equipment.

1 FAM 275.2-4(B) Field Surety Team (IRM/OPS/ITI/TSS/FST)

(CT:ORG-198; 10-15-2008)

The Field Surety Team (IRM/OPS/ITI/TSS/FST):

(1) Implements policies, standards, and procedures regarding field surety programs to conform with Department regulations;

(2) Performs technical counterintelligence processes for foreign posts; and

(3) Provides hardware safeguard services for foreign posts.

1 FAM 275.2-4(C) Systems Safeguards Team (IRM/OPS/ITI/TSS/SST)

(CT:ORG-198; 10-15-2008)

The Systems Safeguards Team (IRM/OPS/ITI/TSS/SST):

(1) Implements policies, standards, and procedures regarding hardware issues to deploy and use analog and digital non-secure telephone systems to conform with national and Departmental regulations;

(2) Implements policies, standards, and procedures regarding the hardware integrity of cryptographic systems and their peripherals; and

(3) Performs assurance procedures, certification, and/or validation of the Department's systems.

1 FAM 275.3 Messaging Systems Office (IRM/OPS/MSO)

(CT:ORG-198; 10-15-2008)

The Messaging Systems Office (IRM/OPS/MSO):

(1) Advises the Deputy Chief Information Officer for Information Resources Management Operations and other high-level officials about messaging;

(2) Has full responsibility for developing, implementing, and operating all Department-wide messaging;

(3) Manages the integration of emerging technologies with existing and planned messaging programs;

(4) Ensures messaging services are accessible to all offices of the Department and to other agencies; and

(5) Provides technical experts for the U.S.-Russian Federation and Newly Independent States direct communications link (DCL), the Nuclear Risk Reduction Center (NRRC), the government-to-government communications link (GGCL), the foreign affairs link (FAL), and other such initiatives.

1 FAM 275.3-1 Management Analysis Staff (IRM/OPS/MSO/MAS)

(CT:ORG-198; 10-15-2008)

The Management Analysis Staff (IRM/OPS/MSO/MAS):

(1) Advises the director regarding all resource issues affecting the managing and administrating of the messaging systems office; coordinates resource requirements among all program elements within an office; and prepares and recommends resource proposals to be submitted to IRM/EX;

(2) Manages the messaging systems office professional development program, ensuring that its employees are appropriately trained for their responsibilities;

(3) Manages, coordinates, and performs building and environmental maintenance in conjunction with IRM/EX and A/OPR offices.

(3) Acts as the messaging systems office’s contracting officer representative for its mission-critical contracts;

(5) Coordinates program resources and is liaison to IRM/EX for all office administrative and management issues such as budget, planning, staffing, training, equipment, space, desktop systems, inventory, procurement, etc;

(6) Prepares and monitors office performance measures and tracks the accomplishment of goals and objectives; keeps the office director informed of progress toward achieving the program’s mission; and

(7) Manages the communications security (COMSEC) account for the Communications Center and Secure Voice Center (i.e., COMSEC),

cryptographic Clearance (Access) procedures, and associated services according to 5 FAH-6, Communications Security Handbook. Manages the STU III/STE's program for distribution, operations, and control for the IRM Bureau.

1 FAM 275.3-2 Messaging Systems Products Division (IRM/OPS/MSO/MSP)

(CT:ORG-198; 10-15-2008)

The Messaging Systems Products Division (IRM/OPS/MSO/MSP):

(1) Oversees the Department's new messaging programs and identifies enhancements for existing systems, providing project management and quality assurance expertise;

(2) Explores new messaging technologies of potential value to the Department, in conjunction with IRM/BPC/EAP, and departmental foreign affairs messaging consolidation initiatives;

(3) Formulates, coordinates, and recommends messaging policies concerning new messaging technologies for Internet initiatives and their applications to existing and planned systems, in coordination with the other IRM Bureau directorates; and

(4) Provides central management and operational support for electronic mail and the combined bureau processing centers (CBPCs) core messaging applications.

1 FAM 275.3-2(A) Design and Build Branch (IRM/OPS/MSO/MSP/DB)

(CT:ORG-198; 10-15-2008)

The Design and Build Branch (IRM/OPS/MSO/MSP/DB):

(1) Participates in the finalization of messaging system requirements;

(2) Develops, presents design concepts, and participates in the selection process;

(3) Builds prototype systems for the customer and provides security and operational reviews; and

(4) Finalizes prototype and builds beta systems.

1 FAM 275.3-2(B) Operational Program Branch (IRM/OPS/MSO/MSP/OP)

(CT:ORG-198; 10-15-2008)

The Operational Program Branch (IRM/OPS/MSO/MSP/OP):

(1) Manages and directs programs supporting worldwide classified and unclassified messaging systems, as appropriate;

(2) Provides expert guidance for formulating tactical plans, policy, goals, and objectives for messaging systems;

(3) Plans, implements, budgets, contracts, procures, and arranges training for full-systems deployment following operational acceptance of new messaging systems;

(4) Provides application support, including guidance, troubleshooting and program resolution, concerning matters pertaining to support messaging systems, in cooperation with the Customer Service Center (IRM/BPC/CST); and,

(5) Evaluates program operations and develops proposals for deactivation or modernization of messaging systems.

1 FAM 275.3-2(C) Product Assurance Branch (IRM/OPS/MSO/MSP/PA)

(CT:ORG-198; 10-15-2008)

The Product Assurance Branch (IRM/OPS/MSO/MSP/PA):

(1) Develops configuration methods, procedures, and standards to support the development and implementation of messaging systems products;

(2) Ensures quality and consistency of software and documentation;

(3) Conducts internal configuration control board meetings, document reviews, and platform audits to define product content, predict user comprehension, and ensure delivery of product;

(4) Ensures compliance with established validation and verification procedures; and

(5) Manages the SA-34 computer network in support of development,

test, and operation activities. Responsibilities include providing user support and conducting software and hardware inventory.

1 FAM 275.3-2(D) Project Management Branch (IRM/OPS/MSO/MSP/PM)

(CT:ORG-198; 10-15-2008)

The Project Management Branch (IRM/OPS/MSO/MSP/PM):

(1) Is the responsible authority for defining and coordinating life-cycle activities for Department-wide messaging projects, from validation of user requirements through operational and customer acceptance; and

(2) Organizes, plans, and aligns measurable project objectives in accordance with established project management methodologies.

1 FAM 275.3-2(E) Test and Deploy Branch (IRM/OPS/MSO/MSP/TD)

(CT:ORG-198; 10-15-2008)

The Test and Deploy Branch (IRM/OPS/MSO/MSP/TD):

(1) Is responsible for testing, accepting, and deploying messaging projects and system enhancements;

(2) Prepares messaging systems for installation at beta sites, including the installation, operational training, and final system validation; and

(3) Performs user product acceptance review and reports on product readiness for production deployment.

1 FAM 275.3-3 Special Messaging Operations Division (IRM/OPS/MSO/SMO)

(CT:ORG-198; 10-15-2008)

The Special Messaging Operations Division (IRM/OPS/MSO/SMO):

(1) Manages and oversees the operations of the Intelligence and Special Communications (ISC) Center Branch and the Nuclear Risk Reduction Center (NRRC) Branch. This includes:

(a) Maintaining program management responsibilities and technical/operational liaison with the Department's Executive Secretariat Operations Center (S/ES-O), Bureau of Intelligence and Research (INR), White House Communications Agency (WHCA), Central Intelligence Agency (CIA), National Security Agency (NSA), Defense Information System Agency (DISA), Department of Defense (DOD) and other DOS bureaus and offices to coordinate operation, maintenance and installation of voice, data and emergency messaging systems;

(b) Maintaining special, direct communications channels between the Department and foreign governments via secure voice programs (Foreign Affairs Links – FAL), and data links (Government-to-Government Communications Links (GGCL), between the Nuclear Risk Reduction Center and foreign governments;

(c) Providing direct support to the Department of State's Chief Information Officer (CIO) including negotiating interagency agreements, memoranda of understandings (MOUs), bilateral agreements and protocols.

(2) Provides daily operational and technical support to the Executive Secretariat's Operations Center (S/ES-O) for specialized communications and requirements. This includes:

(a) In the arena of the ISC, directly supporting the Secretary of State (the Secretary) and other Department principals with secure voice and video requirements both domestically and overseas;

(b) Being responsible for the operation of the Department's interface to the Defense Red Switch Network; and operation of the Ultra High Frequency (UHF) and satellite communications used to support the Secretary while traveling;

(c) Providing Tier 1 service, defined as daily operational and technical support, to the Staff Secretariat's Operations Center (S/S-O) for specialized communications and requirements.

(3) Manages the operation of the NRRC communications facility and related bilateral GGCL. This includes providing coordination with foreign governments regarding maintenance and upgrades to equipment and telecommunications links, and maintaining currency

of and updates to required international agreements.

(4) Provides technical counsel to the Department's head of delegation, the Chief Information Officer (CIO) for U.S. – Russian technical expert. Negotiates international agreements or treaties with foreign governments in support of the NRRC, Foreign Affairs Link (FAL), Direct Communications Link (DCL), Direct Voice Link (DVL), and Direct Telephone Link (DTL). Provides program management and negotiates with host country regarding the Department's FAL and NRRC programs, including drafting/reviewing talking points and bilateral protocols.

1 FAM 275.3-3(A) Intelligence and Special Communications Center Branch (IRM/OPS/MSO/SMO/ISC)

(CT:ORG-198; 10-15-2008)

The Intelligence and Special Communications Center Branch (INR/OPS/MSO/SMO/ISC):

(1) Manages and operates the ISC, a 24x7 operation. This includes providing secure voice and data communications support to the Secretary and other principal officers;

(2) Serves as the Department's liaison and interface with the special intelligence community for data, voice, and message traffic. This includes;

(a) Providing operations and maintenance support for sensitive compartmented information (SCI);

(b) Being responsible for receiving and transmitting Critical Communication (CRITIC-COM) and SCI sensitive record traffic.

(3) Through the Secure Voice Center (SVC), provides the Secretary and other Department principals with accurate, reliable, and secure communications' support when traveling worldwide. This includes installing, operating, and troubleshooting an array of secure data, video, voice, and facsimile communications terminal equipment and transmission links for the Secretary and the traveling party between site locations and the Department;

(4) Operates and maintains a secure video conference facility for all Department principals;

(5) Manages the CRITIC Network operations for the Department, which is the sole access and exit point for the Department's CRITIC traffic;

(6) Performs other critical-sensitive classified communications activities.

1 FAM 275.3-3(B) NRRC Messaging Center Branch (IRM/OPS/MSO/SMO/NRRC)

(CT:ORG-198; 10-15-2008)

The NRRC Messaging Center Branch (IRM/OPS/MSO/SMO/NRRC):

(1) Manages and operates the NRRC, a 24x7 operation;

(2) Maintains liaison and conducts communications facility and related bilateral technical negotiations with foreign counterparts to maintain GGCL and continuous communications links (CCL);

(3) Serves as technical expert representative for the NRRC Communications on various inter-agency working groups (IWG), the Configuration Control Board (CCB), Engineering Working group (EWG) and the Standing Subcommittee on Upgrade (SSU);

(4) Performs other critical-sensitive classified communications activities.

1 FAM 275.3-4 e-Mail Division (IRM/OPS/MSO/EML)

(CT:ORG-209; 03-24-2009)

The E-Mail Division (IRM/OPS/MSO/EML):

(1) Provides program management and direction for classified and unclassified electronic messaging (e-mail) processing systems, internet, *OpenNet,* Network Control Center (NCC), and Combined Bureau Processing Center (CBPC) operations;

(2) Serves as *a senior Department representative* at inter-agency working group meetings on e-mail, firewalls, electronic directories, and associated technologies;

(3) Coordinates, reviews, and monitors the operational life cycle of e-mail, Internet, SIPRNET, *Open Source Information System* (OSIS),

OpenNet, NCC, and CBPC activities and recommends enhancements;

(4) Provides information systems security support for the Department's global classified, unclassified, and SBU e-mail systems and networks;

(5) Provides management oversight and direction to on-site Microsoft Corporation support to the Department; *and*

(6) *Serves as the day-to-day manager of the worldwide Department mobile computing programs that support the Foreign Affairs community remote access requirements. Mobile computing is defined as any program that includes technologies or applications designed to provide classified or unclassified access to Department networks by devices that are not continuously connected to one of the networks.*

1 FAM 275.3-4 (A) Network Control Center Branch (IRM/OPS/MSO/EML/NCC)

(CT:ORG-209; 03-24-2009)

The Network Control Center Branch (IRM/OPS/MSO/EML/NCC):

(1) Manages and operates the Department's *24x7* Sensitive But Unclassified (SBU) and unclassified enterprise e-mail network central infrastructures, a worldwide interconnection of local LAN-based systems that connect the Department to all U.S. embassies, consulates, and missions abroad;

(2) Manages and operates the Department's *24x7* unclassified internet support services;

(3) Manages and operates the Department's *24x7* Sensitive But Unclassified (SBU) remote access system platforms and firewall systems platforms; and

(4) Manages and operates information systems security infrastructure, including *Data Encryption Standard* (DES) and Type 1 encryption devices.

1 FAM 275.3-4(B) Combined Bureau Processing Center Branch (IRM/OPS/MSO/EML/CBPC)

(CT:ORG-209; 03-24-2009)

Combined Bureau Processing Center Branch (IRM/OPS/MSO/EML/CBPC):

(1) *Manages and operates the Department's 24x7 Secret classified enterprise e-mail network central infrastructure, connecting the Department to all U.S. embassies, consulates, and missions abroad;*

(2) Manages and operates the central infrastructure for the Department's *24x7* domestic Secret classified CABLEXPRESS telegraphic distribution systems;

(3) Manages and operates information systems security infrastructure for classified e-mail and telegraphic delivery systems with Type 1 encryption devices; and

(4) Manages and operates the Department's 24x7 Secret classified firewall systems platforms.

1 FAM 275.3-4(C) Mobile Computing Branch (IRM/OPS/MSO/EML/MC)

(CT:ORG-209; 03-24-2009)

The Mobile Computing Branch (IRM/OPS/MSO/EML/MC):

(1) Manages and operates worldwide Department mobile computing programs that support Foreign Affairs community remote access requirements;

(2) Provides technical network, operational, and administrative support to the Department of State and numerous Federal Agencies for OpenNet Everywhere (ONE), Blackberry, Secure Dial-In (SDI), and other mobile computing programs; and

(3) Serves as the Department of State's primary mobile computing site responding to a wide array of customer queries via the IT Service Center's Universal Trouble Ticket (UTT) system and direct contact.

1 FAM 275.3-5 Main State Messaging Center Division (IRM/OPS/MSO/MSMC)

(CT:ORG-198; 10-15-2008)

The Main State Messaging Center Division (IRM/OPS/MSO/MSMC):

(1) Manages and operates the Main State messaging center (MSMC) and the remote messaging center in State Annex 44. Maintains technical and operational liaison with the Department's Executive Secretariat's Operations Center (S/ES-O), INR, and other bureaus, offices, and agencies to coordinate ongoing and emergency messaging;

(2) Responsible for 7x24-hour telegraphic processing, message analysis and distribution, traffic research, and network management for Department enterprise messaging systems;

(3) Serves as the primary technical and operational liaison between IRM and the White House Communications agency, the Executive Secretariat's Operations Center (S/ES-O), the Bureau of Diplomatic Security (DS), and other government entities for routine emergency messaging and telecommunications operational support; and

(4) Provides operational life-cycle management for the Department's Main State messaging center and satellite bureau message centers, supporting core-messaging applications in accordance with prevailing Federal statutes, regulations, and applicable legislation.

1 FAM 275.3-5(A) Messaging Center Office Branch (IRM/OPS/MSO/MSMC/MCO

(CT:ORG-198; 10-15-2008)

The Messaging Center Office Branch (IRM/OPS/MSO/MSMC/MCO):

(1) Maintains 7x24-hour messaging liaison with bureaus, S/ES-O, posts, and other Federal agencies;

(2) Performs high-level coordination of critical-sensitive telegraphic support functions with the Executive Secretariat (S/ES) Staff, White House, Pentagon, and other offices, bureaus, and Federal agencies;

(3) Provides telecommunications guidance to MSMC shift chiefs and communications personnel at posts;

(4) Serves on telecommunication procedural, development, and operations planning groups within the IRM Bureau; and

(5) Manages the worldwide telegraphic collective address and CRITIC test programs.

1 FAM 275.3-5(B) Communications Systems Branch (IRM/OPS/MSO/MSMC/CSB)

(CT:ORG-198; 10-15-2008)

The Communications Systems Branch (IRM/OPS/MSO/MSMC/CSB):

(1) Operates mainframe and ancillary message-processing systems, 7x24 hours;

(2) Performs telecommunications technical and network control, trouble analysis, and circuit management functions; and

(3) Performs trouble analysis and circuit management functions to maintain cryptographic operations.

1 FAM 275.3-5(C) Communications Information Systems Branch (IRM/OPS/MSO/MSMC/CIB)

(CT:ORG-198; 10-15-2008)

The Communications Information Systems Branch (IRM/OPS/MSO/MSMC/CIB):

(1) Performs message handling, processing and analysis, and distribution functions, 7x24 hours;

(2) Operates the MSMC Help Desk;

(3) Manages the Department of State publications (DOSPUB) telegraphic routing indicator program; and

(4) Operates ATS-III terminal and peripheral equipment to retrieve, correct, re-enter, and research telegraphic messages and continuity journals.

1 FAM 275.3-5(D) Programming Branch (IRM/OPS/MSO/MSMC/PRG)

(CT:ORG-198; 10-15-2008)

The Programming Branch (IRM/OPS/MSO/MSMC/PRG):

(1) Performs automated terminal system (ATS), State terminal automated relay system (STARS), and PC hardware and software maintenance for Main State and Beltsville, Maryland 7x24 hours;

(2) Oversees, manages, and performs the contracting officer's representative function for the contract that provides programming and system maintenance for IRM/OPS/MSO/MSMC and some of IRM/OPS/MSO/BMC system computers and peripheral equipment;

(3) Performs LAN administration and hardware/software configuration management for PC and mainframe telegraphic processing systems; and

(4) Serves on the system development, technical, and operations planning group within the IRM Bureau.

1 FAM 275.3-6 Beltsville Messaging Center Division (IRM/OPS/MSO/BMC)

(CT:ORG-198; 10-15-2008)

The Beltsville Messaging Center Division (IRM/OPS/MSO/BMC):

(1) Manages and operates the Beltsville Messaging Center and the alternate Nuclear Risk Reduction Center (NRRC) messaging system. Maintains technical and operational liaison with the Department's Executive Secretariat's Operations Center (S/ES-O), White House Communications Agency (WHCA), Diplomatic Telecommunications Service Programs Office (DTS-PO), CIA, NSA, and other agencies, bureaus, and offices to coordinate ongoing and emergency messaging 7x24 hours;

(2) Provides program oversight for the Department's messaging systems, worldwide;

(3) Manages the Department's primary global telecommunications network center and regional messaging relay facility;

(4) Serves as designated alternate site facility for emergency messaging operations and the State Archiving System (SAS);

(5) Provides management oversight of the entire State Annex 26 facility to include building operations and maintenance support for the tenant organizations;

(6) In accordance with policies and procedures established by A/OEM/PPD and the Domestic Emergency Action Committee, is solely responsible for all emergency operations and relocation facilities within the complex. Responsible for classified operations and support and memoranda of understanding (MOUs) related to the forwarded activities; and

(7) Provides management oversight for the Department's Alternate Communications Site (ACS), supporting backup worldwide networking capability for SBU, classified, and command and control communications.

1 FAM 275.3-6(A) Communications Operations Branch (IRM/OPS/MSO/BMC/OPS)

(CT:ORG-198; 10-15-2008)

The Communications Operations Branch (IRM/OPS/MSO/BMC/OPS):

(1) Manages and operates the State telegraphic automated relay system (STARS) red message switching computers and ancillary systems;

(2) Performs telecommunications network management of the domestic communications links that support the diplomatic telecommunications service (DTS) network;

(3) Serves as the Department's on-site facilitator for inter-agency and inter-office network service requests;

(4) Plans, develops, and implements the telecommunications operational methods and procedures used by the Department of State and other U.S. Government agencies;

(5) Directs and coordinates the development of system and data circuit requirements between the Department and other U.S. Government agencies. Maintains liaison with officials of other U.S. Government agencies concerning common telecommunications programs; and

(6) Manages and operates the Department's alternate command and control system located in the ACS in time of an emergency.

1 FAM 275.3-6(B) Technical Services Branch (IRM/OPS/MSO/BMC/TS)

(CT:ORG-198; 10-15-2008)

The Technical Services Branch (IRM/OPS/MSO/BMC/TS):

(1) Provides primary technical control and maintenance support for BMC Primary Operations and the ACS, including circuit, multiplexer and cryptographic analysis and troubleshooting;

(2) Provides engineering, installation, troubleshooting and analyses for all circuits that terminate at the Alternate Communications Site (ACS);

(3) Liaises with IRM/ENM/GTS on circuit troubleshooting and installations for all overseas and domestic circuits that terminate into the State telegraphic automated relay system (STARS);

(4) Provides COMSEC control for the BMC and ACS COMSEC accounts;

(5) Manages the OpenNet Plus and ClassNet LAN's at BMC for State Department and other agency users;

(6) Manages systems security and Information Assurance for local area networks (LANs) at BMC and the Decision Agent domain at the ACS;

(7) Manages the ACS providing operations support, coordinating testing with posts and monitoring the Decision Agent domain and related systems. Provides support for all other customers who have systems located at the ACS;

(8) Provides site security support for managing and controlling physical access to the Beltsville and Olney locations to include:

(a) Usage;

(b) Handling;

(c) Disposition;

(d) Control of classified equipment and materials; and

(9) Provides guidance and assistance for the security programs and coordinates with tenant organizations' Unit Security Officers, Facilities Management Services, Diplomatic Security and other government security agencies to ensure physical security, communications, personnel, information systems and TEMPEST security is maintained at national standard levels.

1 FAM 275.4 Program Management And Analysis Office (IRM/OPS/PMA)

(CT:ORG-198; 10-15-2008)

The Program Management and Analysis Office (IRM/OPS/PMA):

(1) Manages the Department's information technology-approved programs by utilizing industry-standard project management methodologies. A core staff, trained in program management practices, effectively executes and implements information technology (IT) programs globally, domestically and abroad;

(2) Manages either an entire program's life cycle or specific program life-cycle segments. When managing the entire program life-cycle process, PMA conducts a complete program management review and acquisition strategy review and executes the actual program operations that include survey, design, building, delivery, installation, and transition to operations, maintenance, and customer service;

(3) When managing only specific segments of a program's life cycle, PMA coordinates and interfaces with multiple Department organizational elements to ensure that the program management methodologies are applied effectively;

(4) Establishes or ensures that industry-standard program management methodologies are being effectively executed for all IRM information technology programs conducted outside the PMA office. Provides guidance and direction to all other IRM elements for adhering to the concepts of program management, project scope planning, project time activities, financial accounting, project quality assurance and tracking, production control planning, project resource requirements determination, project risk management, configuration management requirements, and procurement strategies;

(5) Provides management oversight; directs and implements major IRM

information technology programs and projects (domestically and abroad), and advises the Deputy CIO for Operations, as required;

(6) Ensures PMA-managed programs comply with Federal legislation-guiding agencies such as the Federal Enterprise Architecture Framework (FEAF), the e-Government Act of 2001, the Federal Information Security Management Act (FISMA), NSA guidance, OMB A-130, and NIACAP, as well as other legislation directing Federal IT programs;

(7) Establishes a technical operations function for baseline configuration, site-specific requirements, and systems design and provides technical coordination with all customers;

(8) Establishes a deployment function to coordinate installation schedules, logistical deployment of material and personnel to customer sites, site preparation, install team preparation, and customer training;

(9) Establishes a production control function to effectively manage multidisciplinary processes, control gates, quality audits, internal reviews, and production goals to ensure a reliable and timely workflow so that the deployment schedule is met within cost constraints and technical and quality criteria;

(10) Establishes a quality-control function to define and execute system performance measures, contract performance, and configuration management and baselines and ensures that process documentation standards are developed during the program's life and adhered to; and

(11) Establishes a program management function to ensure that life-cycle phases of a program are documented and coordinated in the following areas: requirements definition, cost analysis, planning, financial management, reporting, automated management information system, and customer Web site development.

1 FAM 275.5 Systems and Integration Office (IRM/OPS/SIO)

(CT:ORG-209; 03-24-2009)

The Systems and Integration Office (IRM/OPS/SIO):

(1) In conjunction with other IRM offices, the SIO Office is responsible for:

(a) Providing enterprise technology-based solutions and services in the areas of managerial, compensation, post-specific administrative, websites, and web-based applications;

(b) Developing and implementing Department-wide systems integration and data management standards, policies, and procedures; and

(c) Managing and operating the Department's Enterprise Server Operations Centers (ESOCs).

(2) The office is comprised of one staff entity and four divisions.

1 FAM 275.5-1 System Assurance Team (IRM/OPS/SIO/SAT)

(CT:ORG-209; 03-24-2009)

The System Assurance Team (IRM/OPS/SIO/SAT):

(1) Provides and coordinates delivery of systems assurance services for SIO, including change and configuration management (e.g. patches and ITCCB submissions), quality assurance (e.g. ESOC monthly audits) and compliance (e.g. IMPACT, Privacy Act, Data Management, etc.) to achieve and maintain positive stakeholder relations while providing customer-oriented, cost-effective and secure services from computer systems, applications and programs;

(2) Coordinates the SIO disaster recovery and contingency planning program to reduce risk by developing effective plans and procedures to anticipate and guard against major system problems. (Previously located at 1 FAM 275.5-1(A)(4));

(3) Enforces security compliance by SIO, in accordance with Departmental security requirements, as guided by the Office of Information Assurance and the Bureau of Diplomatic Security. (Previously located at 1 FAM 275.5-1(A)(5));

(4) Coordinates technical and physical security programs to control access to sensitive information, computer hardware, and software; serves as communications security custodian (COMSEC);and

(5) Coordinates with SIO/BEC/PAB regarding activities related to budget, environmental systems, contract administration, acquisitions, customer support services, and project reporting. (Previously located at 1 FAM 275.5-1(A)(7)).

1 FAM 275.5-2 Business Engagement Center Division (IRM/OPS/SIO/BEC)

(CT:ORG-209; 03-24-2009)

The Business Engagement Center Division (IRM/OPS/SIO/BEC):

(a)The Business Engagement Center Division (IRM/OPS/SIO/BEC) provides customer support for existing SLAs, MOUs and ESOC services and also management of SIO budget, acquisition and procurement planning.

(b) The IRM/OPS/SIO/BEC is made up of three sections: Planning, Analysis and Budget (PAB); ESOC Customer Management (ECM); and Information Management Support (IMS).

1 FAM 275.5-2(A) Planning, Analysis and Budget (IRM/OPS/SIO/BEC/PAB)

(CT:ORG-209; 03-24-2009)

The Planning, Analysis and Budget Section (IRM/OPS/SIO/BEC/PAB):

(1) Coordinates SIO resources for all office administrative and management issues such as budget, planning, staffing, training, equipment, inventory, space, and procurement (previously 275.5-1(B) a);

(2) Develops acquisition plans for new computer systems, utilities, and services. Serves as Contracting Officer Representative (COR) for existing contracts for labor, service, and materials. CORs will coordinate with task managers at the branch or division level, as appropriate. (Previously located at 1 FAM 275.5-1(B)(2));

(3) Creates, implements, tracks and ensures the adherence to SIO's management plans and processes; and

(4) Coordinates with SAT regarding activities related to change management, quality assurance, configuration management, disaster recovery, contingency planning, security controls and compliance, and project reporting. (Previously located at 1 FAM 275.5-1(B)(d)).

1 FAM 275.5-2(B) ESOC Customer Management (IRM/OPS/SIO/BEC/ECM)

(CT:ORG-209; 03-24-2009)

The ESOC Customer Management Section (IRM/OPS/SIO/BEC/ECM) represents the interests of SIO, in general, and the ESOC in particular to other Department of State organizations. The ESOC:

(1) Manages relations with SIO customers who utilize ESOC resources;

(2) Conducts initial planning with customers regarding installations of their system into the ESOC;

(3) Negotiates Service Level Agreements (SLAs) with ESOC customers;

(4) Maintains open and positive communications with customers whose systems will be affected by ongoing ESOC activities such as outages, upgrades, moves, and expansion; and

(5) Monitors resolution of customer issues with responsible action teams within the ESOC.

1 FAM 275.5-2(C) Information Management Support (IRM/OPS/SIO/BEC/IMS)

(CT:ORG-209; 03-24-2009)

The Information Management Support Section (IRM/OPS/SIO/BEC/IMS):

(1) Promotes SIO services, products and applications through marketing, multi media, presentations, and demonstrations;

(2) Provides Tier-2 customer support and assistance for SIO applications and products to customers;

(3) Manages and directs negotiation, coordination, and monitoring of agreements between SIO and other Department bureaus, including SLAs and MOUs;

(4) Coordinates the preparation of all service-level agreements between SIO and its internal and external customers. Ensures agreements are consistent with Department information resource management policies, goals, and objectives; and

(5) Performs strategic planning for SIO management to identify life-

cycle management, control, and selection of pertinent information technology to meet SIO's customer's goals. This includes but is not limited to gathering user requirements and systems specifications.

1 FAM 275.5-3 Application Integration Division (IRM/OPS/SIO/API)

(CT:ORG-209; 03-24-2009)

The Application Integration Division (IRM/OPS/SIO/API):

(1) Provides policy direction regarding programs that integrate Department-wide applications. Such policies will be developed in coordination with the Chief Information Officer, the Customer Service Center (IRM/BPC/CST), and the Enterprise Architecture and Planning Office (IRM/BPC/EAP) to ensure conformance with established Department architecture standards and policies;

(2) Directs Department-wide integrated project;

(3) Directs the Department-wide data management program, including data administration and database management systems administration;

(4) Designs and administers centrally coordinated Department-wide data and system interfaces employing specialized enterprise applications integration (EAI) middleware software technology; and

(5) Coordinates within SIO regarding activities related to configuration management, change control, quality assurance, disaster recovery and contingency planning, security controls and compliance, overall financial management activities, environmental systems, contract administration, acquisitions, customer support services, and project reporting.

1 FAM 275.5-3(A) Integrated Projects Team (IRM/OPS/SIO/API/IP)

(CT:ORG-209; 03-24-2009)

The Integrated Projects Team (IRM/OPS/SIO/API/IP):

(1) Designs, implements and administers centrally coordinated Department-wide data and system interfaces employing specialized enterprise applications integration (EAI) middleware software technology;

(2) Develops and provides a set of Department of State enterprise level, Service Oriented Architecture (SOA) compliant standards used for systems/data integration, which include guidelines and training materials for using industry established integration processes and best practices. Adherence to this integration methodology and framework allows groups to seamlessly and cost-effectively share data between various applications and data repositories within the Department as well as with external organizations;

(3) Provides a fully supported (24x7) production integration infrastructure solution to serve as the Department's enterprise nervous system for sharing data and information seamlessly among disparate business processes;

(4) Provides a collaborative state-of-the-art integration facility where API, as well as the Department's IT enablers, can prototype, develop and test the integration of business processes, applications and data without affecting the production environment;

(5) Establishes and maintains project plans, including formulation of the overall project schedule, assessment of vulnerabilities and impacts, conversion cost estimates and guidance, and technical evaluations of project integration; and

(6) Establishes and maintains the IT Asset Baseline (ITAB), and provides management of its integration with other systems, in accordance with the Department's information architecture and security standards.

1 FAM 275.5-3(B) Data Management Team (IRM/OPS/SIO/API/DM)

(CT:ORG-209; 03-24-2009)

The Data Management Team (IRM/OPS/SIO/API/DM):

(1) Provides policy, program direction, and standards regarding Department-wide data; provides the guiding structure and standards for bureau data modeling and development efforts. *DM methodologies* conform to established Department architecture standards and policies;

(2) Identifies and maintains centralized descriptions of Department standard data elements. Assists bureaus in defining new, or capturing existing local data models to identify and remediate

inconsistencies with the enterprise data model;

(3) Assists bureaus in their collaborative efforts by providing data governance guidance. This support improves data quality, and facilitates data sharing between internal and external agencies;

(4) Collects, catalogues and consolidates current Department-wide enterprise data descriptions in a common automated Meta-Data Repository (MDR);

(5) Supports bureaus in acquiring database management systems and defining local databases consistent with enterprise data management standards;

(6) Maintains a central repository of vocabularies as an Enterprise Taxonomy. This repository is used Department-wide to support enhanced search functionality in various information systems such as search engines, websites and database applications;

(7) Maintains a single authoritative source of standard reference tables (SRT) to be used Department-wide. This improves the quality of code reference data in Department systems by eliminating inaccuracies. The SRT also facilitates data sharing and data reusability; and

(8) Develops and extends the Enterprise Extensible Markup Language (XML) Registry. This centrally managed repository provides a common location where all XML artifacts are captured, inventoried and stored. Items such as namespace, schemas, tags, elements, attributes and XML vocabularies are discovered Department-wide, and made available for reuse.

1 FAM 275.5-3(C) Enterprise Collaboration Services (IRM/OPS/SIO/API/ECS)

(CT:ORG-209; 03-24-2009)

The Enterprise Collaboration Services Team (IRM/OPS/SIO/API/ECS):

(1) Provides policy, program direction, and standards regarding Enterprise SharePoint services; provides the guiding structure and standards for bureau use of Department of State SharePoint Services. Policies and standards will conform to established Department website standards and policies;

(2) Provides SharePoint sites on Department SS environments in the

Department's major network;.

(3) Identifies and maintains guidelines for MOSS (Microsoft Office SharePoint Server 2007) implementation. Assists other Bureaus, Posts, and Offices which have approval to run a local MOSS environment with implementation documentation and best practices;

(4) Provides application development for MOSS web parts and custom requirements to meet the user requirements in the MOSS environment; and

(5) Provides Web and portal development services in response to customer requirements from throughout the Department and the foreign affairs community.

1 FAM 275.5-4 Applications Programming Division (IRM/OPS/SIO/APD)

(CT:ORG-209; 03-24-2009)

The Applications Programming Division (IRM/OPS/SIO/APD):

(1) Manages projects based on Departmental customer requests related to the development and enhancement of Department information management systems applicable to retirement, payroll, and other non-messaging initiatives;

(2) Provides desktop, client/server and web based applications development and support activity based on Departmental customer requests;

(3) Provides consultation services in various software engineering technological disciplines;

(4) Manages projects that cross all applications supported in the division. These include software modernization to bring information systems up to current release level of operating software, etc; and

(5) Coordinates within SIO regarding activities related to configuration management, change control, quality assurance, disaster recovery and contingency planning, budget, environmental systems, contract administration, acquisitions, SIO customer support services, and project reporting.

1 FAM 275.5-4(A) Applications Development Branch (IRM/OPS/SIO/APD/ADB)

(CT:ORG-209; 03-24-2009)

The Applications Development Branch (IRM/OPS/SIO/APD/ADB):

(1) Develops software for Department-wide use;

(2) Plans, develops, tests, deploys, and supports custom software solutions for the Department, and consults with functional bureau customers to assist them in defining technology solutions to meet their business needs and then developing and implementing their custom software solutions. APD/ADB will provide services to those bureaus that do not have the capability, required expertise or talent on staff to implement the required software solutions. However, SIO, in adherence to the E-Gov Program Board guidance, realizes that a number of bureaus maintain a staff dedicated to meeting their specialized software development needs. Those bureaus should continue to develop their custom software solutions in support of their mission;

(3) Plans, develops, tests, deploys, and supports Department-wide custom software solutions for legacy client server applications; and

(4) Plans, develops, tests, deploys, and supports the Department's custom web software applications for Department-wide use.

1 FAM 275.5-4(B) Compensation Applications Branch (IRM/OPS/SIO/APD/CAB)

(CT:ORG-209; 03-24-2009)

The Compensation Applications Branch (IRM/OPS/SIO/APD/CAB):

(1) Provides requirements analysis, design, development, maintenance, enhancement, and technical support for the payroll and retirement application mainframe information systems. Work priorities are defined by the customer for each application;

(2) Evaluates new technologies and software tools for use in enhancing existing or planned software engineering activities. This includes conducting feasibility studies to define alternative means of achieving this function. (Previously located at 1 FAM 275.5-3(B)(2));

(3) Provides consultation services in various mainframe systems technological disciplines; and

(4) Defines and manages projects that cross all applications supported in the branch. These include software modernization to bring information systems up to current release of operating software, etc.

1 FAM 275.5-4(C) PASS Applications Branch (IRM/OPS/SIO/APD/PASS)

(CT:ORG-209; 03-24-2009)

The PASS Applications Branch (IRM/OPS/SIO/APD/PASS):

(1) Provides requirements analyses, designs, development, maintenance, enhancement, and technical support for Post Administrative Software Suite (PASS);

(2) Evaluates new technologies and software tools for use in enhancing existing or planned software engineering activities that will impact the PASS software suite. This includes preparation of feasibility studies to define alternative means of achieving necessary functionality within the PASS software suite to meet the needs of DOS Posts overseas;

(3) Provides consultation services and coordination with numerous bureaus for various technological disciplines to ensure that the PASS software suite satisfies the field's software needs as they pertain to the administrative functions performed at the Department's posts overseas; and

(4) Defines and executes all PASS related projects that impact an overseas post's ability to accomplish their administrative tasks using the PASS software suite. These include software modernization to bring information systems up to current release level of operating software, etc.

1 FAM 275.5-4(D) Development LAN Support Team (IRM/OPS/SIO/APD/LAN)

(CT:ORG-209; 03-24-2009)

The DevLAN Support Team (IRM/OPS/SIO/APD/LAN):

(1) Provides the full range of support for the development and testing

networks to ensure that both the SIO/APD and SIO/API development teams have the necessary environment to carry out their development activities;

(2) Synchronizes changes/enhancements to the development and testing networks with the Department's operational networks to ensure that developed systems function properly when released to the operational networks;

(3) Provides advice to development teams on most efficient use of network capabilities; and

(4) In consultation with development staffs, implements new technologies and software tools for use in application development.

1 FAM 275.5-5 Enterprise Server Operations Centers Division (IRM/OPS/SIO/ESOC)

(CT:ORG-209; 03-24-2009)

The Enterprise Server Operations Centers Division (IRM/OPS/SIO/ESOC):

(1) Manages and operates the Department's Enterprise Server Operations Centers and is comprised of four Branches:

(a) Management Service Branch (ESOC/MSB) - provides overall project management and process improvement direction;

(b) Legacy Systems Support Branch (ESOC/LEG) - provides operational support for the mainframe legacy applications;

(c) Open Systems Operations Branch (ESOC/OPS) - provides operational support for the open systems servers used for the majority of Department's applications; and

(d) Technology Services Branch (ESOC/TSB) - provides the overall technical direction for the Department's Open Systems configuration.

(2) Provides the full range of activities related to the management of an enterprise operations center including configuration management, change control, quality assurance, disaster recovery and contingency planning, security controls and compliance, budget preparation and control, establishing environmental systems, contract administration, acquisitions, SIO customer support services, and project reporting; and

(3) Supports the Department's need for managed server services by providing 24x7 server monitoring, problem escalation, enterprise backup and restore, data mirroring, virtual infrastructure, SAN/NAS storage (data base or file/print), patch application, and compliance reporting.

1 FAM 275.5-5(A) Management Services Branch (IRM/OPS/SIO/ESOC/MSB)

(CT:ORG-209; 03-24-2009)

The Management Services Branch (IRM/OPS/SIO/ESOC/MSB):

(1) Provides overall project management direction for all ESOC projects;

(2) Provides direction for process improvement throughout the entire ESOC Division;

(3) Gathers requirements, designs and develops software to support the internal procedures of the ESOC Division; and

(4) Provides internal data collection and reporting to ensure that ESOC meets Service Level Agreements (SLA).

1 FAM 275.5-5(B) Legacy Systems Support Branch (IRM/OPS/SIO/ESOC/LEG)

(CT:ORG-209; 03-24-2009)

The Legacy Systems Support Branch (IRM/OPS/SIO/ESOC/LEG):

(1) Ensures that mainframe operations centers at ESOC sites are fully supported with appropriate and sufficient enterprise mainframe computer processors, and that environmental systems are monitored, controlled, and maintained on a normal operating schedule;

(2) Manages, maintains, and controls the SIO's mainframe backup solution at all ESOC sites;

(3) Manages and directs the activities required to generate, reproduce, store, control, and distribute computer-generated information;

(4) Analyzes and plans the most efficient workload for the mainframe computers, including developing job schedules, task assignments,

timetables, priorities, and modifying job schedules to meet urgent demands or changing requirements. (Previously located at 1 FAM 275.5-4(B)(4));

(5) Maintains and tracks any documents produced by the Department's enterprise mainframe computers and maintains accurate up-to-date records of deliveries, pickups, and authorized Department customer offices;

(6) Operates, maintains, and troubleshoots mainframe communications by recording events, detecting problems, and restoring services to communication equipment;

(7) Manages operating systems, utility software development, installation, and maintenance for the Department's mainframe computers; and

(8) Provides the requirement analyses, design, development, maintenance, and deployment of mainframe communications control programs in order to facilitate open exchange of information between the enterprise mainframe computers and the Department's customer systems, in conformance with established Department security architecture standards and policies.

1 FAM 275.5-5(C) Open Systems Operations Branch (IRM/OPS/SIO/ESOC/OPS)

(CT:ORG-209; 03-24-2009)

The Open Systems Operations Branch (IRM/OPS/SIO/ESOC/OPS):

(1) Ensures that the open-systems operations centers at ESOC sites are fully supported with appropriate and sufficient server capabilities and that all environmental systems are monitored, controlled, and maintained on a 24x7 basis;

(2) Ensures that all open systems are backed up in accordance with Department standards. Conducts periodic tests to verify that all backup and restore procedures are working as designed;

(3) Monitors all servers and the various connectivity points and interfaces to ensure systems are operating. When outages occur, escalates the problem to the appropriate system owner;

(4) Manages the configuration elements of all systems owned by SIO that are within the ESOC;

(5) Manages placement and inventory of all systems owned by bureaus that are placed within the ESOC;

(6) Analyzes and plans the most efficient workload for the various ESOC servers, including monitoring production systems to identify trouble spots or bottle necks before actual failures occur, and responding to urgent demands to make configuration modifications;

(7) Operates, maintains, and troubleshoots communications equipment by recording events, detecting problems, and restoring services to communication equipment;

(8) Manages operating systems, utility software, installation, and maintenance for the Department's ESOC-based servers; and

(9) Coordinates the facilities management activities for all ESOC server locations.

1 FAM 275.5-5(D) Technology Services Branch (IRM/OPS/SIO/ESOC/TSB)

(CT:ORG-209; 03-24-2009)

The Technology Services Branch (IRM/OPS/SIO/ESOC/TSB):

(*1) Provides the overall technical recommendations for the Open Systems direction, selects hardware/software/firmware products, evaluates virtual processing capabilities, and provides management with the blueprint for future enhancements;*

(2) Provides the technical guidance for selecting, evaluating, implementing and monitoring the standard operating systems used on all ESOC Open Systems;

(3) Identifies technical solutions for the Department's storage solutions, evaluates software, makes selections, oversees the implementation, and monitors the ongoing storage processes for accuracy and efficiency;

(4) Plans the most efficient server configuration, server virtualization strategies, and utilization of computer-room space, backup configuration, and continuity of operations plans; and

(5) Provides managed services support to ESOC customers including patch management, system upgrades, security compliance reporting, information assurance support, and product production

testing and rollout.

1 FAM 276 REGIONAL INFORMATION MANAGEMENT CENTERS (RIMC)

(CT:ORG-198; 10-15-2008)

IRM/OPS manages four regional information management centers (RIMC'S) worldwide. They perform the following duties:

(1) Provide technical and operational assistance on all information management programs to the posts within their geographic region;

(2) Formulate information management programs in the field, develop supporting budget and financial reports, and submit required administrative, technical, and analytical reports;

(3) Provide direction to the Information Management Technical Specialists (IMTS) under their supervision and monitor technical program performance;

(4) Examine and assess the effectiveness of ongoing communications and information systems programs and provide expertise necessary for enhancing area diplomatic missions' overall information management posture. Recommend improvements to achieve maximum efficiency and security on information management projects and programs;

(5) Conduct technical site surveys and develop plans for constructing or upgrading communications and data processing facilities. Assist other foreign affairs agencies with their communications requirements;

(6) Coordinate Diplomatic Telecommunication Service (DTS) operations and policies with the Area Telecommunications Office (ATO); and,

(7) IRM Regional Information Management Centers are located in:

(a) U.S. Embassy Bangkok, RIMC/EAP/SA with satellite offices in Beijing, Canberra, Manila, New Delhi, and Tokyo;

(b) U.S. Embassy Pretoria, RIMC/AF with satellite offices in Lome and Harare;

(c) Fort Lauderdale Regional Center, RIMC/WHA; and

(d) U.S. Consulate General Frankfurt, RIMC/EUR/NEA/AFW with a satellite office in Cairo.

1 FAM 277 THROUGH 279 UNASSIGNED

1 FAM EXHIBIT 271.3
BUREAU OF INFORMATION RESOURCE MANAGEMENT (IRM)

(CT:ORG-198; 10-15-2008)