5 FAM 120
INFORMATION MANAGEMENT STAFFING ABROAD

(TL:IM-41; 08-27-2003)
(Office of Origin: IRM/APR/RG)

5 FAM 121 INFORMATION MANAGEMENT ROLES AND RESPONSIBILITIES ABROAD

(TL:IM-41; 08-27-2003)

a. The purpose of these sections is to explain the roles and responsibilities of the personnel working in the Information Management (IM) sections abroad. Information Management (IM) is used in 5 FAM 120 to refer to the offices and personnel responsible for the management of information resources. Information Technology (IT) is used in 5 FAM 120 to refer to all programs and responsibilities for the management of information resources and includes non-technology responsibilities such as diplomatic pouch and mail operations and records management.

b. Information Systems Security Officer (ISSO) responsibilities will be designated at each post according to post capacities and circumstances. ISSO roles and responsibilities are outlined in 5 FAH-2 H-128.6, *Information Systems Security Officer (ISSO),* and 12 FAM 600, *Information Security Technology*.

5 FAM 121.1 INFORMATION MANAGEMENT OFFICER (IMO)

(TL:IM-41; 08-27-2003)

a. The IMO is the senior Information Management (IM) person at post. The IMO supervises IM services, operations, and the activities of post IM personnel. The IMO reports to the Management Officer.

b. IMO duties are not limited to the scope of these sections and are coordinated with post management. It is understood that the IMO at post has the ultimate responsibility for any decisions made by the IM section that may have been delegated down to the Information Programs Officer (IPO) or Information Systems Officer (ISO).

(1) Budget: The IMO creates a post-specific IT Budget Plan that

includes, but is not limited to, lifecycle replacement costs for all post-funded IT equipment and other assets (including monitoring the lifecycle of Information Resource Management (IRM)-funded IT equipment); current and future projects as identified in the post-specific IT Strategic Plan; and IT services offered under International Cooperative Administrative Support Services (ICASS);

(2) Contacts and Representation: The IMO serves as the initial point of contact with RIMC, the Geographic Bureau, the IRM Bureau, and other agencies for all IM matters.

(a) The IMO is the liaison to host nation authorities regarding telecommunications rights and services.

(b) The IMO represents IM in post's Counter-Intelligence Working Groups (CIWG); Emergency Action Committees (EAC); and the ICASS boards to promote use of IT assets, products, and services by these groups.

(c) The IMO serves as the chairperson on the local Change Control Board (CCB), which deals with post's IT hardware and software issues. The IMO also serves as the contact point for the IT CCB.

(d) The IMO serves as the Department of State representative at post for telecommunications services provided to client agencies.

(3) Human Resources:

(a) The IMO rates the IPO and ISO and reviews Employee Evaluation Reports (EER) for personnel in the IM section as appropriate. The IMO creates work requirements and conducts formal counseling for the rated employees.

(b) The IMO promotes and supports leadership and supervisory training for all IMSs, and leadership and management training for the IPO and ISO. The IMO must ensure post's Information Systems Security Officer(s) (ISSO), and alternates, attend ISSO training and refresher courses (see 12 FAM 622.1-1, *Information Systems Security Officer (ISSO) Designation*).

(c) The IMO creates and/or updates position descriptions for all IM staff, including locally engaged personnel, to include IPO and ISO capsule descriptions used in the bidding process.

(d) The IMO works with subordinates to develop an individual development plan (IDP) that ensures their training and development needs are met.

(4) Internet and Intranet: The IMO ensures proper security

configurations and service availability of Internet and intranet sites within the scope of the Department's guidelines provided by Diplomatic Security (DS) and IRM.

(5) Logistics and Infrastructure:

(a) Based on input from the IPO and ISO, or other IM staff when appropriate, the IMO finalizes lifecycle replacement costs and schedules in keeping with the Department's general replacement cycles. These schedules support funding requirements listed in the post IT Budget Plan and Mission Performance Plan (MPP) and serve to ensure all equipment are updated/replaced periodically.

(b) The IMO provides procurement guidance on IT equipment to other mission sections or agencies. This is especially true for equipment used in controlled access areas (CAA).

(6) Management:

(a) The IMO, as the senior IM officer, reports to the post's Management Officer. The IMO oversees all IT operations and IM personnel at post.

(b) The Embassy IMO, in coordination with Regional Information Management Center (RIMC), is the first point of contact for all constituent posts for IT issues and assistance. The IMO periodically visits each constituent post to assess its IT operations, equipment, and infrastructure.

(c) The IMO advises post management when staffing levels and workloads warrant requests for TDY assistance. Similarly, the IMO advises post management if staffing levels and workloads permit rendering TDY assistance to constituent posts when requested.

(d) For posts without an IPO and/or ISO, the IMO assumes the IPO/ISO responsibility. The IMO at such a post may delegate elements of those roles as appropriate to IMSs at post.

(7) Operations:

(a) The IMO is responsible for the effective, efficient, and secure IT operations at post.

(b) As the focal point for all telecommunications issues, the IMO oversees the planning of alternate routes and contingencies for all IT programs at post.

(c) The IMO is the post's Accountable Property Officer for IT equipment and assets. Working closely with the general services office (GSO), the IMO confirms the accuracy of the relevant inventories, including Consular Affairs (CA) IT assets; and, ensures all CAA equipment is ordered and

shipped in accordance with regulations.

(d) All IT projects, plans, and issues are reported to the IMO.

(8) Planning and Reporting:

(a) The IMO is responsible for the post's IT Contingency Plan and for ensuring that it is fully coordinated with the post's Emergency Action Plan (EAP). In addition, The IMO assists post with Site Contingency Plans.

(b) The IMO is responsible for the mission's IT Strategic Plan. This plan covers post's IT operational, technical, and staffing plans, for the next 3 to 5 years.

(c) The IMO participates in relevant portions of the post's reporting requirements, specifically updates the IRM Annex of post's Mission Performance Plan (MPP); updates Annex A, Communications, of post's Emergency Action Plan (EAP); and quarterly ICASS reports for IT services.

(9) Security:

(a) The IMO ensures that all personnel in the IM section are current on all security regulations, awareness, and guidelines as they pertain to IT operations, equipment, and infrastructure.

(b) The IMO serves as the post's alternate Top Secret Control Officer or delegates that responsibility.

(c) The IMO is the post's COMSEC Officer and, with the COMSEC custodian, maintains the integrity of all COMSEC assets at post.

(d) The IMO ensures proper safekeeping of classified materials and equipment in the IM section in accordance with Department security guidelines.

(e) The IMO works closely with the ISSOs, System Administrators, and RSOs implementing the Department's Automated Information Systems (AIS) security program on all classified and unclassified IT networks at the mission and/or at constituent posts (see 12 FAM 613, *Responsibilities*).

5 FAM 121.2 INFORMATION PROGRAM OFFICER (IPO)

(TL:IM-41; 08-27-2003)

a. The IPO manages the Information Programs Center (IPC) and is responsible for all IPC systems, programs, and telecommunications operations

b. The IPO supervises all personnel whose duties fall under the IPC. The IPO reports to the IMO.

c. IPO duties are not limited to the scope of these sections and are coordinated with the IMO.

(1) Budget: The IPO assists the IMO with the post's IT budget plan and MPP submission. The IPO provides the IMO with annual budget figures for lifecycle costs of all post-funded IPC equipment. The IPO provides the IMO and the local ICASS board with information on IPC's services on the ICASS service list.

(2) Contacts and Representation: The IPO serves as the initial point of contact with RIMC, the Geographic Bureau, IRM, and other agencies for technical matters falling within the IPC's responsibilities. The IPO maintains close contact with IT vendors for equipment and support. The IPO may serve on the local Change Control Board (CCB) dealing with IT hardware and software issues at post. As the head of IPC, the IPO must meet regularly with users to assess customer needs and satisfaction.

(3) Human Resources:

(a) The IPO rates or reviews IPC personnel, including Foreign Service Nationals (FSN) as appropriate. The IPO creates work requirements and conducts periodic formal counseling for these personnel as appropriate.

(b) The IPO promotes and supports leadership and supervisory training for all IPSs and IMSs under his/her supervision.

(c) The IPO updates the position descriptions of all IPC staff, including FSNs, to include IPS and IMS capsule descriptions used in the bidding process.

(d) The IPO works with subordinates to develop an individual development plan (IDP) to ensure their training and development needs are met.

(4) Internet and Intranet: The IPO ensures proper security configurations and service availability of internet and intranet sites within the scope of the Department's guidelines provided by DS and IRM.

(5) Logistics and Infrastructure:

(a) The IPO determines the lifecycle schedule for all post-funded IPC equipment and assets in accordance with Department guidance and replaces equipment according to this schedule.

(b) The IPO monitors the IPC equipment lifecycle replacement process to ensure projected equipment are delivered according to the established

lifecycle and in accordance with Diplomatic Security (DS) shipping requirements for Controlled Access Area (CAA) equipment.

(c) The IPO is responsible for keeping mailrooms furnished with the necessary expendable and non-expendable supplies in conjunction with GSO.

(d) The IPO ensures accurate inventory accounting and records for IPC assets.

(e) The IPO provides guidance to other agencies on the purchasing of IT equipment for CAAs.

(6) Management:

(a) The IPO manages all IPC operations, assets, and personnel. These operations and personnel may include the mailroom and its personnel; the telephone switchboard and the operators; receptionists; and FSN telephone and/or radio technicians.

(b) The IPO informs all IPC personnel, ISO, and IMO of immediate plans, tasks, responsibilities, and pending items to encourage effective two-way communication.

(c) The IPO must schedule periodic technical and operational support to constituent posts and support any emergency telecommunication needs. The IPO should coordinate with appropriate Department offices and other agencies to accomplish goals.

(7) Operations:

(a) The IPO oversees the IPC's data network operations, administration, and maintenance. They exercise control of telecommunications circuits and related equipment, providing guidance on alternate route testing and contingencies.

(b) The IPO provides oversight for the mission's telegraphic system and classified local area network in accordance with Department policies and guidance.

(c) The IPO coordinates, with the Regional Security Officer (RSO) and post management, testing and reporting of all post's short-range radio networks, excluding the E&E and EAC networks.

(d) The IPO must ensure the regularly scheduled HF radio tests and follow-up procedures are performed in accordance with their area Net Operating Instructions.

(e) The IPO ensures the telephone systems, including secure phones,

are operational at all times.

(f) The IPO confirms that COMSEC responsibilities are correctly discharged.

(g) The IPO is responsible for ensuring classified pouch materials are properly stored and handled.

(h) The IPO creates and maintains standard operating procedures (SOP) for all IPC operations and responsibilities.

(8) Planning and Reporting:

(a) The IPO provides input for post's IT Contingency Plan, Strategic Plan, and MPP.

(b) The IPO maintains a complete inventory of all post-procured software for IPC, including all applicable licensing documents.

(c) The IPO should ensure the IPC Emergency Destruction Plan (EDP) is current and coordinate quarterly EDP drills with the RSO and post management. The IPO, RSO, and post management must sign the memorandum documenting that the drills were performed.

(d) The IPO ensures that the weekly long-range High Frequency (HF) E&E radio test is performed and, if the post is the net control station (NCS), that the results are reported telegraphically. The IPO must also coordinate short-range radio network test results with the RSO and post management to ensure all the radios are operational and users are familiar with radio operations.

(e) The IPO brings to the attention of the IMO new programs and projects that will enhance customer relations and improve post operations.

(9) Security:

(a) The IPO ensures IPC security procedures are in place and followed.

(b) The IPO coordinates with the ISSO to ensure that adherence to Department-mandated security settings are implemented, documented, and available for OIG and DS inspections. In the event a mandate cannot be implemented, the IPO ensures that any requests for exceptions to policy are sent to the Chief Information Officer (CIO) who in turn would defer the waiver request to either DS or IRM/IA.

(c) The IPO develops and implements a policy for user access to and deletion from IPC systems. The ISSO, or his or her designee, must provide security awareness training before an appropriately cleared new user is given access to the system.

(d) The IPO ensures proper safekeeping of classified IPC materials and equipment in accordance with Department security guidelines.

5 FAM 121.3 INFORMATION SYSTEMS OFFICER (ISO)

(TL:IM-41; 08-27-2003)

a. The ISO manages the Information Systems Center (ISC) and is responsible for all unclassified data processing equipment and systems. See 5 FAM 800, *Information Systems Management,* 12 FAM 500, *Information Security,* and 600, *Information Security Technology* for more specific guidance and policies governing unclassified data processing and the ISC.

b. The ISO supervises all personnel whose duties fall under the ISC. The ISO reports to the IMO.

c. ISO duties are not limited to the scope of these sections and are coordinated with the IMO.

(1) Budget: The ISO assists the IMO with the post's IT budget plan and Mission Performance Plan (MPP) submission. The ISO provides the IMO with annual budget figures for lifecycle costs of all post-funded ISC equipment. The ISO provides the IMO and the local ICASS board with information on ISC's services on the ICASS service list.

(2) Contacts and Representation: The ISO, at the IMO's direction, serves as the post's initial point of contact with RIMC, the Geographic Bureaus, IRM, and other agencies for technical matters falling within ISC's responsibilities. The ISO maintains close contacts with local and stateside IT vendors for equipment and support. The ISO may serve on the local Change Control Board (CCB). As the head of ISC, the ISO meets regularly with users to assess customer needs and satisfaction.

(3) Human Resources:

(a) The ISO rates and reviews ISC personnel, including FSNs, as required. The ISO creates work requirements and conducts periodic formal counseling for these employees.

(b) The ISO supports leadership and management training for all IMS under his or her supervision.

(c) The ISO updates position descriptions for all ISC staff, including FSNs, to include IMS capsule descriptions used in the bidding process.

(d) The ISO works with subordinates to develop an individual

development plan (IDP) to ensure their training and development needs are met.

(4) Intranet and Internet responsibilities: The ISO ensures the proper security configurations and service availability of internet and intranet sites within the scope of the Department's guidelines provided by DS and IRM.

(5) Logistics and Infrastructure:

(a) The ISO determines the lifecycle schedule for all post-funded ISC equipment and assets in accordance with Department guidance and replace equipment according to this schedule.

(b) The ISO monitors the ISC equipment lifecycle replacement process to ensure projected equipment are delivered according to the established lifecycle and in accordance with Diplomatic Security (DS) shipping requirements for Controlled Access Area (CAA) equipment.

(c) The ISO ensures accurate inventory accounting and records for ISC assets. This includes an inventory of all other hardware and software installed on ISC assets.

(d) The ISO provides guidance to other agencies on the purchasing of IT equipment for the non-CAA spaces.

(6) Management:

(a) The ISO manages all ISC operations, assets, and personnel.

(b) The ISO informs all ISC personnel, IPO and IMO, of immediate plans, tasks, responsibilities, and pending items to encourage effective two-way communication.

(c) The ISO schedules periodic technical and operational support to constituent posts and supports any emergency telecommunication needs. The ISO coordinates with appropriate Department offices and other agencies to accomplish goals.

(7) Operations:

(a) The ISO exercises control of unclassified data network operations, administration, and maintenance, providing guidance on alternate route testing and contingencies.

(b) The ISO provides oversight for the mission's unclassified LANs in accordance with Department policies and guidance.

(c) The ISO creates and maintains standard operating procedures (SOP) for all ISC operations and tasks.

(8) Planning and Reporting

(a) The ISO provides input for post's IT Contingency Plan, Strategic Plan, and MPP.

(b) The ISO maintains a complete inventory of all post-procured software and hardware for the ISC, including all applicable licensing documents.

(c) The ISO ensures all reporting requirements for IT systems, as indicated in 5 FAM 800, *Information Systems Management,* are submitted.

(d) The ISO brings to the attention of the IMO new programs and projects that will enhance customer relations and improve post operations.

(9) Security:

(a) The ISO ensures ISC security procedures are in place and followed. The ISO is responsible for implementing the necessary security procedures in the ISC

(b) The ISO coordinates with the ISSO to ensure that adherence to Department-mandated security settings are implemented, documented, and available for OIG and DS inspections. In the event a mandate cannot be implemented, the ISO ensures that any requests for exceptions to policy are sent to the CIO who, in turn, would defer the waiver request to either DS or IRM/IA.

(c) The ISO develops and implements a policy for user access to and deletion from ISC systems. The ISSO, or his or her designee, must provide security awareness training before an appropriately cleared new user is given access to the system.

(d) The ISO coordinates with CA and ISSO to ensure security standards are maintained on CA systems.

(e) The ISO ensures proper safekeeping of classified ISC materials and equipment in accordance with Department security guidelines.

5 FAM 121.4 INFORMATION PROGRAMS SUPERVISOR (IPS)

(TL:IM-41; 08-27-2003)

a. The IPS position is instituted at larger posts where more than one shift and at least two IMS employees per shift adequately satisfy operational needs.

b. Traditionally, the IPS is responsible for the operational programs and activities of the IPC staff during a rotational shift. However, at posts where the IPC work hours provide for a staggered shift, the IPSs can, instead, supervise various disciplines or programs in the IPC, drawing a work force from the IMSs in IPC, as required. IPSs report to the IPO.

c. IPS duties are not limited to the scope of these sections and are coordinated with the IPO and IMO.

(1) Budget: The IPSs must be familiar with budget requirements in order to fill in during IPO's absence.

(2) Contacts:

(a) The IPSs meets periodically with users to assess customer needs and satisfaction and to inform them of upcoming IRM plans and projects.

(b) The IPSs maintains contact with local vendors for local support of IPC equipment and software.

(c) The IPSs assists the IPO in conducting periodic IPC staff meetings to disseminate information to all IMSs, ISOs, and IMOs.

(3) Human Resources:

(a) The IPSs may rate or provide input for the rating of IMSs and FSNs in the IPC. They create and conduct periodic formal counseling for these personnel as appropriate.

(b) The IPSs work with their subordinates to develop individual development plans (IDP) to ensure their training and development needs are met.

(c) The IPSs promote and support applicable training for all IPC personnel.

(4) Intranets: The IPSs ensure the proper security configurations and service availability of internet and intranet sites within the scope of the Department's guidelines provided by DS and IRM.

(5) Logistics and Infrastructure: The IPSs assist with the inventory and lifecycle requirements for the IPC. They also assist with tracking projected equipment and ensuring proper shipment in accordance with DS requirements for CAA equipment.

(6) Management:

(a) The IPSs maintain duty rosters and leave schedules, as applicable, and coordinate schedules with IPO.

(b) The IPSs provide daily management oversight of personnel and operations as applicable.

(c) The IPSs direct IMSs, as necessary, in tasks, including:

- Telecommunications circuits and equipment;
- Daily telegraphic traffic processing and maintenance of the TERP V and CableXpress systems;
- Administration and maintenance of ClassNet and its associated systems;
- Long and short-range radio tests in accordance with 5 FAM 540, *Voice Radio Systems,* and 5 FAH-2 H-700; *Internet and Intranet Use;*
- Proper cryptographic operations, procedures, and reporting;
- The use and testing of alternate routes and system contingencies;
- Diplomatic pouch operations;
- Property accounting, inventories, reconciliations, and reporting;
- Records management; and
- Housekeeping.

(7) Operations:

(a) The IPSs are responsible for the operation and maintenance of all classified telecommunications equipment and circuits.

(b) The IPSs provide oversight for the mission's classified LANs in accordance with Department policies and guidance.

(c) The IPSs are responsible for following SOPs.

(8) Planning and Reporting: The IPSs are responsible for reporting any issues or concerns to the IPO so that they may be addressed in accordance with the mission's established plans and schedules.

(9) Security:

(a) The IPSs ensure adherence to security policies and guidelines set out by the mission and the Department for the IPC.

(b) The IPSs ensure proper safekeeping of classified IPC materials and equipment in accordance with Department security guidelines.

5 FAM 121.5 INFORMATION MANAGEMENT SPECIALIST (IMS)

(TL:IM-41; 08-27-2003)

a. IMS refers to all IRM employees within the 2880 skill code. For this subsection IMS refers to those IRM personnel without supervisory responsibilities.

b. IMSs typically have no supervisory responsibilities unless otherwise directed, although some posts pass the managerial responsibility of an office of FSNs, e.g. the mailroom, to an IMS for managerial experience. IMSs report to the IPSs, if any, IPOs, or ISOs.

c. The following subsections explain IMS roles and responsibilities in generic terms but specific job duties are the discretion of the IPS, if any, IPO or ISO, and IMO. Their duties are not limited to the scope of these subsections and are coordinated with post's IM management.

(1) Budget: Not applicable.

(2) Contacts and Representation:

(a) IMSs serve as the first point of contact for users in the unclassified and classified sections of the post. IMSs may also meet with FSN staff to ensure problem-free operations.

(b) IMSs report any daily requirement to IM management.

(3) Human Resources:

(a) IMSs develop an individual development plan (IDP) to ensure training and development needs are met.

(b) IMSs who are assigned managerial responsibility of an FSN unit should be familiar with 3 FAH-2, *Foreign Service National Handbook*.

(4) Internet and Intranets: IMSs ensure the proper security configurations and service availability of internet and intranet sites within the scope of the Department's guidelines provided by DS and IRM.

(5) Logistics and Infrastructure:

(a) IMSs maintain adequate spares and supplies for equipment. Notify IM management of equipment shortages.

(b) IMSs provide inventory information to management when equipment is replaced.

(c) IMSs dispose of defective equipment in accordance with Department guidelines.

(d) IMSs assist with property accounting, inventories, reconciliations, and reporting.

(6) Management: Not applicable.

(7) Operations:

(a) IMSs process daily telegraphic traffic.

(b) In accordance with mission standard operating procedures, IMSs administer and maintain systems.

(c) IMSs test backup systems for usability and accessibility.

(d) IMSs maintain user accounts in accordance with the policies and procedures established by the IPO and ISO (5 FAM 121.2.c.(9)(c), *Information Program Officer,* and 121.3.c.(9)(c), *Information Systems Officer).*

(e) IMSs install and configure new IT equipment in accordance with mission and Department guidelines as directed or required.

(f) IMSs perform radio tests according to established standard operating procedures and 5 FAM 540, *Voice Radio Systems,* and 5 FAH-2 H-700, *Managing Radio Networks*.

(g) IMSs prepare and process classified pouch material as directed in accordance with standard operating procedures and 5 FAH-10, *Pouch and Mail Handbook.*

(h) IMSs provide assistance to users as required or requested.

(8) Reporting:

(a) IMSs record and report to IM management any anomalies with the system infrastructure.

(b) IMSs record and draft outage reports for IM management in accordance with the mission's escalation procedure.

(9) Security:

(a) IMSs configure and maintain all systems in accordance with Department security guidelines.

(b) IMSs ensure proper safekeeping of classified IT materials and

equipment in accordance with Department security guidelines.

(c) IMSs attend all mandated security training courses in accordance with Department guidance.

(d) IMSs attend ISSO training when appropriate to assume lead or alternate ISSO duties as required.

5 FAM 122 THROUGH 129 UNASSIGNED