5 FAM 600 INFORMATION TECHNOLOGY SYSTEMS

5 FAM 610 DEVELOPING AND MANAGING INFORMATION TECHNOLOGY (IT) SYSTEMS

(CT:IM-95;   02-13-2008)
(Office of Origin: IRM/BPC/PRG)

5 FAM 611 GENERAL

(CT:IM-95;   02-13-2008)

a. This policy establishes Department standards for effective and efficient management of information technology (IT) investments.

b. Project managers must adhere to this policy throughout the systems life cycle.

c. Project managers must take a Department approved project management course and complete the Department’s mandatory leadership training program offered by the Foreign Service Institute (FSI) before taking on a project.

d. Project managers must develop performance criteria for measuring project performance based on the Department’s enterprise architecture (EA) and latest Office of Management and Budget (OMB) Performance Reference Model (PRM) and Performance Measures required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-80. (See 5 FAM 670.)

e. All systems (including applicable contractor systems) and applications associated with any projects must be registered in Information Technology Applications Baseline (ITAB). (For more information on how to register system and applications in the ITAB, refer to the ITAB Web site.)

f. Managers must coordinate all long- and short-term training requirements (domestically and abroad) related to the project with FSI before starting any IT project.

g. All major projects must be evaluated through the Capital Planning and Investment Control (CPIC) process. (See the E-Gov Program Management Office (PMO) Web site.)

h. Project managers must use an approved Earned Value Management System (EVMS) for all major projects in accordance with guidelines established in American National Standards Institute/Electronics Industries Alliance (ANSI/EIA-STD-748). (See 5 FAM 680.)

i. Electronic Signature (E-Sign) is authorized for use to digitally sign contracts and other legal forms and documents that are usually written on paper. (See 5 FAM 612, paragraph b.)

j. A government program/project manager (GPM) or other designated full-time U.S. Government employee must represent organizations for training, briefings, and seminars regarding major and nonmajor investments.

k. The Department requires that project managers incorporate IT security into the life cycles of their projects and systems (per Procurement Information Bulletin 2006-10, Information Technology Security and Contracts) and use performance-based measures in the performance of all IT contracts (per FAR 37.6 Performance-Based Acquisition).

l. Project managers must involve data management in the beginning and throughout the project life cycle of all major applications and general support system activities. (See 5 FAM 630.)

m. Project managers must indicate that quality is being integrated in projects by taking the necessary steps to lay out the requirements and the method for managing them. (See 5 FAM 640.)

n. Program managers must seek the involvement of the Contracts and Procurement Division for all acquisition initiatives and requirements. Their participation beginning in the initial phases will likely contribute to exploring strategic approaches, establishing requirements, simplifying the procurement plan, obtaining required internal approvals, preparing specifications, and achieving milestones.

o. System owners should consult the Privacy Division of the Office of Information Programs and Services (A/ISS/IPS/PRV) when conducting a Privacy Impact Assessment (PIA). Under the E-Government Act of 2002, agencies are required to conduct a PIA before:

(1) Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about a member of the public, or

(2) Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies), instrumentalities or employees of the Federal Government).

p. OMB M-07-16 and related memoranda mandate additional controls for all information systems (electronic or otherwise). These systems must implement additional protections for Personally Identifiable Information (PII) (see 5 FAM 613).

5 FAM 612 SCOPE AND AUTHORITY

(CT:IM-95; 02-13-2008)

a. This policy applies to all Department organizations and entities as the authority governing management of major and nonmajor IT investments. The policy provides requirements for project development, integration, modification, and maintenance of the Department IT systems, products, and services. This policy applies to all Department personnel, as well as contractors involved in Department systems and program planning, development, modification, integration, operation, and maintenance.

b. The authorities establishing this policy include:

(1) Paperwork Reduction Act, Public Law 104-13;

(2) Clinger-Cohen Act, Public Law 104-106 (formerly known as the Information Technology Reform Act);

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

(4) E-Government Act of 2002, Public Law 107-347

(5) Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, Title III;

(6) Government Paperwork Elimination Act of 1998, Public Law 105-277;

(7) Electronic Signatures in Global and National Commerce Act, June 30, 2000, Public Law 106-229;

(8) OMB Circular A-130, Appendix III, February 8, 1996;

(9) Presidential Decision Directive (PDD) 63, May 22, 1998;

(10) Federal Acquisition Regulation (FAR) Sections 7.102, 10.002 and 11.105;

(11) FAR, Subpart 34.2;

(12) ANSI/EIA-STD-748-A;

(13) Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d);

(14) Executive Order 13011 (Federal Information Technology);

(15) NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, June 2004;

(16) NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process;

(17) Privacy Act of 1974, (5 U.S.C and 552a), as amended;

(18) M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007);

(19) M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006);

(20) M-06-16, Protection of Sensitive Agency Information (June 23, 2006); and

(21) M-06-19, Reporting Incidents Involving Personally Identifiable Information (July 1, 2006).

5 FAM 613 DEFINITIONS

(CT:IM-85; 04-02-2007)

Acquisitions period: One of the three periods in the project cycle proceeded by study period and followed by the operations period. The acquisition period encompasses the source selection period.

Alternatives analysis: Identifies alternatives to meeting project objectives:

(1) Selection of the top three alternatives;

(2) Comparison of the three alternatives using a set of reasonable criteria;

(3) Identification of the preferred alternative; and

(4) Documentation of the benefits associated with the preferred alternative.

Annual operating costs: A one-year expenditure or cost projection for required resources to produce products and services.

Benefit cost analysis (BCA): A project development technique used as a systematic approach for comparing alternatives in project development; see also s**implified BCA**. (See 5 FAM 660.)

Business case: An executive report which outlines an evaluation of a proposed investment in terms of Department missions and objectives, purpose and approaches, costs and desired outcome, as well as investment risk analyses (including security risks). (This report is required for all IT projects and systems meeting the enterprise level of investment, defined as a major project by the E-Government Program Board (E-GovPB)).

Capital expenditures: Costs incurred for purchasing capital assets or tangible property, including durable goods, equipment, buildings, installations, and land.

Capital planning: A systematic effort to manage the risks and returns on capital assets for a given mission.

Capital planning and investment control (CPIC) process: A decision-making process, directed through the Department's E-Government Program Board (E-GovPB) to ensure that information technology investments integrate strategic planning, budgeting, procurement, and the management of IT in support of the Department's mission and business needs.

Concept of operations document: A detailed document that defines and establishes the human-to-machine workflow of the product for the operational environment.

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

Contracting officer: See FAR 2.101.

Contracting officer's representative (COR): A technically-qualified person designated as the contracting officer's authorized representative to assist in the administration of a contract. The designation must be made in writing by the contracting officer in accordance with DOSAR 642.270(f). (See 14 FAH-2, Contracting Officer's Representative Handbook, for more information and additional requirements.)

Control gate: A management review process in the project cycle designed to examine and evaluate project status (milestones) and to determine if the project will proceed to the next management event.

Conversion: Addresses requirements to change software, hardware, data values, forms, or organizational structures to enhance data use.

Data management (DM): The Department's management office for developing, standardizing, maintaining, and approving data elements for use in IT systems development projects.

Data mapping: A method used to identify and link selected data to one or more equivalent standard data elements.

Data modeling: Identifies informal graphical and textual representation and the entities and relationships involved in a data process; provides a mechanism for understanding the intended activity of a new system and designing the data.

Data reference model (DRM): One of the five reference models of the Federal Enterprise Architecture (FEA). The DRM is a framework of which its primary purpose is to enable information sharing, to allow reuse across the Federal Government via the standard description and discovery of common data, and to promote uniform data management practices.

Earned value management (EVM): See 5 FAM 680.

E-Government Program Board (E-GovPB): See 5 FAM 115.3.

Electronic signature (E-Signs): GPEA defines "electronic signature" as a method of signing an electronic message that:

(1) Identifies and authenticates a particular person as the source of the electronic message; and

(2) Indicates such person's approval of the information contained in the electronic message.

Executive management: Personnel (i.e., division chiefs, office directors, policy staff assistants) directly responsible for the approval and management of program planning and implementation, staffing requirements and assignments, and budget allocation and disbursement.

Federal Enterprise Architecture (FEA): The Federal Enterprise Architecture (FEA) is a set of inter-related reference models designed to facilitate cross-agency analysis and collaboration.

Information system: See 5 FAM 913.

I**nformation Technology Change Control Board (IT CCB):** A centralized body of knowledgeable personnel with the appropriate authority to evaluate change requests that impact the operational stability or maintainability of IT assets controlled, managed, or supported by the Department of State.

Managing State projects (MSP): A project management methodology consisting of periods, phases, activities, and control gates, designed specifically for the Department of State.

Object: Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, files, directories and programs, as well as bits, bytes, words, fields, keyboards, clocks, printers, network nodes. (See 5 FAM 630.)

Operations period: The third period in the project cycle, preceded by the study period and the acquisition period. The operations period encompasses the deployment phase, the operations and maintenance (O&M) phase, and the deactivation phase.

Performance-based service contracts: Contracts that incorporate a process for obtaining results that add value and benefit to the Department. These performance-based service contracts may include incentives and disincentives based on actual services performed.

Performance measures: Indicators of progress toward achieving goals and objectives based on actual vs. planned targets established.

Personally identifiable information (PII)*: Refers to information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Department employees should exercise their best judgment in determining the sensitivity of the PII. Sensitivity of the PII would depend on factors such as whether its unauthorized disclosure may result in any of the following harms to the records subject: fiscal or physical harm, identify theft, personal or professional embarrassment, inconvenience, unfairness, security risks, coercion, and/or other adverse effects.*

Privacy impact assessment (PIA)*: An analysis of how personal information is collected, stored, shared, and managed in a Federal system:*

(1) To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) To determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(3) To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Program: A coordinated group of planned undertakings (projects) having a common goal, objective, or mission.

Project: A carefully planned task or undertaking that has been scheduled to meet specified performance goals and achieve a desired result within defined budget and time constraints.

Project management certificate: An official document awarded to students who successfully complete a sequence of courses (i.e., a mixture of required and elective courses).

Project plan: A documented collection of achievable goals that establishes a beginning and end; groupings of milestones and tasks; in MSP, a collection of control gates based on a work breakdown structure outlining tasks.

Project quality assurance: A process consisting of features and functions used in project development to ensure that the system is reliable, authentic, and meets all the requirements of the quality assurance plan.

Project quality control: Activities performed continually throughout a project to verify that project management and project deliverables are of high quality.

Project quality management: A management function that includes all activities that determine the policy, objectives, and responsibilities, and implements them through quality planning, quality control, and quality assurance.

Project r**isk management:** A method to identify and evaluate risks associated with a project, system, or overall investment, and incorporates input into planned project/system/investment goals.

Quality assurance manager: The person responsible for overseeing all aspects of achieving the required quality performance, including inspectability, testability, process control, and related factors(also called the QA process).

Return on investment (ROI): The result for projects that show positive gains (improved mission performance; reduced cost; increased quality, speed, or flexibility; increased customer/employee satisfaction) have been demonstrated.

Risk: The potential for encountering negative technical, costs, or schedule impacts in a project.

Simplified BCA: A scaled-down version of the BCA that focuses only on those elements that the project manager deems relevant.

Study period—MSP: The conceptual planning phase, (i.e., requirements gathering, details); time used to establish the scope and direction of the project by recommended phases (i.e., user-requirements definition, concept definition, system definition, and acquisition planning).

System: See 5 FAM 913.

Task manager: The person on the project team responsible for ensuring completion of tasks in the work breakdown structure of the project plan; the individual responsible for managing a task or cost account.

Validation: The generic term that applies to the whole range of data quality issues, from elimination of duplicate records to compliance with format standards to matching values with reference tables.

Vendor: Used synonymously with supplier of material or services for sale through catalog, reverse auction, and/or price quote. (Certain laws apply for funding thresholds between $2,500.00 - $25,000.00.)

5 FAM 614 ACQUIRING IT SERVICES

(CT:IM-79; 11-08-2006)

a. Managers must begin coordinating all acquisition requirements with the contracting officer (CO) as soon as the requirements are initially identified. Managers must fully cooperate with COs and contracting officers representatives (CORs) in all aspects of the award and administration of all contracts. COs, CORs, and managers must hold contractors accountable for performance in accordance with the contract. Only the CO can modify the contract, if necessary.

b. See 5 FAM 900 for IT Acquisition policies.

5 FAM 614.1 Performance Work Statements

(CT:IM-85; 04-02-2007)

a. The CO is responsible for implementing performance-based service contracting. The CO is also ultimately responsible for everything that goes into the contract, include the performance work statement.

b. The COR is responsible for the quality (see 5 FAM 640) of the performance work statement that is submitted to the CO and should reject procurement requests that do not meet this requirement. The COR must have completed COR training before performing contract management responsibilities. FSI is the preferred source for this training.

c. Program offices must arrange for training of employees who write performance work statements for services. Employees may receive training through FSI or from other sources.

d. Project managers must establish criteria to scrutinize incoming procurement requests for project development.

5 FAM 614.2 Requirements for Contracts

(CT:IM-79; 11-08-2006)

a. All new service contracts must be performance-based, with defined deliverables and performance standards, unless justified in writing and approved by the Office of the Procurement Executive (A/OPE) (see 5 FAM 915.4).

b. Per FAR 11.105, all new supply contracts shall be solutions-based and results-oriented rather than specifying a specific brand name. If only one or a limited number of brand names are acceptable, then the brand name specification must be justified in accordance with FAR 11.105(b) or 11.105(c), as determined to be applicable by the CO.

c. The Department is accountable to OMB through the e-CPIC process for periodic reports on the progress made in performance-based service contracting.

5 FAM 615 THE PROJECT PLAN

(CT:IM-79;   11-08-2006)

A project plan must be in place before beginning any project for accountability purposes and successful results. A typical project plan should include the clearly defined requirements, tasks, schedule, tasks assignments, resources, and expected results. The project plan becomes the primary source of information for how the project will be planned, executed, monitored and controlled and closed. All project plans must include the following:

(1) Project background—briefly describe effort and state goals;

(2) Responsibilities—name key personnel;

(3) Objectives and performance measures—clearly state objectives to include performance measures and how these objectives will be accomplished;

(4) Business case—prepare a business case, during the project's study period, that addresses risks in terms of specific security considerations as well as the cost, schedule, performance, functional and technical requirements;

(5) Work breakdown structure—subdivide the major project deliverables and project work into smaller, more manageable components, including security requirements, to accomplish the goals;

(6) Issues, risks, security, constraints—identify concerns, problems, and possible delays;

(7) Annual operating costs—estimate annual operating costs, including short-term and long-term training and security requirements costs;

(8) Signatures—project manager must sign and secure other approval signatures as required;

(9) Courses and students—list of training required and individuals to be trained; and

(10) Contract review performed by the Office of the Procurement Executive (A/OPE).

5 FAM 616 REVIEW BOARDS

(CT:IM-79; 11-08-2006)

a. The following senior-level boards evaluate IT projects in accordance with 5 FAM 110:

(1) Electronic Government Program Board (E-GovPB): An advisory entity to the Under Secretary for Management that addresses the full range of Department e-Government and IT investment portfolio and project management activities;

(2) The E-Gov Advisory Group: Provides a business, technical, and investment evaluation of IT initiatives before submission to the E-GovPB, considering potential risk, cost, benefit, alignment with the Department's EA, and priority in relation to other IT investments. It also identifies issues for E-GovPB review to ensure senior-level attention;

(3) Electronic Government Program Office (E-GovPMO): The office that ensures the completion of all program elements related to the Department's IT investments for meeting E-Government guidance and to ensure that major milestones are met throughout all stages of the Capital Planning and Investment Control (CPIC) process;

(4) Information Technology Change Control Board (IT CCB): (see 5 FAM 110);

(5) Local Change Control Board (CCB): (see 5 FAM 110).

b. Both advisory groups review proposed IT programs to ensure that technical objectives can be achieved and proposed projects are sound investments that contribute to the organization's mission and the Department's strategic goals for IT endeavors to include all individuals in 5 FAM 110.

5 FAM 617 ROLES AND RESPONSIBILITIES

(CT:IM-79; 11-08-2006)

Executive management is responsible for the overall direction, policy, and priorities of IT programs and projects. Project roles and responsibilities are stated in 5 FAM 617.1 through 5 FAM 617.7.

5 FAM 617.1 Executive Management

(CT:IM-79;   11-08-2006)

Executive management facilitates support and resolves conflict. Responsibilities include the following:

(1) Commits appropriate resources, including training, to the project;

(2) Defines review board's goals and objectives;

(3) Defines and clarifies corporate goals through established architecture using review board's results;

(4) Appoints project manager and defines project manager's authority to lead and control work and resources;

(5) Defines decision channels for project;

(6) Provides project manager with long-range planning and budget information to establish timely control gates within the project plan;

(7) Ensures the project operates within budget constraints; and

(8) Assigns management responsibility to ensure security controls are identified.

5 FAM 617.2 Project Manager

(CT:IM-79;   11-08-2006)

a. Every project must have a project manager to oversee the IT investment and ensure progress towards project goals and deliverables. The project manager assigns specific roles and a responsibility to project team members and ensures accurate and timely completion of all required documentation and reporting requirements.

b. The project manager:

(1) Manages resources and activities to meet technical objectives and satisfy user requirements by ensuring completion of the project plan and requirements analysis documents at the outset;

(2) Is accountable for overall planning, direction, and execution;

(3) Directs team, monitors progress, and resolves conflict;

(4) Reviews requests for project development, modification or integration and technical products, problem reports, and change requests;

(5) Keeps abreast of changes to the operating environment to determine how to properly respond;

(6) Ensures the project operates within budget constraints;

(7) Manages the budget and ensures timely funding by executive management, if project exceeds budget year(s);

(8) Controls configuration management (CM) processes and establishes quality assurance (QA) guidelines for the team;

(9) Identifies training requirements in support of new projects or extensions of existing projects;

(10_ Ensures adequate funding is requested for training in support of new projects or extensions of existing projects;

(11) Keeps executive management abreast of the project status; and

(12) Includes security costs (including certification and accreditation) when budgeting for the project.

5 FAM 617.3 Project Team

(CT:IM-79; 11-08-2006)

a. The project team is comprised of members with various technical and functional levels of expertise (e.g., analysts, contractors, technical writers, and IT experts), as required to complete a project.

b. At a minimum, the project team will consist of the following members:

(1) Project manager;

(2) Contracting officer (CO);

(3) Contracting officer’s representative (COR);

(4) Project task manager for tasks that are established within the work breakdown structure of the project plan;

(5) Budget coordinator;

(6) Quality assurance manager;

(7) End user and/or sponsor;

(8) Vendor and/or contractor representative, if a contract is in place;

(9) Information system security officer (ISSO);

(10) Training officer; and

(11) Configuration manager.

c. Team members are assigned tasks by the project manager and work together to accomplish the following tasks:

(1) Collect and analyze requirements;

(2) Coordinate budget and resource requirements;

(3) Report periodically to project manager or project task manager;

(4) Produce project quality assurance documentation needed to meet requirements; and

(5) Represent vendor and/or contractor to assist with deliverables, if necessary.

d. Team members may be required to serve on the project team for any portion of the project lifecycle.

5 FAM 617.4 Sponsor

(*TL:IM-52; 06-25-2004)*

The sponsor is the primary point of contact in the end user (sponsor) organization. The sponsor does the following:

(1) Submits and authorizes requests;

(2) Commits resources to define and specify requirements;

(3) Represents the user and/or customer;

(4) Interacts with the project manager and others outside of the sponsor organization;

(5) Coordinates user participation, when necessary;

(6) Participates in quality assurance and security reviews;

(7) Reviews and approves products;

(8) Accepts the system when it meets users’ requirements; and

(9) Identifies training users will need, if any, to use the end product.

5 FAM 617.5 User And/Or Customer

(CT:IM-85; 04-02-2007)

Anyone who will use the system or end product being developed and/or accepts the end product(s) is a user or a customer. The user and/or customer specify that software requirements are based on business needs by participating in interviews and providing reference materials to substantiate requested replacement system. The user and/or customer may provide additional input as follows:

(1) Reviews and provides input to documentation prepared by the project team;

(2) Develops and/or approves acceptance test;

(3) Administers and participates in acceptance test;

(4) Prepares appropriate administrative and/or user documentation, such as responsibility for developing training /guides and standard operating procedures;

(5) Develops a concept of operations document if necessary;

(6) Participates in system/product/services testing;

(7) Attends any training needed in order to be able to use the end product; and

(8) Accepts system, product, or service after user requirements are satisfied.

5 FAM 617.6 Quality Assurance Manager

(CT:IM-79; 11-08-2006)

The quality assurance (QA) manager is the primary contact for project quality assurance and configuration management issues. The QA manager:

(1) Monitors and updates development requests per the initial statement of work or functional requirements;

(2) Ensures the project manager establishes an IT engineering process based on managing State projects (MSP) or other approved engineering processes;

(3) Interacts with the project manager and others outside of the sponsor organization concerning all configuration management (CM) and/or QA issues;

(4) Participates in project quality assurance reviews;

(5) Reviews and approves products;

(6) Establishes and records a baseline for the product throughout its lifecycle; and

(7) Defines product naming and tracking standards.

5 FAM 617.7 Data Administrator

(CT:IM-79; 11-08-2006)

The data administrator develops physical database models for major and nonmajor projects that comply with the data reference model (DRM); approves, maintains, and ensures accuracy of data and database performance; coordinates with the Data Administration Working Group (DAWG) on behalf of the project team. (See 5 FAM 636.)

5 FAM 618 PROJECT RISK MANAGEMENT

(CT:IM-79; 11-08-2006)

a. Project risk management is a process used to manage or predict future outcomes based on present knowledge. Project managers must be committed to addressing the management of risk proactively and consistently throughout the project.

b. Risk assessment judges the probable effect of each risk factor on the project, so that the project manager can minimize the effort in responding appropriately.

c. A risk is usually brought about by lack of resources, lack of information, or lack of control over the decision-making process. An analysis of this risk and any strategy adopted to control it should consider these causes. Common risk factors include (but are not limited to) the following:

(1) Volatility of requirements;

(2) Project scope;

(3) Project management ability;

(4) Project staffing levels and skills;

(5) Technology experience and degree of innovation;

(6) Technical complexity;

(7) Realism of project schedules;

(8) Availability of funding;

(9) Senior management support;

(10) Number and types of procurement;

(11) Security risks;

(12) Logistics and/or transportation of materials;

(13) Host-country factors (e.g. customs, infrastructure); and

(14) Inadequate training for developers or users.

d. Project managers should consider these basic risk control strategies:

(1) Reduce the likelihood or consequence of risk (e.g., “buy” information, i.e., a study or prototype);

(2) Protect the project from risk by arranging the project plan to accommodate risk (much like fault tolerance);

(3) Set up contingency funds or additional time to cover unexpected loss;

(4) Decide whether to accept the consequences; and

(5) Focus visibility and management attention on clearly defined tasks (i.e., control gates).

5 FAM 619 SYSTEM AUTHORIZATION

(CT:IM-95;   02-13-2008)

a. Security safeguards must be in place to protect the automated information system and its data against unauthorized access, modification, destruction, and unavailability.

b. Project managers must issue a letter of intent to perform C&A to the Office of Information Assurance (IRM/IA) after registering in the ITAB and completing IT CCB base line validation to ensure timely system authorization and to avoid unnecessary delays.

c. Department system owners responsible for Department information systems, including those responsible for non-Department entities (e.g., contractors, vendors), must ensure that system authorization is performed on all FISMA reportable Department systems. (See 5 FAM 1064.)

d. Project managers must budget for security costs including certification and accreditation when incorporating each safeguard and/or countermeasure into the system. IRM/IA will assist project managers in preparing the security portion of their investment documents. Consider programming, time needed for testing, security equipment purchases, etc. (See the IRM/IA Web site.)

e. System authorization must be performed in accordance with Department requirements. See 5 FAM 1060; the appropriate sub-chapters of 5 FAH-11; also see IRM/IA and the Office of Computer Security (DS/SI/CS) Web page.

f. Systems owners are responsible for all funding required to perform C&A of their systems. (See 5 FAM 1065.)