5 FAM 900
INFORMATION TECHNOLOGY (IT) ACQUISITION

5 FAM 910
INFORMATION TECHNOLOGY (IT) ACQUISITION POLICIES

(CT:IM-101; 12-08-2008)
(Office of Origin: IRM/BPC/PRG)

5 FAM 911 SCOPE

(CT:IM-101; 12-08-2008)

a. This chapter discusses the policies and procedures for acquiring IT. The acquisition of IT is a critical phase in the life-cycle process for planning, budgeting, and managing IT assets in the Department. The Department's planning processes, including IT, are discussed in 5 FAM 1000, Information Technology (IT) Planning.

b. The operation and management of installed IT assets, i.e., system installation and maintenance, system security, training, and the Internet, are discussed in 5 FAM 800, Information Systems Management. The development and management of Departmental IT systems are contained in 5 FAM 600, Information Technology Systems.

c. Program offices and *posts* must use guidance in 14 FAM for overall generic acquisition policy. 5 FAM 900, Information Technology (IT) Acquisition, contains unique IT acquisitions guidance. It supplements and must be combined with 14 FAM guidance to ensure effective, efficient, and economical IT acquisitions.

5 FAM 912 AUTHORITIES

(CT:IM-64; 06-20-2005)

The authorities for these policies and procedures are:

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

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

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

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

(5) Public Law 105-277, Div. A, Section 101(h), Title VI, Section 632 of the Omnibus Appropriation and Authorization Act for FY 1999;

(6) Public Law 105-520, Workforce Investment Act of 1998;

(7) Public Law 106-398, sec. 821, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001;

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

(9) 41 CFR Chapter 101, Federal Property Management Regulations;

(10) 41 CFR Chapter 102, Federal Management Regulation;

(11) 48 CFR Chapter 1, Federal Acquisition Regulation (FAR);

(12) 48 CFR Chapter 6, Department of State Acquisition Regulation (DOSAR);

(13) E.O. 12845 (Requiring Agencies to Purchase Energy Efficient Computer Equipment);

(14) E.O. 12931 (Federal Procurement Reform);

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

(16) E.O. 13101 (Greening the Government);

(17) E.O. 13103 (Computer Software Piracy);

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

(19) OMB Circular A-109, Major System Acquisitions;

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

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

(22) Capital Programming Guide, Version 1.0, Supplement to OMB Circular A-11, Part 7: Planning Budgeting, Acquisition and Management of Capital Assets;

(23) 36 CFR Part 1194, Architectural and Transportation Barriers Compliance Board Electronic and Information Technology Accessibility Standards; and

(24) NSTISSP (National Security Telecommunications and Information Systems Security Policy) No. 11, Subject - National Policy Governing the Acquisition of Information Assurance (IA) and IA-

Enabled Information Technology (IT) Products, January 2000, revised July 2003.

5 FAM 913 DEFINITIONS

(CT:IM-64; 06-20-2005)

a. **CENTREX** is a designation for "Central Exchange", a telephone system that uses the carrier's network to provide the functionality of a PBX without the user needing to purchase and manage one.

b. **Commercial Off-the-Shelf (COTS)** are IT products that are widely available and are developed with general commercial applications in mind.

c. **Competitive sourcing** is the process of studying the cost of public vs. private sector performance, with the ultimate goal being to ensure efficient and effective U.S. Government. Competitive sourcing is not simply outsourcing (contracting out), but rather the analysis of whether commercial activities are best performed in-house or by contractors. The competitive sourcing process could result in retaining a function within the Department or outsourcing it, depending on which makes better business sense. OMB Circular A-76 establishes Government-wide policy on competitive sourcing.

d. **Electronic and Information Technology (EIT)** for purposes of providing accessibility includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, is not information technology (36 CFR 1194.4).

e. **Government Off-the-Shelf (GOTS)** are IT products that are developed by U.S. Government organizations with U.S. Government-related requirements in mind and are designated as available only to other U.S. Government organizations. In the context of NSTISSP No. 11, GOTS are Information Assurance or Information Assurance-Enabled products that

often require special features and assurances that are not found in typical Commercial-Off-the-Shelf (COTS) products. These additional features and assurances are usually developed with U.S. Government cooperation and results in products that contain domestic and/or international restriction.

f. **Information Assurance (IA)-Enabled Product** is an IT product or technology whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities. Examples include products such as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems (NSTISSP No. 11).

g. **Information Assurance (IA) Product** is an IT product or technology whose primary purpose is to provide security services (e.g., integrity, authentication, confidentiality, access control, and non-repudiation); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include products such as data encryptors, firewalls, and intrusion detection devices (NSTISSP No. 11).

h. **Information Life Cycle** means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition (OMB Circular A-130).

i. **Information Resources** means information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. 3502(6)).

j. **Information System** means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

k. **Information Technology (IT)** means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

   (1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires:

      (a) Its use; or

      (b) To a significant extent, its use in the performance of a service or the furnishing of a product.

   (2) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services

(including support services), and related resources.

(3) The term "information technology" does not include any equipment that:

(a) Is acquired by a contractor incidental to a contract; or

(b) Contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, is not information technology (FAR Subpart 2.1).

l. **Inherently Governmental Function** is an activity that is so intimately related to the public interest as to mandate performance by U.S. Government personnel. These activities require the exercise of substantial discretion in applying U.S. Government authority and/or in making decisions for the U.S. Government. Inherently governmental activities normally fall into two categories: the exercise of sovereign U.S. Government authority or the establishment of procedures and processes related to the oversight of monetary transactions or entitlements. An inherently governmental activity involves:

(1) Binding the United States to take or not to take some action by contract, policy, regulation, authorization, order, or otherwise;

(2) Determining, protecting, and advancing economic, political, territorial, property, or other interests by military or diplomatic action, civil or criminal judicial proceedings, contract management, or otherwise;

(3) Significantly affecting the life, liberty, or property of private persons; or

(4) Exerting ultimate control over the acquisition, use, or disposition of United States property (real or personal, tangible or intangible) including establishing policies or procedures for the collection, control, or disbursement of appropriated and other federal funds. (OMB Circular A-76, Attachment A, page A-2, May 29, 2003).

m. **Modular contracting** is an acquisition strategy in which an information system is acquired in successive, interoperable, increments or modules (41 U.S.C. 434(b)).

n. **Undue burden** in the context of providing accessibility means significant difficulty or expense. An agency shall consider all agency resources

available to the program or component for which the product is being developed, procured, maintained, or used in determining whether an action would result in an undue burden (36 CFR 1194.4).

5 FAM 914 RESPONSIBILITIES

(CT:IM-101; 12-08-2008)

a. Program offices and posts must:

(1) Acquire, whenever possible, IT in accordance with the Department's IT Strategic Plan, which is prepared under the guidance and direction of the Department's Chief Information Officer (CIO);

(2) Submit a Preliminary Forecast Plan (PFP) for IT hardware and software equipment and service acquisitions over $100,000, following the annual instructions from A/OPE, for potential IT acquisitions for the next two fiscal years. (See 14 FAM 221.*2*, Year-End Spending - policy contains departmental policy on year-end procurement since it may affect the PFP);

(3) Support all IT acquisitions with the necessary documentation as identified in Exhibit 916 (Matrix for the Review/Approval of Thresholds and Documentation Requirements for all IT Resource Acquisitions.) (See 14 FAM 210, Acquisition of Supplies and Services and FAR Part 7 for more information on acquisition planning);

(4) Obtain approval of the program area's Deputy Assistant Secretary, or position ranked equivalent (see 1 FAM 021.3, Authorities), for all IT resource acquisitions estimated to be valued between $10 million and less than $30 million;

(5) Obtain the approval of the program area's Assistant Secretary, or position ranked equivalent (see 1 FAM 021.3, Authorities), for all IT acquisitions valued at $30 million and above;

(6) Obtain approval of the Department's CIO, in writing, for all IT acquisitions with a value of $10 million or more per fiscal year, before submitting the request to the Office of Acquisition Management (A/LM/AQM);

(7) Ensure that when they procure EIT, the technology is accessible to people with disabilities, unless an exception applies or an undue burden would be imposed on the Department. (Contact the IRM Program for Accessible Computer/Communication Technology (IMPACT) and A/OPE for more information);

(8) Use the Information Technology Investment Portfolio System (I-TIPS) to enter data on all IT projects for review and approval and

inclusion in the IT Tactical Plan. The Electronic Government Program Board (E-GovPB) uses the I-TIPS data to assist with departmental funding decisions. The E-Gov Advisory, and the E-Gov Working Groups support the E-GovPB; and

(9) Use 14 FAM 230, Acquisitions Abroad and 12 FAH-6 OSPB (Overseas Security Policy Board) Security Standards and Policy Handbook, when posts need more information.

b. The Bureau of Information Resource Management's (IRM) Chief Information Officer (CIO) provides advice and other assistance to the Secretary of State and other senior management personnel of the Department to ensure that IT is acquired and information resources are managed for the Department in a manner that implements the policies and procedures of existing law and regulations.

c. The Bureau of Administration, Logistics Management's Office of Acquisition Management (A/LM/AQM) is a centralized acquisition service for the Department to ensure the Department's compliance with all applicable regulations, budgetary priorities and established standards within the Department.

d. The Bureau of Administration, Office of the Procurement Executive (A/OPE) has Department-wide responsibility to issue acquisition policy, provide advice and guidance to the Department's domestic and foreign contracting offices and staff, and promote innovation. A/OPE is also responsible for managing the implementation of electronic commerce in the Department. (See 1 FAM 212.2, Office of the Procurement Executive for additional acquisition responsibilities held by A/OPE.)

e. The Electronic Government Program Board (E-GovPB), which is comprised of senior Department officials and chaired by the Under Secretary for Management reviews all IT projects that are funded from the Department's IT Central Fund. The E-Gov Advisory Group (also composed of Department officials) provides a business, technical, and investment evaluation of E-Gov/IT initiatives prior to submission to the E-GovPB. (Contact the E-Gov Program Management Office for more information.)

f. The Chief Financial Officer (CFO) (Assistant Secretary for Resource Management (RM)), working with the CIO and the E-GovPB, must develop a full and accurate accounting of IT expenditures, related expenses, and results outlined in the Paperwork Reduction Act (PRA) of 1995.

5 FAM 915 GENERAL IT ACQUISITION POLICIES

5 FAM 915.1 IT Planning Process

(CT:IM-64; 06-20-2005)

a. Decisions about which IT programs and projects in the Department will be supported and how the needed assets will be obtained are made during the IT planning processes. The acquisition phase can begin to obtain the needed IT assets once funds have been approved and made available. The responsible program office must confirm that any decisions made during the planning process on the direct purchase of the needed asset or the need for development are still appropriate at the onset of an acquisition.

b. OMB Circular A-130 requires that federal agencies establish a multi-year strategic planning process for acquiring and operating IT that meets program and mission needs, reflects budget constraints and forms the basis for its IT budget requests. IT acquisitions will be based upon the Department's IT Strategic Plan, which is the 5-year plan for meeting its IT needs.

c. Bureaus are required to incorporate the capital planning and investment process into acquisition planning using I-TIPS. I-TIPS, a web-based application assists federal agencies in managing their IT investments. Costs, risks, return on investments, and maintaining the appropriate mix of organizational and technical considerations are among I-TIPS' goals. (See 5 FAM 1000, Information Technology (IT) Planning for additional information concerning the Department's IT Capital Planning and Investment Process.) (IRM/BPC/EAP/PL can provide information on the E-GovPB and its subgroups.)

5 FAM 915.2 IT Acquisition Risk Management

(CT:IM-64; 06-20-2005)

Program offices must identify and analyze risks in acquiring and implementing IT system projects. This is an important consideration when making IT investment decisions. Program offices should limit the amount of development work, especially writing custom-code from scratch, and make effective use of competition and financial incentives for vendors to minimize the risks in IT acquisitions. Program offices should include known risks in a solicitation to encourage offerors to provide recommendations on risk mitigation and management.

5 FAM 915.3 IT Acquisition Reform Initiative - Past Performance

(CT:IM-64; 06-20-2005)

This initiative, based upon the Federal Acquisition Streamlining Act (FASA), (Public Law 103-355), requires that the past performance of contractors in supplying similar supplies and services must be considered in the technical evaluation for any IT acquisition competition. Program managers must offer additional justification when they decide to use an offeror with past performance problems. Past performance must be thoroughly addressed in any IT solicitation to ensure that all offerors fully understand the role it will play in the selection process.

5 FAM 915.4 Performance-Based Contracting

(CT:IM-101; 12-08-2008)

Performance-based service contracting (PBSC) is the preferred method for acquiring services. (Public Law 106-398, section 821 (FAR, section 37.102(a).) The results and outcomes to be accomplished, rather than dictating to the contractor how to obtain them, are described in PBSC. PBSC is also known as solutions-based contracting or quality sourcing. Performance-based contracting may be used for systems, hardware, or software. Since fiscal year 2001 all new IT service contracts must be performance-based unless justified in writing and approved by A/OPE. (See 5 FAM 614, *Acquiring IT Services,* and 5 FAM 614.1, *Performance Work Statements*.) The Departmental Competition Advocate in A/OPE will address questions concerning PBSC. Contract performance must be measured when program managers consider future work.

5 FAM 915.5 Modular Contracting for IT

(CT:IM-64; 06-20-2005)

The Clinger-Cohen Act, Section 5202 (41 U.S.C. 434) provides that federal agencies should use modular contracting for acquisition of a "major system" of IT, **to the maximum extent practicable**. (See 14 FAM 200, Supplies, Equipment, and Nonpersonal Services for more information on "major systems.") Modular contracting is an alternative process that provides the Department the opportunity to incrementally acquire a system. (See FAR 39.103 for more information on modular contracting.)

5 FAM 915.6 Major Systems Acquisition

(CT:IM-64; 06-20-2005)

The Department satisfies OMB Circular A-109, Major Systems Acquisition, requirements through the IT Capital Planning process. (See 5 FAM 1000, Information Technology (IT) Planning.) (See FAR Part 34 for additional policy and guidance concerning major system acquisitions under OMB Circular A-109.)

5 FAM 915.7 Accessibility Requirements for People with Disabilities

(CT:IM-101; 12-08-2008)

a. Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the *Section 408(b)* of the Workforce Investment Act of 1998 (Public Law 105-220), requires Federal agencies to make *Electronic and Information Technology (EIT)* accessible to people with disabilities. Section 508 requires that when the Department develops, procures, maintains, or uses EIT, Federal employees with disabilities will have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the Department.

b. Section 508 also requires that individuals with disabilities who are members of the public seeking information or services from the Department, *will* have access to and use of information and data that is comparable to that provided to *members of* the public who are not individuals with disabilities, unless an undue burden would be imposed on the Department.

c. *Procurement Information Bulletin (PIB) No. 2001-17, available through A/OPE, provides additional guidance on Section 508. The PIB is primarily for use by requirements and program offices in identifying whether a particular requirement is subject to Section 508, identifying compliant Section 508 products and services, preparing undue burden and non-availability determinations (for purposes of seeking an exemption from Section 508's requirements), and conducting technical evaluations vis-à-vis the accessibility standards. It provides more detailed guidance to contracting officers on Indefinite delivery/Indefinite quantity (IDIQ) requirements and provides a sample solicitation provision and contract clause for use in solicitations and contracts subject to Section 508.*

d. *Contact the IRM Program for Accessible Computer/Communication Technology (IMPACT) for assistance to bureaus to attain Web site and application compliance with Section 508 requirements at the planning, development, and/or procurement stages of obtaining accessible EIT, and the A/OPE Web site for more information about PIB No. 2001-17.*

5 FAM 915.8 Checklist for IT Acquisitions

(CT:IM-64; 06-20-2005)

Program offices managing IT acquisitions must refer to the checklist for IT acquisitions contained in Exhibit 915 (IT Acquisitions Checklist). This checklist reminds offices of questions that need to be answered and documentation that needs to be prepared throughout the life cycle of an IT

acquisition.

5 FAM 915.9 IT Hardware-Operating System Compatibility

(CT:IM-64; 06-20-2005)

Department offices procuring IT hardware must ensure that acquisitions include planned requirements that IT hardware will be compatible with the Department's operating systems. Offerors must demonstrate in writing that their hardware is compatible with the Department's operating systems.

5 FAM 915.10 Support Services and Warranties

(CT:IM-64; 06-20-2005)

Contractor-provided support services and warranties for hardware or software, e.g., maintenance and troubleshooting, must be considered as part of the evaluation process that is used to select the source being acquired for the IT need.

5 FAM 915.11 Software

(CT:IM-64; 06-20-2005)

All Department employees and contractors must ensure that U.S. Government-acquired commercial software is safeguarded against licensing violations and copyright infringements. Home use of software is generally prohibited. All software running on Department systems must have a valid license from the contractor; e.g., a single user license or a vendor provided site license. Department offices are encouraged to obtain multiple-user or site licenses when procuring software for a large number of users. A warranted Contracting Officer can only execute software licenses after obtaining legal review from L/BA.

5 FAM 915.11-1 Software Licensing

(CT:IM-101; 12-08-2008)

a. Executive Order 13103 requires the Department to adopt procedures to ensure that computer software is not acquired, reproduced, distributed, or transmitted in violation of applicable copyright laws. Severe penalties exist for violators.

b. The Information Technology Change Control Board (IT CCB) manages changes to the Department's global IT environment and must approve any software installed on unclassified and classified infrastructures through the Secret level. IT CCB approval is not required for standalone

development/test laboratory infrastructures. (See 5 FAM 651 d, The Information Technology Change Control Board (IT CCB) for more information on the roles of the IT CCB and local CCBs and/or contact IRM/OPS/ENM.)

c. The Department's Internet Steering Committee maintains a recommended list of software applications for Web site development. Software license procurement is authorized from this list.

d. Software upgrades must be made in accordance with the licensing agreement used to purchase the software.

e. The Department has some enterprise agreements. Contact the IT Asset Management Branch (IRM/OPS/ENM/NLM/ITA) for more information on these agreements or inquire about plans for other software that might have an enterprise license in the future.

5 FAM 915.11-2 Software Use at Home

(CT:IM-64; 06-20-2005)

a. Generally, one software package per computer user is permitted unless the license agreement allows for multiple use of the program. But, some software publishers' licenses allow for "remote" or "home" use of their software. In some cases, software may be copied onto a second machine outside the office if a user travels or telecommutes. Check the software license carefully to see what is allowable.

b. Some enterprise agreements prohibit software use for work at home. Exceptions have been granted. Contact IRM/OPS/ENM/NLM before any work-at-home software installations are attempted.

5 FAM 915.12 Federal Acquisition Regulations (FAR) and the Department of State Acquisition Regulation (DOSAR)

(TL:IM-42; 09-26-2003)

All Departmental contract actions to acquire IT must comply with the FAR (see 48 CFR Chapter 1) and DOSAR. (See 48 CFR Chapter 6 and contact A/OPE for more information.)

5 FAM 915.13 Acquisition Quality Review Statement

(TL:IM-42; 09-26-2003)

Program offices must incorporate the quality assurance requirements from 5

FAH-5 H-400, Quality Assurance and must complete an acquisition quality review statement during the course of the acquisition to assist them in performing a self-assessment and developing lessons learned. (See 5 FAM 924, which contains more information on the Acquisition Quality Review Statement.)

5 FAM 915.14 IT Baselines

(CT:IM-64; 06-20-2005)

a. Program offices must satisfy defined standards contained in IRM/BPC/EAP/AE's Enterprise Architecture (EA) document in order to achieve successful integration and standardization of information processing systems and data when making IT acquisitions. This document codifies a set of IT standards to be relied upon in deciding what IT products to buy, how to build IT components, and how to connect new components within the overall IT structure. It is designed to set priorities for IRM and to pursue IT advancements within the Department. The document defines both layered and crosscutting architectures of IRM's IT environment.

b. The IT CCB led by the Enterprise Network Management (ENM) Office in IRM, manages changes to the Department's classified and unclassified IT infrastructure. The IT CCB is concerned with the availability, reliability, integrity, security, interoperability, and performance of the Department's enterprise infrastructure.

c. The IT CCB works with the Electronic Government Program Board (E-GovPB) to ensure that projects meet the Department's IT standards and ensure that their scope does not adversely affect the enterprise infrastructure. (See 5 FAH-5 H-512, The Information Technology Change Control Board (IT CCB), for more information on the IT CCB.)

d. The IT CCB recommends unclassified and classified IT hardware specifications (baselines) for procurement. The IT CCB defines the minimum existing hardware specifications. (Contact IRM/OPS/ENM for more information.)

e. The IT CCB also recommends software configurations (baselines) for workstation and servers. (Contact IRM/OPS/ENM for more information.)

f. The Technical Security and Safeguards Division (IRM/OPS/ITI/TSS) evaluates and validates the technical security integrity of equipment considered for classified processing at U.S. Foreign Service posts. This division recommends to the Bureau of Diplomatic Security (DS) the approval or disapproval of the equipment. The division maintains a list of DS approved and division tested equipment for processing classified information.

5 FAM 915.15 Acquisition of IT Equipment To Process Sensitive or Classified Information

(CT:IM-64; 06-20-2005)

a. All IT acquisitions must contain appropriate security requirements to ensure that acquired systems and the information to be processed by these systems will be protected from unauthorized disclosure and accidental destruction. The Department's Bureau of Diplomatic Security, Office of Information Security Technology (DS/C/ST) develops Computer Security and Privacy Plans (CSPPs). CSPPs outline the major components of the Department's overall computer security program as required by the Federal Information Security Management Act (FISMA) (Public Law 107-347, Title III).

b. Program offices must coordinate with DS/C/ST and DS/SI/CS whenever initiating an IT acquisition to process classified information. Program offices must also coordinate with DS/C/ST and DS/SI/CS when initiating a significant IT acquisition for a sensitive system. However, program offices are permitted to use random procurement for minor, component (e.g., an "off-the-shelf" printer or "off-the-shelf" software) IT acquisitions for a sensitive system.

c. In addition, program offices must do the following whenever there is a need to acquire IT equipment that will process **classified** information:

   (1) **For locations abroad**: submit requests, as well as any appropriate supporting documentation for the Classified LAN to the Program Management and Analysis Office (IRM/OPS/PMA). PMA's Joint Laboratory evaluates COTS, Zoned, and TEMPEST products for the Classified-NT and Windows 2000 Classified LAN to ensure CableXpress, Windows NT 4.0, and Windows 2000 compatibility. (Contact IRM/OPS/PMA for more information.) The selection of the proper equipment, to satisfy the need, will be based upon the TEMPEST requirements, established by DS/C/ST for the requesting post.

   (2) **For domestic locations**: obtain the approval of DS' Office of Security (DS/C/ST), which will determine if the office requires TEMPEST-approved, or non-TEMPEST hardware.

5 FAM 915.15-1 Acquisition of Digital Copiers Used to Process Classified Information

(CT:IM-64; 06-20-2005)

Digital copiers for classified processing are categorized as Classified Automatic Information Systems (CAIS) and Classified Information Processing

Equipment (CIPE). Digital copiers that are used to copy, print, scan, or otherwise process classified information must meet the TEMPEST, technical and computers security requirements of 12 FAH-6 H-310, Classified Information Processing Equipment (CIPE) and 12 FAH-6 H-541, Classified Automatic Information Systems (CAISs). This requirement applies even if the digital copier will be used only as a stand-alone device for copying.

5 FAM 915.15-2 Acquisitions for Controlled Access Areas (CAA)

(TL:IM-42; 09-26-2003)

a. All items purchased for the CAA must conform to the Overseas Security Policy Board (OSPB) security standards as set forth in 12 FAH-6 H-310 (available only on ClassNet).

b. IT acquisitions destined for the CAA must conform to security requirements in various subsections of 12 FAH-6, OSPB Security Standards and Policy Handbook, and 12 FAM 536.5, Access by Foreign National Employees.

c. A/LM/AQM/IT periodically issues guidance on acquisitions for the CAA via an ALDAC telegram.

5 FAM 915.15-3 Acquisition of Information Assurance (IA) Products and IA-Enabled Products for Classified Systems

(CT:IM-64; 06-20-2005)

a. National Security Telecommunications and Information Security Policy (NSTISSP) No. 11 is a national security community policy governing the acquisition of information assurance (IA) and IA-Enabled information technology products. The following paragraphs contain acquisition policies and procedures based upon NSTISSP No. 11.

b. For all classified systems procured **on or after** July 1, 2002, the acquisition of all Commercial Off-the-Shelf Products (COTS) IA and IA-Enabled products (see 5 FAM 913 for examples of these products) shall be limited only to those that have been validated in accordance with one of the three programs specified below:

   (1) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

   (2) National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Program; or

   (3) The NIST Federal Information Processing Standard (FIPS)

Cryptographic Module Validation Program (CMVP).

c. For all classified systems procured **prior** to July 1, 2002, all **new** IA and IA-enabled IT products must be validated in accordance with one of the three programs specified in paragraph a above.

d. The validation of COTS IA and IA-enabled IT products will be conducted by a NIAP accredited Common Criteria testing Laboratory (CCTL). This is the product vendor's responsibility.

e. The acquisition of all U.S. Government Off-the-Shelf (GOTS) IA and IA-Enabled products to be used on classified systems shall be limited to products that have been evaluated by NSA, or in accordance with NSA-approved processes.

f. COTS or GOTS IA and IA-Enabled IT products acquired **prior** to July 1, 2002 shall be exempt from the policies contained in this section. However, the policy that was in effect at the time of that procurement still applies. Automated information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions should be considered as replacement upgrades at the earliest opportunity.

g. Full and immediate compliance with NSTISSP No. 11, as reflected in this section, may not be possible. In such cases, program managers need to obtain a CIO approved Deferred Compliance Authorization (DCA). Information on the procedures for obtaining a DCA is contained in 5 FAM 915.15-4. Additional guidance regarding this process is available by contacting IRM's Office of Information Assurance (IRM/IA) (email address is InformationAssurance@state.gov).

h. IRM/IA is responsible for managing and overseeing this process as it involves all non-SCI (Sensitive Compartmented Information) classified systems. DS/SI/IS is responsible for all SCI classified systems.

5 FAM 915.15-4 Deferred Compliance Procedures for the Acquisition of Information Assurance (IA) Products and IA-Enabled Products for Classified Systems

(CT:IM-101; 12-08-2008)

a. All requests for deferred compliance for COTS IA and IA-Enabled products to be used on classified systems shall use the Department's Deferred Compliance Authorization (DCA) process.

b. The issuance of a DCA applies only to environments not requiring the encryption of classified information. A DCA will not be submitted for encryption products. Encryption products for protecting classified information will be certified by *the National Security Agency (*NSA*)*, and

encryption products intended for protecting sensitive information will be certified in accordance with NIST FIPS 140-2.

c. A DCA is applicable only to the acquisition of a specific COTS product for a specific application within the Department IT enterprise. It does not constitute blanket approval for future acquisitions of the same product and does not obviate the requirement for the system owner to obtain necessary certification and accreditation approval for the application or system in which the product will be used prior to its operational use. A DCA shall be approved for no more than one calendar year from the effective date of approval. A record of all DCAs will be included in the System Security Plan documentation.

d. Requests for a DCA will be sent by official memorandum (domestically) or telegram (abroad) from the system owner directly to the IRM/IA - Chief Information Security Officer (CISO). The memorandum or telegram should contain the information listed below and include as much detail as possible to support the request:

   (1) A description of the intended application and type of product needed;

   (2) Details of why an evaluated product is not being procured (e.g., no products of this type have been evaluated, or an explanation as to why available evaluated products do not meet user's functional or security requirements);

   (3) Product information, ideally the product's Security Target (i.e., the security claims being made by the vendor), and evidence (as documented by a National Information Assurance Partnership (NIAP) accredited Common Criteria Testing Laboratories (CCTL) testing facility, that the product's features and assurances are adequate for the intended application;

   (4) The quantity of product that is being acquired;

   (5) A statement that the requesting system owner will, as a condition of purchase, require the product and its associated Security Target to be submitted by the vendor for evaluation and validation to a Common Criteria Testing Laboratory accredited by the NSA/NIST NIAP Evaluation and Validation Program or a member nation recognized under the International Common Criteria for Information Technology Security Evaluation Security Mutual Recognition Arrangement; and

   (6) The authorization status of your system.

e. A telegram, memo, or email will be sent by IRM/IA to the requesting system owner acknowledging receipt of the DCA request and the start of the process. Because DCAs are handled on a case-by-case basis,

timelines may vary.

f. IRM/IA will complete a risk estimate detailing the mission impact of the request.

g. Upon completion of the above, the Chief Information Officer (CIO) will send an official memorandum (domestically) or telegram (abroad) via the CISO to the requesting system owner detailing the final decision. If the DCA is approved, the domestic system owner will have 10 working days to endorse the memorandum, in writing, acknowledging his or her understanding and acceptance of the decision, make a copy of the endorsed memorandum for the record, and return the original memorandum with endorsement to the CISO. Abroad, within 10 working days of receipt of the DCA, the system owner will send a telegram to the CISO acknowledging acceptance of the decision and terms/conditions, if any. The system owner must retain copies of all DCA documents for future reference and possible inspection.

NOTE: The Certifiers and Accreditors of systems are relying on the security features and assurances of a product submitted and approved for a DCA. The system owner should recognize that the security claims of the product have yet to be independently validated and therefore, an Interim Approval to Operate (IATO) rather than Approval to Operate (ATO) may be issued for these systems.

h. In the event an installed product fails to meet established validation and certification testing requirements during the period of the authorized DCA, it is recommended that ISSOs take steps to remove the product from classified systems falling under their purview. The CIO has the option of authorizing continued use of the failed product and accepting the risk of continued use, but should mandate follow-on actions that will ensure that the product is evaluated and validated for use on a national security system. Such decisions should be formally documented and included in the overall system certification and accreditation documentation.

i. The DCA approving authority (CIO) will review and approve the DCA and submit the DCA documentation to the CNSS Secretariat through the Information Assurance Directorate (IAD) of the National Security Agency.

5 FAM 916 APPROVALS AND DOCUMENTATION REQUIREMENTS FOR IT ACQUISITIONS

(CT:IM-101; 12-08-2008)

The requirements for approvals and documentation for IT acquisitions are

described in the following dollar threshold ranges (see Exhibit 916 for a summary of these requirements):

(1) **$0 through $100,000 (Simplified Acquisition Threshold)**: The responsible requiring and procurement offices will provide all necessary reviews and approvals; no other reviews/approvals are required. No specific documentation is required, however it is recommended that a statement of need/requirements should be prepared to justify the acquisition. Justification is required, however, for sole source. (Go to *14* FAH-2 H-212, Simplified Acquisition Methods for more information on simplified acquisition procedures.)

(2) **$100,001 through $9,999,999**: The Office Director within the bureau or office requiring the acquisition shall review/approve the IT acquisition request to assure its accuracy and completeness and shall submit the request to A/LM/AQM. In addition, the following documents must be completed and retained by the requesting office:

(a) Statement of Work (SOW) – (See *14* FAH-2 H-340, The Statement of Work for guidance and procedures);

(b) Simplified Benefit/Cost Analysis (BCA) - (See 5 FAM 660, Benefit Cost Analysis (BCA) and 5 FAH-5 H-620, Benefit Cost Analysis Process);

(c) Procurement Request Package (PRP) - (See *14* FAH-2 H-330, Procurement Request Package); and

(d) Justification for Other Than Full and Open Competition (JOFOC) – sole source or a specific make and model specifications (See *14* FAH-2 H-226, Justifications, Approvals, and Notice Requirements for Other Than Full and Open Competition).

(3) **$10,000,000 through $29,999,999**: The Deputy Assistant Secretary of the requiring office shall review/approve the IT acquisition request prior to submitting the request to A/LM/AQM. The CIO also approves, in writing, all IT acquisitions with a value of $10 million or more per fiscal year, before submitting the request to AQM. The Departmental Competition Advocate's approval is required at the $10 million level when the acquisition is using other than full and open competition and the Head of the Contracting Activity (HCA) has a Competition Advocate. For acquisitions, which are using other than full and open competition and there is no HCA Competition Advocate, the Department's Competition Advocate approval is required at the $500,000 threshold. The documentation required for this level is equal to what is identified above in

paragraph "b" except that a full BCA is required for IT acquisitions over $10 million. (See 5 FAM 660, Benefit Cost Analysis (BCA).)

(4) **$30,000,000 or above**: The Assistant Secretary in the requiring office's parent bureau is required to review/approve the IT acquisition request prior to submitting to A/LM/AQM. AQM will coordinate the review/approval of the IT acquisition request with IRM (CIO), the Chief Financial Officer (CFO), and the Procurement Executive (A/OPE). The documentation required for this level is equal to what is identified above in paragraph (3).

5 FAM 917 ACQUISITION OF TELEPHONE SYSTEMS

5 FAM 917.1 Unclassified Domestic Telephones

(CT:IM-64; 06-20-2005)

a. Bureaus must acquire all telephone and related adjunct systems and services for unclassified domestic use through IRM's Telecommunication, Wireless and Data Services Division (IRM/OPS/ITI/TWD).

b. Bureaus must obtain the approval of DS' Countermeasures Program Division (DS/ST/CMP) for the acquisition of speakerphones prior to the submission of Telecommunications Service Requests (TSRs) to IRM's Business Operations Management Branch (IRM/OPS/ITI/TWD/BOM).

5 FAM 917.2 Telephones Abroad

(CT:IM-101; 12-08-2008)

a. Bureaus and posts must acquire only telephones for use abroad that conform to the technical and security standards defined in 5 FAM 500, Telecommunications. The requesting organization is responsible for obtaining the approvals identified below in paragraphs b, c and d.

b. The Foreign Post Telephones Branch of IRM's LAN WAN Services Division (IRM/OPS/ITI/LWS/FPT) must approve the acquisition of new non-cryptographic security devices for telephones and telephone systems.

c. *The Technical Surveillance Countermeasures Branch in Diplomatic Security, Office of Security Technology, Countermeasures Program Division (*DS/CMP/TSC*)* must approve requests for telephone and PBX (private branch exchange) equipment for posts that are: designated "high" or "critical" technical threat in the composite threat list. Future equipment installation within CAA must be procured, shipped, stored, and installed per the requirements set forth in 12 FAH-6 H-551, Non-secure

Telephone Systems.

d. The local Regional Information Management Center (RIMC) and IRM/OPS/ITI/LWS/FPT must approve all acquisitions of key systems, multi-button telephone instruments, single line telephone instruments, and other telephone station equipment.

e. See 5 FAM 528, Telephone Funding, which describes how telephone projects are funded abroad.

5 FAM 917.3 Acquisition of Secure Terminal Equipment (STE)

(TL:IM-42; 09-26-2003)

a. Secure Telephone Units, Third Generation (STU-III) are being replaced by Secure Terminal Equipment (STE). IRM's Systems Integrity Division (IRM/OPS/ITI/SI) will exhaust the present supply of STU-III telephones upon receipt of a justification memorandum. Each request will be considered on a case-by-case basis since supplies are limited. Requests for specific makes or models cannot be accommodated.

b. Posts, bureaus, or offices requesting a specific make or model will contact IRM/OPS/ITI/SI for assistance in determining equipment to meet requirements and for procurement of those units (with post, bureau, or office funding) through the NSA contract. However, no new STU-III purchases will be made. Instead, the new STE must be purchased. Post and bureau personnel may obtain STE using funding through IRM/OPS/ITI/SI/CSB.

c. The requesting post, bureau, or agency must provide the funds for procurement of the new STE units should the STU-III inventory, maintained by IRM/OPS/ITI/SI/CSB, become depleted. IRM/OPS/ITI/SI will continue to assist the requesting entity for the purpose of maintaining inventory control for this family of Cryptographic Controlled Items (CCI) in this case.

d. Bureaus must submit a Telephone Service Request (TSR) to IRM/OPS/ITI/TWD/BOM to have a line changed to accommodate a STU III (analog) instrument. An ISDN line is recommended for a STE instrument.

5 FAM 917.4 Acquisition of Secure Digital Devices (SDD)

(TL:IM-42; 09-26-2003)

a. Posts, bureaus, or offices must submit their requirements for all STU-III SDDs, whether for use domestically or abroad, to IRM/OPS/ITI/SI.

IRM/OPS/ITI/TWD will work with the post, bureau, or office to determine the proper equipment needed to satisfy their requirements and arrangements for maintaining the equipment after installation. Domestic requirements are the responsibility of IRM/OPS/ITI/TWD/DTD; requirements abroad are the responsibility of IRM/OPS/ITI/LWS/FPT.

b. The post, bureau, or office will provide funding for this equipment. The STU-III Program Office assists the post, bureau, or office by procuring the unit(s) through NSA contracts and includes the devices in the Department's worldwide cryptographic database.

5 FAM 917.5 Acquisition of Secure Facsimile (FAX) Equipment

(CT:IM-101; 12-08-2008)

a. IRM/OPS/ITI/TSS maintains a list of NSA-approved, TEMPEST-certified, and Department-approved FAX equipment. Approval for operation of a classified FAX device by a Departmental office is contingent upon written approval by S/ES-O prior to installation of the FAX. The *chief* of *mission* (COM), Regional Security Officer (RSO), and Information Management Officer (IMO) approve installation and operation of TEMPEST FAX machines for offices abroad. Only the COM and RSO approve tenant agencies.

b. Posts, bureaus, or offices requesting FAX machines must provide funding for the machines.

5 FAM 918 ACQUISITION OF TELECOMMUNICATIONS CIRCUITRY

5 FAM 918.1 Domestic Circuits

(TL:IM-42; 09-26-2003)

Bureaus must contact IRM/OPS/ITI/TWD/DTD to obtain domestic voice and data circuitry. IRM/OPS/ITI/TWD/DTD will verify user requirements and make a recommendation for the appropriate network service, data communications equipment, and encryption devices. Bureaus must submit a Telephone Service Request (TSR) to IRM/OPS/ITI/TWD/BOM to order services and equipment. Type Two Encryptors may be ordered through IRM/OPS/ITI/TWD. Type One Encryptors must be purchased through IRM/OPS/ITI/SI/CSB.

5 FAM 918.2 Overseas Circuits

(CT:IM-101; 12-08-2008)

a. Two major steps are required before bureaus can acquire non-voice telecommunications circuitry between the Department and posts abroad, and between posts. IRM/M/CST/LD/EA is the liaison office that bureaus must work through to acquire circuits abroad. Circuits abroad must be acquired through coordination with IRM/M/CST/LD/EA and IRM/OPS/ENM/NED. Bureaus must acquire non-DTS circuitry abroad through IRM/OPS/ENM and IRM/M/CST.

b. Telecommunication circuitry services, with the exception of telephone circuits, whether international (*United States* to post) or OCONUS (outside continental *United States;* i.e., post to post), will be **end-to-end**.

c. Posts are responsible for acquiring local telephone service (i.e., the circuitry needed for communications within the host country). Local telephone service may consist of individual PBX trunks, multi-channel, digital PBX trunks, or local loops. Trunks traditionally connect from the Local Exchange Carrier (LEC) to the post PBX. Local loops that connect post extensions to residences or remote buildings can also be obtained from the LEC. Posts are responsible for acquiring trunks and/or local loops by awarding contracts or using simplified acquisitions in accordance with the FAR and DOSAR.

5 FAM 919 UNASSIGNED

5 FAM EXHIBIT 915
IT ACQUISITIONS CHECKLIST

(TL:IM-43; 10-09-2003)

U.S. Department of State

IT ACQUISITIONS CHECKLIST

[THIS CHECKLIST IS TO BE MAINTAINED WITH THE ACQUISITION REVIEW FILE]

DATE *(mm-dd-yyyy)*: _____

PROJECT NAME: _____

NAME OF PROJECT MANAGER: _____

BUREAU/POST: _____

LIFECYCLE OF EQUIPMENT (YRS): _____

ESTIMATED COST OF EQUIPMENT: _____

	YES	NO
1. Will the IT acquisition provide hardware, software, or services that will support core/priority mission functions that need to be performed by the Office/Department? *	_____	_____
2. Have all pertinent national and Department security requirements been considered if the IT acquisition is going to process classified information or is intended to be located in a sensitive or Controlled Access Area (CAA)?	_____	_____
3. Is this IT acquisition necessary because no alternative private sector or government source can effectively support the mission function? *	_____	_____
4. Have the work processes, which will be supported by the acquired IT, been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology? *	_____	_____
5. Has the IT acquisition demonstrated a projected return on the investment that is clearly equal to or better than alternative uses of available public resources? *	_____	_____
6. Is the IT acquisition consistent with established Department information architecture? *	_____	_____
7. Has the IT acquisition considered ways to reduce risks by:		
(a) avoiding custom-designed components?	_____	_____
(b) using fully tested pilots, simulations or prototype implementations before going production?	_____	_____
(c) established clear measures and accountability for project progress? and	_____	_____
(d) securing substantial involvement and buy-in throughout the project from the program officials who will use the system? *	_____	_____
8. Will the acquisition provide IT that will be implemented in phased, successive chunks as narrow in scope and brief in duration as practicable, each of which solves a specific part of an overall mission problem and delivers a measurable net benefit independent of future chunks? *	_____	_____
9. Does the acquisition		
(a) employ an acquisition strategy that appropriately allocates risk between government and contractor?	_____	_____
(b) effectively use competition?	_____	_____
(c) ties contract payments to accomplishments?	_____	_____
10. Does the Statement of Need show a clear relationship between identified need(s) and Department mission?	_____	_____

* OMB Memorandum 97-02, 10/25/96 ("Raines Rules")

DS-915
10-2003

Page 1 of 2

	YES	NO
11. Is software being acquired or developed?		
(a) Off-the-shelf?	_____	_____
(b) To be developed under contract	_____	_____
(c) To be developed in-house with sufficient resources identified?	_____	_____
12. Will contractor provided IT services require security clearances or investigations for contractor access to specifically designated SBU information on Department systems?	_____	_____
13. Are software tools/techniques proposed to assure programmer productivity and software quality?	_____	_____
14. Have software conversion and maintenance been factored into overall system costs?	_____	_____
15. Will the needed hardware be compatible with the current operating system?	_____	_____
16. Are sufficient funds, including out year funding, identified and documented?	_____	_____
17. If any of the following are present, give brief explanation in comments sections.		
(a) Restrictive elements such as compatibility limited requirements;	_____	_____
(b) Sole source or other than full and open competition;	_____	_____
(c) 8(a) set-aside; or	_____	_____
(d) Other issues not addressed.	_____	_____
18. Does this acquisition need to satisfy any recommendations from OIG?	_____	_____
19. Does this acquisition need to satisfy any recommendations from GAO?	_____	_____
20. Competitive Sourcing: Have you analyzed the estimated cost and effectiveness of in-house performance vs. contracting out?	_____	_____
21. State First: Before sending acquisition dollars to another agency, did you consult with A/LM/AQM?	_____	_____
22. Performance-Based Contracting: With this be a performance-based contract? If you require assistance, did you contact A/LM/AQM? (Note: A waiver is required if performance based services will not be acquired. Contact A/OPE for more information.)	_____	_____
23. Have section 508 requirements been addressed?	_____	_____
24. Are user requirements in I-TIPS? Will updates occur?	_____	_____
25. Is the acquisition in Department forecasting or planning documents (e.g., Master Buy Plan, Preliminary Forecast Plan)?	_____	_____
26. Has market research been performed and the results coordinated with the Contracting Officer or General Service Officer?	_____	_____
27. Has an acquisition plan been processed and approved in accordance with Departmental policy if the estimated value of the acquisition is $5M or above?	_____	_____
28. Does the acquisition incorporate any lessons learned and/or best practices?	_____	_____
29. COMMENTS: Substantiate as necessary the answers above.		

DS-915

Page 2 of 2

5 FAM EXHIBIT 916
MATRIX FOR REVIEW/APPROVAL OF THRESHOLDS AND DOCUMENTATION REQUIREMENTS FOR ALL IT RESOURCE ACQUISITIONS

(TL:IM-42; 09-26-2003)

$ THRESHOLDS (*)	$0 - 100,000 Simplified Acquisitions, includes micro purchases	$100,001 through $9,999,999	$10,000,000 through $29,999,9990	$30,000,000 and above
1ST LEVEL REVIEW	RESPONSIBLE REQUIRING OFFICE	OFFICE DIRECTOR IN PARENT OFFICE	DEPUTY ASS'T SEC.IN PARENT BUREAU	ASS'T SEC. IN PARENT BUREAU
2ND LEVEL REVIEW	RESPONSIBLE PROCUREMENT OFFICE, as necessary	A/LM/AQM	A/LM/AQM IRM (CIO) ($10 Million or more per fiscal year) Competition Advocate ($10 million and over – if competition is limited)	A/LM/AQM, IRM (CIO) Competition Advocate ($10 million and over – if competition is limited) A/OPE ($50 million and over – if competition is limited) CFO
DOCUMENTATION REQUIREMENTS	Justification, if competition is limited. (It is recommended that a statement of need/requirements should be prepared to support the acquisition.)	SOW PRP Simplified BCA JOFOC [If competition is limited.]	SOW PRP BCA(Simplified BCA below $10 million) JOFOC [If competition is limited.]	SOW PRP BCA JOFOC [If competition is limited.]

(*) DOLLAR THRESHOLDS INCLUDE ALL OPTIONS.

ACRONYMS

A/LM/AQM Bureau of Administration, Logistics Management, Office of Acquisition Management
A/OPE Office of the Procurement Executive
BCA Benefit/Cost Analysis
CFO Chief Financial Officer
CIO Chief Information Officer
DAS Deputy Assistant Secretary
IRM Bureau of Information Resources Management
JOFOC Justification for Other Than Full and Open Competition

PRP Procurement Request Package
SOW Statement of Work