5 FAM 100
INFORMATION TECHNOLOGY (IT) MANAGEMENT

5 FAM 110
IT MANAGEMENT

(CT:IM-94; 02-05-2008)
(Office of Origin: IRM/BPC/PRG)

5 FAM 111 GENERAL POLICY

(CT:IM-73; 05-02-2006)

a. Department officials identified in 5 FAM 115 have primary responsibilities for the development, oversight, and implementation of the Department's IT program and activities.

b. System managers must follow 5 FAM 800 for their specific responsibilities. IT project managers must follow requirements in 5 FAM 600, Web site managers 5 FAM 700.

5 FAM 112 SCOPE

(CT:IM-73; 05-02-2006)

All Department organizations must follow the guidance in this subchapter when establishing Bureau Performance Plans (BPPs) and Mission Performance Plans (MPPs) for information technology investments.

5 FAM 113 AUTHORITIES

(CT:IM-73; 05-02-2006)

The authorities for this policy include:

(1) Government Performance and Results Act of 1993, Public Law 103-62 (GPRA) (5 U.S.C. 306 and 31 U.S.C. 1115, et. seq.);

(2) Paperwork Reduction Act of 1995, Public Law 104-13 (44 U.S.C. 3501, et. seq.);

(3) Clinger-Cohen Act of 1996, Public Law 104-106 (formerly known as the Information Technology Reform Act of 1996, renamed by section 808, Public Law 104-208) (40 U.S.C. 1422, et. seq.);

(4) Federal Financial Management Improvement Act of 1996, Public Law 104-208, sections 802 and 803 (31 U.S.C. 3512 note);

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

(6) Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, Title III (44 U.S.C. 3541 et. seq.);

(7) Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, Public Law 99-399, as amended (22 U.S.C. 4802(a));

(8) E.O. 13011 (Federal Information Technology);

(9) OMB Memoranda (M-04-04), E-Authentication Guidelines for Federal Agencies;

(10) OMB Circular A-11, Preparation, Submission and Execution of the Budget (issued annually by OMB), including Part 7, Planning, Budgeting, Acquisition, and Management of Capital Assets and Capital Programming Guide, Version 1.0 Supplement to Part 7;

(11) OMB Circular A-123, Management’s Responsibility for Internal Control;

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

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

(14) Rehabilitation Act of 1973, Public Law 93-113, as amended, Section 508 (29 U.S.C. 794d);

(15) 36 CFR Part 1194, Electronic and Information Technology Accessibility Standards;

(16) Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003;

(17) Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004;

(18) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Guidelines for Identifying an Information System as a National Security System, August 2003; and

(19) Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, February 25, 2005.

5 FAM 114 DEFINITIONS

(CT:IM-73; 05-02-2006)

Electronic and Information Technology (EIT): Is defined in 5 FAM 913.

Enterprise Architecture (EA): Is defined in 5 FAM 674.

Firewall Rule Set: A set of rules or operating conditions encoded into the firewall device to allow and/or disallow TCP/IP traffic to and from the public network. Rule sets are based upon either senior management or IT management defined policy.

Information Life Cycle: Is defined in 5 FAM 913.

Information Resources: Is defined in 5 FAM 913.

Information System: Is defined in 5 FAM 913.

Information Technology (IT): Is defined in 5 FAM 913.

Personal Identity Verification (PIV) Card: A secure, electronic, rapid, and verifiable means of individual identification that is resistant to fraud, tampering, counterfeiting, and terrorist exploitation.

Public Key Infrastructure (PKI): A methodology for securing data transmission of Sensitive-But-Unclassified information across Department of State automated information system assets.

5 FAM 115 WHO HAS PRIMARY RESPONSIBILITY FOR IT MANAGEMENT?

(CT:IM-73; 05-02-2006)

The principal management officials and organizations that manage, advise, and support IT activities are:

Under Secretary for Management (M)

Chief Information Officer (CIO)

Deputy CIO for Business, Planning, and Customer Service/Chief Knowledge Officer (DCIO/BPC)

Chief, Enterprise Architecture and Planning Office (IRM/BPC/EAP)

Chief, Enterprise Architecture Division (IRM/BPC/EAP/EA)

Chief, Planning Division (IRM/BPC/EAP/PL)

Deputy CIO for Operations/Chief Technology Officer (DCIO/OPS)

Chief Information Security Officer (CISO)

E-Gov Program Board (E-GovPB)

E-Gov Advisory Group

E-Gov Program Management Office (E-Gov PMO)

E-Gov Working Group

Assistant Secretary, Diplomatic Security (DS)

Chief Financial Officer (CFO)

Information Technology Change Control Board (IT CCB)

Local CCBs

Department Program Managers

Other Department Organizations (See 5 FAM 115.8 for details.)

5 FAM 115.1 Under Secretary for Management (M)

(CT:IM-73; 05-02-2006)

The Under Secretary for Management (M) directs and administers the Department’s worldwide IT resources and chairs the E-GovPB. M has responsibility and authority over the IT budget.

5 FAM 115.2 Chief Information Officer (CIO)

(CT:IM-73; 05-02-2006)

The CIO (equivalent to an Assistant Secretary) heads the Bureau of Information Resource Management (IRM) and serves as the principal information technology adviser to the Secretary of State and M. The CIO ensures development; implementation; and as necessary, revision of IT policies, plans, and programs. The CIO (along with the CFO) is the Deputy co-chair of the E-GovPB. (See 1 FAM 271 for additional CIO duties and responsibilities.)

5 FAM 115.2-1 Deputy CIO for Business, Planning, and Customer Service/Chief Knowledge Officer (DCIO/BPC)

(CT:IM-73; 05-02-2006)

The DCIO/BPC provides assistance and advice in the execution of the CIO’s responsibilities. Additional duties include ensuring that the Department’s information resource management decisions reflect the needs of the Department’s business sponsors by anticipating changes in both technology and the business practices of the Department. Performing these duties validate that the Department’s information resource programs fully meet information, E-Government and knowledge management objectives. (See 1 FAM 274 for more information on this office.)

5 FAM 115.2-1(A) Enterprise Architecture and Planning Office (IRM/BPC/EAP)

(CT:IM-73; 05-02-2006)

EAP is the E-Gov PMO which supports the entire IT Capital Planning Process for the E-GovPB. EAP is directed by the CIO and DCIO/BPC. EAP helps to coordinate and ensure completion of all program elements related to the Department's E-Gov/IT projects. (See 1 FAM 274.2.)

5 FAM 115.2-1(B) Enterprise Architecture and Engineering Division (IRM/BPC/EAP/EA)

(CT:IM-73; 05-02-2006)

The Division is responsible for developing and maintaining the Department's enterprise architecture, under the direction and supervision of the CIO, DCIO/BPC, and Director, EAP. This Division provides the linkage between the various components of an organization which includes business functions, performance, services, technology, and information. It also provides support to other business elements, such as stakeholders, facilities, programs, investments, and security requirements. (See 1 FAM 274.2.)

5 FAM 115.2-1(C) Planning Division (IRM/BPC/EAP/PL)

(CT:IM-73; 05-02-2006)

The Planning Division implements the Department's strategic IT planning activities, the Department's Electronic Capital Planning and Investment Control (eCPIC) System program activities, and supports the E-GovPB. PL provides the primary interface with the Department's bureaus in the planning, oversight, and reporting functions for IT investments. (See 1 FAM 274.2.)

5 FAM 115.2-2 Deputy CIO for Operations/Chief Technology Officer (DCIO/OPS)

(CT:IM-73; 05-02-2006)

The DCIO/OPS assists and advises the CIO concerning technical operations. Additional duties include providing direction and policy guidance on operational activities in IRM to ensure that the Department and other foreign affairs agencies receive rapid, reliable, responsive, and secure, classified and unclassified voice and data information management operating systems, networks, and programs. (See 1 FAM 275.)

5 FAM 115.2-3 Chief Information Security Officer (CISO)

(CT:IM-73;   05-02-2006)

The CISO carries out the information security responsibilities of the CIO under the supervision of the CIO (see 44 U.S.C. 3544(a)(3)(A)). The CISO heads IRM's Office of Information Assurance (IRM/IA) ensuring agency compliance with the Federal Information Security Management Act (FISMA) (44 U.S.C. 3544), and other applicable laws. (See 1 FAM 272.)

5 FAM 115.3 Electronic Government Program Board (E-GovPB)

(CT:IM-73;   05-02-2006)

The E-GovPB is the principal IT advisory entity to the Under Secretary for Management (M), and functions as the Department's capital planning Executive Review Committee. It ensures systematic selection, control, and evaluation of the Department's E-Gov/IT programs and investments; approves the Department's IT Strategic Plan; and reviews and recommends IT funding priorities and budget requests. (See 1 FAM 274.2-2.)

5 FAM 115.3-1 E-Gov Advisory Group

(CT:IM-73;   05-02-2006)

The E-Gov Advisory Group provides a business, technical, and investment evaluation of IT initiatives before submission to the E-GovPB. The group also considers potential risk, cost, benefit, alignment with the Department's enterprise architecture, and priority of IT investments. The makeup of this group is below the Assistant Secretary level. It identifies and provides information on IT initiatives to those at Assistant Secretary level and above to ensure that they are adequately informed prior to E-GovPB review.

5 FAM 115.3-2 E-Gov Program Management Office (E-Gov PMO)

(CT:IM-73;   05-02-2006)

a. The E-Gov PMO ensures that

(1) all program elements related to Department IT investments are completed.

(2) investments meet E-Government guiding principles.

(3) major milestones are met throughout all stages of the CPIC process.

b. The E-Gov PMO has two operational elements: IRM/BPC/EAP/EA (5 FAM 115.2-1(B) and IRM/BPC/EAP/PL (5 FAM 115.2-1(C)).

5 FAM 115.3-3 E-GovPB Working Group

(CT:IM-73; 05-02-2006)

The E-GovPB Working Group is made up of technical subject matter experts and representatives from numerous bureaus. It supports, and works under the direction of, the E-Gov PMO in conducting detailed analysis and providing recommendations concerning specific IT investment portfolio issues.

5 FAM 115.4 Assistant Secretary, Bureau of Diplomatic Security (DS)

(CT:IM-73; 05-02-2006)

a. All IT activities and programs must have a secured environment for conducting U.S. diplomacy and promoting U.S. interests worldwide. To support this objective, DS helps ensure that a secure, comprehensive, technically current and cost effective IT security program is maintained according to FISMA, and other applicable laws and National Security Directives. (See Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, as amended (22 U.S.C. 4802(a)) and Delegation of Authority 214 of September 20, 1994, Section 8.)

b. DS provides

- Network Monitoring
- Cyber Incident Handling
- Cyber Threat Analysis
- Compliance Verification and Vulnerability Analysis
- Cyber Security Policy and Configuration Development
- Cyber Security Awareness and Training
- the Regional Computer Security Officer (RCSO) program.

c. DS is also responsible for the physical, technical, information, and personnel security programs that enable a secure IT environment, and administers the Cyber Security Incident Program. These actions help maintain a secured environment for conducting U.S. diplomacy and promoting U.S. interests worldwide. (See 12 FAM 615 for other DS-related IT responsibilities.)

5 FAM 115.5 Chief Financial Officer (CFO)

(CT:IM-73; 05-02-2006)

a. The CFO, along with the CIO, provides complete and accurate accounting of IT expenditures, related expenses, and results in accordance with the

Paperwork Reduction Act of 1995 (see 44 U.S.C. 3506(b)(3)(B)). The CFO implements systems and financial policies that control the Department's costs. The CFO (along with the CIO) is Deputy co-chair of the E-GovPB. (See Sections 802 and 803 of the Federal Financial Management Improvement Act of 1996 (FFMIA) (31 U.S.C. 3512 note).)

b. The CFO publishes Department policy for identifying specific financial thresholds and other criteria to determine when software must be capitalized.

c. The CFO also provides advice on current and prospective intelligence resources and critical infrastructure protection matters, including developing strategies and initiatives for the Department.

5 FAM 115.6 Change Control Boards

5 FAM 115.6-1 Department's Information Technology Change Control Board (IT CCB)

(CT:IM-73; 05-02-2006)

The IT CCB manages the Department's global IT environment that consists of classified and unclassified upgrades and addresses issues of configuration tracking, change control, and network planning and operations. It sets the standard for the Department's classified and unclassified technical baselines and monitors compliance with that standard.

5 FAM 115.6-2 Local Change Control Board (CCB)

(CT:IM-73; 05-02-2006)

a. Bureaus and posts must establish and maintain a local CCB. A local CCB reviews changes affecting systems or applications for which the bureaus or posts are responsible. The local CCB can be in the form of a committee or it can consist solely of IRM representative(s) at post. The local CCB determines whether a change request can be approved locally or should be submitted to the IT CCB.

b. The post security officer should supplement a CCB with only a sole IRM representative to avoid conflicts of interest problems.

c. Local CCBs must report local/post activity and approval of IT items to their IT CCB Voting Representatives and the IT CCB Change Manager.

5 FAM 115.7 Department Program Managers

(CT:IM-73; 05-02-2006)

Department program managers, in consultation with the CIO and CFO, as well as the CISO, E-Gov PMO, and DS, determine IT program information resource needs and develop strategies, systems, and capabilities to meet and comply with those needs. (See the Paperwork Reduction Act of 1995 (44 U.S.C. 3506(a)(4)).) These program managers must also comply with OMB guidance on IT activities, including E-Government initiatives, sound financial management practices, and performance measurement guidance, to assess their IT programs and activities.

5 FAM 115.8 What Other Department Organizations Support IT Management?

(CT:IM-73; 05-02-2006)

Other Department organizations are also involved in the management and oversight of IT activities and provide major additional advice and support. Those organizations are included in this subsection.

5 FAM 115.8-1 Firewall Advisory Board (FAB)

(CT:IM-73; 05-02-2006)

a. FAB reviews, approves, and tracks configuration changes to the Department-level firewalls. IRM/OPS/MSO/EML is the chair of the FAB. Other members include the Virus Incident Response Team (VIRT) and DS personnel.

b. The office responsible for the FAB is IRM DCIO for Operations, Messaging Systems Office, E-Mail Division (IRM/OPS/MSO/EML). The responsibilities of the board include the following:

(1) establishing baseline configurations for all Department-level firewall installations;

(2) establishing criteria to control connectivity of non-Department of State organizations to Department networks;

(3) receiving all requests for changes to the Firewall Rule Set, performing a risk assessment of each request, and authorizing appropriate changes to the rule set;

(4) recommending changes to the firewalls and network architecture to improve network security;

(5) providing assistance in developing firewall-related solutions to meet the operational requirements of new network applications; and

(6) reviewing the Firewall Rule Set annually.

5 FAM 115.8-2 Personal Identity Verification (PIV) Implementation Board

(CT:IM-73; 05-02-2006)

a. The PIV Implementation Board was established to implement the requirements of Homeland Security Presidential Directive (HSPD-12). The Board is co-chaired by the Deputy Assistant Secretary and Director of Countermeasures (DS/C) and the Deputy CIO for Operations (IRM/OPS). Other Department officials are Board members.

b. A PIV Working Group was also established and governed by the Board. The Group's purpose is to plan, coordinate, and ensure implementation of the Department's PIV Program in compliance with HSPD-12 and National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) 201. The Group also provides responses on behalf of the Department of State to reporting agencies.

c. HSPD-12 was issued to help standardize the form and level of security by which Federal employees and contractors are identified for access to Federal facilities and information systems. HSPD-12 establishes U.S. Government policy to

(1) enhance security against potential terrorist threats,

(2) reduce identity fraud,

(3) increase Government efficiency through standardization, and

(4) protect the personal privacy of individuals.

d. HSPD-12 mandates that the Department establish a program to ensure that identification issued to State employees and contractors meets FIPS 201.

e. The Department must also require the use of identification by State employees and contractors that meets FIPS 201 to gain physical and logical access to federally controlled facilities and information systems, respectively.

f. Federal Information Processing Standards (FIPS) 201 implements HSPD-12 by specifying the architecture and technical requirements for a common identification standard for Federal employees and contractors.

g. The PIV program is composed of systems and processes that support a common smart card-based identity authentication platform for accessing multiple types of physical and logical access environments. Smart cards will be the vehicle that carries the physical and digital components that form the user's PIV credentials. (See 5 FAM 115.8-3 below.)

5 FAM 115.8-3 Smart Card Public Key Infrastructure (PKI) Biometric Governance Board (SCPBGB)

(CT:IM-94; 02-05-2008)

a. SCPBGB, along with the PIV Implementation Board above, coordinates a centralized approach for PIV implementation through the smart card technology for physical access, logical access, PKI, and other Department applications.

b. The PIV Working Group and DS Security Technology, Facility Security Engineering Division, Domestic Management and Engineering (DS/ST/FSE/DME) have primary roles to manage the physical access to Department domestic facilities, including the use of appropriate technologies to accomplish that mission.

c. The Under Secretary for Management designated the PKI Program Team, created under IRM/OPS/ITI/SI, as the sole entity within the Department to implement public key infrastructure utilizing Smart Card technology.

d. The Board will operate in compliance with Department policies and procedures and under the auspices of the PIV Implementation Board by

(1) identifying smart card requirements, recommending policy and procedures, and developing standards that support the use of smart cards at the Department.

(2) providing clear, strong leadership during the development and implementation phases of the Smart Card Program.

(3) providing guidance and assistance in implementing smart card related applications; *and*

(4) providing oversight of the Department’s smart card activities, and establishing interoperability, technical, and security requirements for products related to the Department’s Smart Card Program.

e. The PIV Implementation Board and other authorities and regulations may result in additional specific responsibilities.

5 FAM 116 WHAT IS THE ROLE OF THE IT RESPONSE AND POLICY PROGRAM (ITRPP) IN IT MANAGEMENT?

(CT:IM-92; 08-01-2007)

a. The ITRPP was established by the CIO in November 2004 to provide a centralized place for the Department and other Federal entities to obtain information on the Department of State’s IT policy and related IT issues.

b. IRM/BPC/PRG oversees the process for collecting, analyzing, and corroborating IT policy and related inquiries from respondents, and other internal and external contacts as deemed appropriate. The results of these activities are documented and compiled for dissemination, in response to Web site inquiries.

c. IRM/BPC/PRG’s Web site is the official location to submit IT policy questions or to request IT-related information on these activities. Department organizations, both domestic and abroad, must use this Web site for IT policy and related IT issues. E-mail inquiries may be generated automatically through IRM/BPC/PRG’s Web site mail box, or directed to an RG office contact.

5 FAM 117 WHAT IS THE POLICY FOR ACCESS TO IT FOR INDIVIDUALS WITH DISABILITIES?

(CT:IM-73; 05-02-2006)

a. Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and relevant implementing regulations (36 CFR 1194) require Federal departments and agencies that develop, procure, maintain, or use electronic and information technology to ensure that Federal employees and members of the public with disabilities have access to and use of information and data, comparable to that of the employees and members of the public without disabilities–unless it is an undue burden to do so. If an agency invokes the undue burden exception, the statute requires the information and data be provided to individuals with disabilities by an alternative means of access.

b. The Information Resource Management Program for Accessible Computer/Communication Technology (IMPACT) initiative provides access to IRM technology, information, and programs for all customers, including individuals with disabilities. (Contact the IMPACT Outreach Center for more information on the IMPACT initiative.)

5 FAM 118 INFORMATION TECHNOLOGY (IT) SKILLS INCENTIVE PROGRAM

(CT:IM-94; 02-05-2008)

*The Information Technology (IT) Skills Incentive Program (SIP) was established to foster the development of advanced industry standard skills, certifications, and credentials by IT professionals who must maintain certain skills and requirements to continue in the SIP. (**Note**: IT professionals must be Department employees working in certain IT-related job series to be eligible for SIP.) The Department provides monetary incentives to those IT professionals who achieve designated skill sets. The Schultz Foreign Affairs Training Center’s Foreign Affairs Institute, School of Applied*

Information Technology (FSI/SAIT) administers the SIP, including the IT Skills Incentive Panel (see 5 FAM 118.1) and the Senior Advisory Panel (see 5 FAM 118.2). These organizations review SIP continuously, along with sustainment training, to meet the Department's needs (see the SIP Web site for more information on SIP including eligibility and approved job series.)

5 FAM 118.1 IT Skills Incentive Program Panel

(CT:IM-94; 02-05-2008)

The Director, Foreign Service Institute (FSI), selects an FSI senior manager to chair the IT Skills Incentive Program Panel. The Bureaus of Human Resources (HR), Information Resource Management (IRM), a functional and regional bureau, and the U.S. Agency for International Development (USAID) are panel member representatives. The respective heads of the above bureaus appoint their representatives, except that each functional and regional bureau will appoint one representative on an annual rotational basis when that bureau is scheduled to have a representative on the panel. The IT Skills Incentive Program Panel makes policy recommendations to the Senior Advisory Panel. The recommendations are not limited to policies, but include other changes such as adding or deleting certifications and/or credentials, and limiting or extending the timeframes of these certifications/credentials.

5 FAM 118.2 IT Skills Incentive Program Senior Advisory Panel

(CT:IM-94; 02-05-2008)

The IT Skills Incentive Program Senior Advisory Panel adjudicates policy recommendations made by the IT Skills Incentive Panel. The Chief Information Officer (CIO); the Deputy Assistant Secretary (DAS) for HR; and the Dean of FSI/SAIT comprise the membership of this Advisory Panel.

5 FAM 119 INFORMATION SECURITY STEERING COMMITTEE (ISSC)

(CT:IM-94; 02-05-2008)

a. The Information Security Steering Committee (ISSC) was established by the Undersecretary for Management (M) in 2005. The ISSC is a Department wide Deputy Assistant Secretary level group consisting of owners of information systems. The ISSC is co-chaired by the Chief Information Security Officer and the Senior Coordinator for Security Infrastructure.

b. ISSC members advise and instruct in a consultative and collaborative manner that stresses transparency, responsiveness, and cooperation. This enables an information security program that is service oriented, cost effective and meets statutory, regulatory, and business needs in a timely manner. The ISSC:

(1) Develops priorities and advocates for the availability of resources for the security of Department Information Systems;

(2) Recommends to the E-Gov Program Board revisions or development of specific operating policies, objectives and priorities as required by Federal information security standards and guidance;

(3) Provides clearance on high impact documents (e.g., Information Security Program Plan and Security Architecture);

(4) Coordinates strategic direction of the Department's information security efforts;

(5) Offers recommendations to the Department concerning identified duplication and omissions relating to information security;

(6) Supports Department funding/budget mechanisms as they relate to information security;

(7) Establishes common or type metrics for information security related activities;

(8) Ensures that processes and procedures are in effect to address Department information security requirements throughout the lifecycle; and

(9) Empowers Integrated Information Security Teams (IISTs) (see 5 FAM 119.1) to pursue efficient implementation of and or address challenges in meeting the Department's information security objectives.

5 FAM 119.1 Integrated Information Security Teams (IIST)

(CT:IM-94; 02-05-2008)

This policy establishes Integrated Information Security Teams (IIST) that consist of cross-bureau working-level subject matter experts from varied information security areas. Teams may be established or dissolved with the approval of the ISSC.