CHAPTER 12, PART 1
SECURITY REQUIREMENTS FOR CPIC

1 BACKGROUND

The Clinger-Cohen Act of 1996 requires that Federal agencies institute a disciplined approach to managing and controlling Information Technology (IT) investments. The Office of Management and Budget updated Circular A-130, "Management of Federal Information Resources" also mandates the disciplines of Capital Planning and Investment Control (CPIC) and information system security. These requirements, combined with the newly enacted Federal Information Security Management Act (FISMA), have now established a clear and convincing need for a systematic capital planning and investment process in each USDA agency and staff office.

For the past several years, the Office of Management and Budget has pressed agencies and staff offices to take successive steps to demonstrate their ability to more clearly plan and articulate their Information Technology (IT) costs. A key element of IT planning is the costs associated with an effective Security Program and Infrastructure.

The material in this chapter, including Attachment A, is intended to be a reference document to be used in maintaining a comprehensive planning process for the security costs of information systems within each agency/mission area. Actions taken during the CPIC process support the development of Security Plans, FISMA reporting and security administration within agencies and staff offices throughout the System Life Cycle. Attachment A contains information on cost categories, strategic security criteria and information on security requirements for each CPIC phase. Implementation of a formal IT Capital Planning and Investment Control Process is required by law and is essential for making better security investment and program decisions.

2 POLICY

All USDA agencies and staff offices will institute a formal Capital Planning and Investment Control (CPIC) process and execute all CPIC responsibilities. CPIC will be used to plan costs for both the

Overall Security Program and all Major Information Technology (IT) investments.

Each agency will follow the instructions in the Responsibilities Section below in planning costs for security programs and investments. Cost data will be entered into the IT Portfolio Management System on annual basis or as an investment is initiated. These figures will be updated as the figures change in the System Life Cycle or on an annual basis for the Overall Security Program. Attachment A provides spreadsheets that will be downloaded for cost figures and uploaded to the IT Portfolio Management System Resource Library when completed.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. CS will monitor all approved exceptions.

3 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Provide guidance and tools and strategies to assist USDA agencies in complying with the security requirements of the Capital Planning and Investment Control (CPIC) process;

(2) Work with agencies and staff offices to ensure that they utilize the IT Portfolio Management System to plan security costs for Major IT Investments and their overall security program;

(3) Perform reviews of all Major IT Investments to ensure that security requirements have been met and costs

have been adequately formulated; provide recommendations to the CIO and agencies for security improvements; and

(4) Perform oversight reviews of agencies/staff offices to ensure compliance with this policy.

b Agency Chief Information Officer will:

(1) Establish and implement a formal Capital Planning and Investment Control (CPIC) process outlined in Attachment A to define security requirements for all Major IT Investments; costs for the Overall Security Program will also be developed in accordance with Attachment A;

(2) Ensure that Agency Investment Portfolio Managers, ISSPMs and field security representatives are familiarized with the CPIC Security Requirements for all phases;

(3) Ensure that security costs are entered into the IT Portfolio Management System for all Major IT Investments and the Overall Security Program; updates will be made to costs on a routine basis to ensure that they reflect the most recent information available;

(4) Ensure that all Major IT Investment Project Teams include an agency security representative, preferably the agency ISSPM; and

(5) Review the security requirements of all Major IT Investments to ensure that they comply with this policy.

c The Agency Information Systems Security Program Managers will:

(1) Become thoroughly familiar with all CPIC security requirements;

(2) In conjunction with the business owner and developer, assist in the development of security requirements and costs for all Major IT Investments; develop the Overall Program Security costs;

(3) In coordination with the agency Investment Portfolio Manager, ensure that security costs are entered into the IT Portfolio Management System for all Major It Investments and the Overall Security Program;

(4) Participate as a Security Representative for Major It Investment Teams, as required; and

(5) Participate in the development of waiver requests to this policy, as required.

-END-

ATTACHMENT A

Guide to Capital Planning and Investment Control for the Cyber Security Infrastructure

Table of Contents

Introduction

The Clinger-Cohen Act of 1996, the most significant IT reform of the last decade, requires that Federal agencies institute a disciplined approach to managing and controlling Information Technology (IT) investments. The Office of Management and Budget recently updated Circular A-130, "Management of Federal Information Resources" to reflect the disciplines of capital planning and information system security in order to reinforce the critical nature of Capital Planning and Investment Control (CPIC). This legislation combined with the newly enacted Federal Information Security Management Act (FISMA) that replaced GISRA, have now established a clear and convincing case for systematic capital planning and investment process. USDA is one of the leaders in implementing this process and intends to keep moving forward with this initiative.

For the past several years, OCIO, in response to the Office of Management and Budget, has pressed agencies and staff offices to take successive steps to demonstrate their ability to more clearly plan and articulate their Information Technology (IT) costs. A key element of IT planning is the costs associated with an effective Security Program and Infrastructure.

This guide is intended to be a reference document to be used in maintaining a comprehensive planning process for the security costs of information systems within each agency/mission area. The actual CPIC Spreadsheets output of this process remains unchanged, however we eliminated Figure 3, Physical Security Operations Resources Base/Budget Requirements Detailed Back Up Sheet. In addition, we added information for the Pre-Select Phase to include security requirements, definitions, and scoring. Recognizing that agencies have been actively engaged in the process for a while, we streamlined the information into subject areas and tables. We have not abolished the requirements to perform a comprehensive security analysis and plan/update detailed costs during the life cycle for both the overall agency program and each major investment.

Actions taken during the CPIC process will support and require the development of Security Plans, the FISMA/GISRA reporting and security administration within agencies and staff offices throughout the System Life Cycle. Each agency Chief Information Officer with their Information System Security Program Manager is requested to take this opportunity to actively engage in this process and develop realistic security costs. Implementation of an IT Capital Planning and Investment Control Process is required by law and is essential for making better investment and program decisions.

Point of Contact

This guide is supported and maintained by the USDA Office of the Chief Information Officer's (OCIO) Associate CIO for Cyber Security. For further information about this guide, please contact the Cyber Security Representative for your Agency or your Cyber Security Liaison.

Security infrastructure and Security Objectives

A security infrastructure is a model for integrating security services, mechanisms, objects and management functions, across multiple hardware and software platforms and networks. The infrastructure supports the strategy for providing end-to-end protection of applications and information within the Department.

The overall objectives of security that apply to all Capital Planning Phases are defined below:

- Use of new technologies to sustain, not erode, the privacy protections provided in statutes
- Protection of Federal computer resources commensurate with the risk of harm resulting from misuse of unauthorized access to such systems
- Security risks and incidents managed in a way that complements and does not unnecessarily impede agency business operations

- An overall strategy to manage security is essential and should be based on a cycle of risk management that identifies significant risks, clearly establishes responsibility for reducing them and ensures that risk management remains effective over time

Security Analysis

The first step in CPIC planning of Security Costs is to conduct a Security Analysis. To ensure success, an IT investment must include accurate, reliable, and up-to-date data on project costs, benefits and risks. This includes a determination on the criticality of the system and the value and sensitivity of the data. The security analysis should be performed by the business owner in coordination with the agency Information Systems Security Program Manager (ISSPM) and other security specialists to ensure that estimated costs are based on experience and market research. The ISSPM subsequently works in tandem with the agency Portfolio Manager to ensure detailed backup sheets are entered into the I-TIPS Resource Library. All data entered should be representative of the anticipated/actual costs for a program or initiative.

Security Strategic Investment Criteria

The Executive Information Technology Investment Review Board (EITIRB) is responsible for the approval and management of the USDA IT Investments. Each investment is rigorously reviewed against approved strategic investment criteria. The strategic investment criteria for the evaluation of the Cyber Security Infrastructure have been outlined in the section below. Specifically, the factors applicable to each investment phase have been determined for the Pre-Select, Select, Control, Evaluate and Steady State phases. This process is used to ensure that the investment is sound and remains on target throughout its life cycle. OCIO has developed the following evaluation factors to be used in the Capital Planning and Investment Control (CPIC) cyber security infrastructure review and oversight process for new or existing investments in the USDA's Portfolio. The security criteria have been expressed in five CPIC phases as they are followed during the investment scrutiny process. The criteria below will be used to evaluate existing investments in the USDA Portfolio and all new investments received each fiscal year. In addition, CS has included a Security Scoring Chart to further clarify scoring for investments in all phases. Investments must have a score of 4 or 5 to be recommended for movement to the next phase in the CPIC process.

SECURITY SCORING CHART

Score	Color	Remarks
5	**GREEN**	**All Security Requirements for Phase Met**
4	**GREEN**	**All Security Requirements for Phase Met, Approved Conditionally, 60-90 days to correct omissions**
3	**YELLOW**	**Borderline Investment, Major Sec. Omissions (Fix Before Proceeding to Next Phase)**
2	**RED**	**Did not meet Security Requirements – Recommend Remaining In Phase – Some attempt made to outline security**
1	**RED**	**Did not meet Security Requirements – Recommend Remaining In Phase – No attempt made to outline security**

SECURITY INVESTMENT CRITERIA

Objective: To protect the availability, confidentially and integrity of system assets by maximizing security safeguards and performance, while controlling vulnerabilities.

Data Sensitivity High

Safeguards High

Data Sensitivity Low

Safeguards Low

Elements of a Security Protection

Pre-Select Phase:	Initial Security Plan (Draft) User Requirements Defined; Preliminary Risk Assessment performed Data Sensitivity Identified
Select Phase:	Select Security Analysis Completed Majority of Security Plan Completed Risk Assessment/Mitigation's done
Control Phase:	Control Security Analysis Completed Security Cost and Performance Goals Reviewed Certified and Accredited System, ST&E done Disaster Recover Plan Completed
Evaluation Phase:	Evaluation Security Analysis Completed Security Post Implementation Review with IV&V Disaster Recovery Plan Tested
Steady State:	Upgrades/Patches, Maintenance/Production Record Certification and Accreditation Review Conducted Disaster Recovery Plan Tested Annually System Retirement and Disposal Activities Completed (no scored)

Security Evaluation Factors

Pre-Select Phase:	Have Pre-Select security documents been prepared? Has a project plan been developed showing security target dates?
Select Phase:	Has a Select security analysis been conducted?

	Has a Security Plan been completed? Are security risks identified and mitigation strategies proposed?
Control Phase:	Has a Control security analysis been conducted? Have estimated security costs been compared to actual costs? Have security goals and measures been established? Has a review of risks and mitigations been done?
Evaluation Phase:	Has a Evaluation security analysis been conducted? Is the system security functioning as anticipated? Are additional security countermeasures needed to protect assets?
Steady State:	Has a Steady State security analysis been conducted? Are system/application patches and upgrades being applied in a timely manner? Are security controls being maintained? Have retirement and disposal actions been taken, if necessary, to protect sensitive data?

Rating Award Basis

Pre-Select Phase:

5 Pre-Select Security Analysis has been completed to include draft Security Plan, Data/User Requirements, Preliminary Risk Assessment, Data Sensitivity determined and security officer has been identified. [Green]

4 Pre-Select Analysis has been partially completed with omissions and submitted with CPIC package. Conditional approval granted; security omissions must be corrected within 60-90 days. [Green]

3 A project plan has been developed showing the due and completion dates of all Security Analysis required documents that accompanies CPIC submission. Major security omissions; must be corrected prior to proceeding to next phase. [Yellow]

2 Investment did not meet security requirements. Some attempt made to address security; remain in phase. [Red]

1 Investment did not meet security requirements. No attempt made to address security; remain in phase. [Red]

Select Phase:

5 Select Security Analysis completed to include information on all security analysis factors, Security Plan completed appropriate risks identified, mitigation strategies sound, a validated costs/benefit analysis for security performed with constraints/assumptions, and security complements departmental architecture.
[Green]

4 Select Analysis has been partially completed with omissions and submitted with CPIC package. Conditional approval granted; security omissions must be corrected within 60-90 days. [Green]

3 Select security analysis done and submitted with CPIC package. Major security omissions; must be corrected prior to proceeding to next phase. [Yellow]

2 Investment did not meet security requirements. Some attempt made to address security; remain in phase. [Red]

1 Investment did not meet security requirements. No attempt made to address security; remain in phase. [Red]

Control Phase:

5 Control Security Analysis completed; security costs are accurately accounted for, controlled, managed; original cost estimate is current; detailed performance goals/measures established; ST&E done; Certification and Accreditation of System done and Disaster Recover Plans completed. [Green]

4 Control Security Analysis has been partially completed with omissions and submitted with CPIC package. Conditional approval granted; security omissions must be corrected within 60-90 days. [Green]

3 Control security analysis done and submitted with CPIC package. Major security omissions; must be corrected prior to proceeding to next phase. [Yellow]

2 Investment did not meet security requirements. Some attempt made to address security; remain in phase. [Red]

1 Investment did not meet security requirements. No attempt made to address security; remain in phase. [Red]

Evaluation Phase:

5 Evaluation Security Analysis completed. Agency has done commendable job in conducting the post-implementation security reviews with an IV&V, DR Plan tested, reviews report attainment of the goals, benefits, and expectations that were originally envisioned for the project. [Green]

4 Evaluation Security Analysis has been completed with omissions and submitted with CPIC package. Conditional approval granted; security omissions must be corrected within 60-90 days. [Green]

3 Evaluation security analysis done and submitted with CPIC package. Major security omissions; must be corrected prior to proceeding to next phase. [Yellow]

2 Investment did not meet security requirements. Some attempt made to address security; remain in phase.
[Red]

1 Investment did not meet security requirements. No attempt made to address security; remain in phase. [Red]

Steady State Phase:

5 Steady State Security Analysis completed. System/application upgrades and patches being applied, security controls being maintained and high/medium vulnerabilities promptly corrected, Annual review of the Security Controls, Certification and Accreditation of System and Disaster Recover Plan conducted for life of system. [Green]

4 Steady State Security Analysis has been partially completed with omissions and submitted with CPIC package. Conditional approval granted; security omissions must be corrected within 60-90 days. [Green]

3 Steady State Security Analysis done and submitted with CPIC package. Major security omissions; must be corrected prior to proceeding to next phase. [Yellow]

2 Investment did not meet security requirements. Some attempt made to address security; remain in phase.
[Red]

1 Investment did not meet security requirements. No attempt made to address security; remain in phase. [Red]

CPIC Phase Security Requirements

The following are security requirements for all phases in the Capital Planning and Investment Control (CPIC) process.

Pre-Select Phase:

The Pre-Select Phase provides a process to assess a proposed investment's support of agency strategic and mission needs and to provide conceptual information to further support investment action. It is during this phase, that the business/mission needs are identified and relationships to the Department and/or agency strategic planning efforts are established. There are significant information requirements and a potential expenditure of funds in the preliminary planning phase to prepare for review and selection of IT investments. The Pre-Select Phase provides an opportunity to focus efforts on the initiative's concept. It also allows project teams to begin the process of defining security and business requirements and associated system performance metrics, performance measures, benefits, and costs, as well as subsequent completion of a business case and project planning efforts in preparation for inclusion in the Department's investment portfolio.

Entry Criteria

Prior to entering the Pre-Select Phase, investments must have a concept to address a mission need that is anticipated to include an IT component and meet at least one of the threshold criteria identified in the overall CPIC guidance.

Process

During the Pre-Select Phase, mission analysis results in the identification of a mission need necessitating consideration of an IT alternative. The mission analysis and corresponding development of the Mission Needs Statement are closely linked to the strategic planning process of the USDA and sponsoring agency. Following mission analysis, the Functional Manager further develops the proposed solution's concept. Objectives are established, evaluation criteria are defined, concept alternatives are identified, and an alternative analysis approach is documented as part of the concept management plan to support concept and mission need approval. A preliminary business case with budget estimates and associated CBA is also completed in addition to a Pre-Select Security Analysis.

The following Security Analysis steps are required in the Pre-Select phase:

User Requirements Definition The agency Information System Security Program Manager (ISSPM) will work with the business owner to fully define the security requirements. How important is the information protection to their mission? How many users will be accessing the system/application (internal, external, trusted partners, clients, public)? What are peak time periods of user activity? When does the customer need security to be operational?

System Security Plan The agency ISSPM needs to work with the business owner to establish adequate security measures for each major investment, taking into account the security of all systems in which the new application/system will operate. The plan shall be consistent with guidance issued by NIST 800-18. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act and each CPIC Investment Proposal. At this point, a skeleton Security Plan will be prepared with draft information available that will be refined and updated during the CPIC process.

Sensitivity of Information The agency business owner will take action to determine the sensitivity of the information. Sensitive information is defined as any information, the loss, or unauthorized access to or modification of which could adversely affect the national interest or conduct of federal/agency programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a(the privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. The Computer Security Act of 1987 (P.L. 100-235) was enacted to create "a means for establishing minimum acceptable security practices" for federal unclassified computer systems. The Act also emphasizes that federal information requires protection against unauthorized modification or destruction, as well as unauthorized disclosure. To distinguish systems covered by this law from those used to process national security information, the law uses the term "sensitive". Confusion over this term may have led some agencies to focus their limited computer security resources on determining which systems would be labeled "sensitive". Information owners should use a risk based approach to determine what harm may result if a system is inadequately protected.

The Security Protection Chart (Figure 1) below depicts the factors to be considered and levels of concern for information sensitivity. The higher the sensitivity of information and vulnerabilities identified the greater the need for Security Protection. The intent of the Computer Security Act is to assure adequate protection of all federal IT systems. NIST believes that all agency information requires some degree of protection to provide confidentiality, integrity or availability. Therefore each agency must determine the appropriate level of protection required for their systems including the rationale for identification of sensitive information. Protecting sensitive information means providing security protection based on for
one or more of the following:

- Confidentiality – The system contains information that requires protection from unauthorized disclosure.
- Integrity – The system contains information that must be protected from unauthorized, unanticipated or unintentional modification.
- Availability – The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.

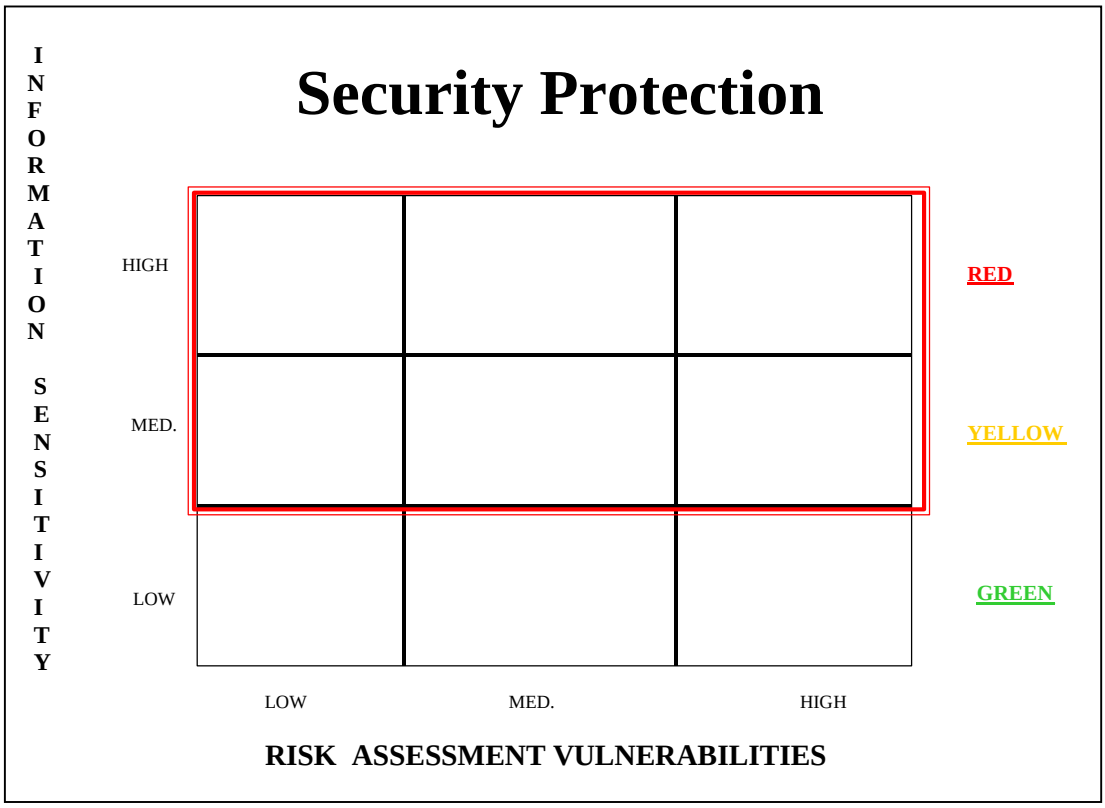

Figure 1

Preliminary Risk Assessment - The ISSPM needs to work with the business owner to assess risk and examine the sensitivity, criticality and value of the system. This process helps determine the need for both general and specialized security controls and provides input into the draft Security Plan.

Exit Criteria

Prior to exiting the Pre-Select Phase, investments must obtain CIO and Executive Information Technology Investment Review Board (EITIRB) approval for the mission need and concept and a security analysis must be in progress. A Pre-Select Security Analysis must have been completed, including the initiation of a Security Plan, determination of information sensitivity, Preliminary Risk Assessment, and selection of a Security Representative on the investment project team. Agency Records Officer has been appoint and the system in accordance with the Electronic Records Management Program.

Select Phase:

Purpose

In the Select Phase, USDA ensures the IT investments that best support the mission and USDA's approach to enterprise architecture, are chosen and prepared for success (i.e., have a good project manager, are analyzing risks, etc.). Individual investments are evaluated in terms of technical alignment with other IT systems and projected

performance as measured by Cost, Schedule, Benefit, and Risk (CSBR). Milestones and review schedules are also established for each investment during the Select Phase.

In this phase, USDA prioritizes each investment and decides which investments will be included in the portfolio. Investment submissions are assessed against a uniform set of evaluation criteria and thresholds. The investment's CSBR are then systematically scored using objective criteria and the investment is ranked and compared to other investments. Finally, the EITIRB selects which investments will be included in the Department's portfolio.

Entry Criteria

Prior to entering the Select Phase, investments must have obtained EITIRB approval for the mission need and concept. The Pre-Select Security Analysis must have been completed, including the initiation of a draft Security Plan, determination of information sensitivity, preliminary risk assessment and selection of a Security Representative on the project team.

Process

The Select Phase begins with an investment concept (approved during the Pre-Select Phase) and moves through the development of the business case, acquisition plan, risk analysis, performance measures, security plan, and a project plan. These plans lay a foundation for success in subsequent phases. The Select Phase culminates in a decision whether to proceed with the investment.

The following Security Analysis steps are required in the Select phase:

Responsibility for Security The agency ISSPM is responsible for assuring that security of each major system/application is assigned to a management official knowledgeable in the nature of the information. This individual should also understand the process supported by the system/application, and the management, personnel, operational, and technical controls used to protect it. The ISSPM will assure that security products and techniques are appropriately used in the system /application. The designated official will be contacted when a security incident occurs concerning the application. This representative may nor may not be the individual participating on the Project Team for Security, but will be responsible for coordinating with the team member to ensure appropriate security protection is proposed or in place for the new investment.

Security Risk Management: Risk management addresses risks that arise from an organization's use of information technology. Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic steps: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results. The agency ISSPM is responsible for developing the appropriate risk assessment and mitigation strategies for all major investments. This includes procedures for conducting a risk assessment, what approach is used or recommended, what type of documentation is maintained, and whether the assessments are based on specific components such as technical, operational and cyber security within a data center or based on the entire organization. Risk mitigation involves the selection and the implementation of security controls used to reduce risk to a level acceptable to management. The risk assessment should discuss the selection of safeguards and risk acceptance, and cost considerations within your security program. Identified risks in the system are considered when making determinations of information sensitivity. Preliminary risk assessments are conducted on a system once a final design has been identified, updated prior to implementation of the system and throughout the production/steady state phases as major changes are made.

Specialized Training Before allowing individuals access to the system, the agency ISSPM will ensure that all individuals receive specialized training focused on their responsibilities and the system rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval system) to formal training (e.g., for an employee that works with a high-risk system.

Personnel Security The agency Information Systems Security Program Manager in coordination with the System Administrator will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. In cases where such controls cannot adequately protect the system or information in it, they will ensure that individuals are screened commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the system and periodically thereafter.

Planning Process and Disposal of Records The agency ISSPM and business owner will work with the departmental Records Officer to ensure that procedures are established for adequate records keeping, especially in the case of electronic records. This includes proper system design and disposition requirements and a plan for maintenance of critical records.

Technical Controls The agency Information Systems Security Program Manager will ensure that appropriate security controls are specified, designed into, tested, and accepted in the system in accordance with appropriate guidance issued by NIST 800-18.

Information Sharing The agency ISSPM will ensure that information shared from the system is protected appropriately, comparable to the protection provided when information is within the application.

Public Access Controls Where an agency's system promotes or permits public access, additional security controls shall be added by the ISSPM and System Administrator to protect the integrity of the system and the confidence the public has in the system. Such controls shall include segregating information made directly accessible to the public from official agency records.

Security Architecture The ISSPM will ensure that the investment security architecture, which all participants trust, will include the logical and physical security controls to appropriately mitigate risks and address the five core information security requirements. These are authentication/identification, access control, data privacy, data integrity, and non-repudiation. The factors to be addressed are: Physical, Network, System, Application and Data Security. The architecture design must be based on a structured risk assessment to ensure implementation costs are commensurate with identified risks and vulnerabilities. In part, it consists of policy formulation to clearly establish operational security guidelines and define exactly what connections are allowed to pass on the network. This includes connections to other systems/applications and networks. The architecture is also composed of coordination of agency firewall implementations to facilitate interoperable encryption of data-flows; secure dial-in communication services from remote locations; and proper management of Internet and Intranet Services.

Security Performance Measures In conjunction with the business owner and or developer, the ISSPM will establish system/application security performance measures that include at a minimum: redundancy, availability, data integrity, confidentiality and security plan effectiveness. The system must, wherever cost effective, operate with full redundancy to ensure no single point of failure could disable the system. The system must restrict disclosure of the information to designated parties, must be protected from errors or unauthorized modification, and must be available within some given timeframe. In addition, the effectiveness of the Security Plan in defining the protections in place should be measured. These measures will include goals for performance in each category.

Cost/Benefit Analysis (CBA) In conjunction with the business owner and or developer, the ISSPM will conduct a cost/benefit analysis, identify and quantify benefits and costs, and prepare estimates for the security to support the investment. Benefits should describe how the investment security enhances the agency ability to meets its mission needs, and they should outline functionality or cost savings. Benefits are defined as a profit, advantage or gain attained by using the security. Cost refers to both the incurred expenses of an investment and its capitalized costs, and can be categorized as direct or indirect. Cost that are unidentified in the planning phase frequently account for a large number of IT project cost overruns. This Cost/Benefit Analysis can be part of the overall investment CBA. Include assumptions and constraints that were used to develop these figures. Ensure that costs have been validated either independently or using a self-assessment process. Costs developed must be captured for the projected Life Cycle and detailed in the appropriate I-TIPS security spreadsheet. Life Cycle costs include projected acquisition, installation, construction, operational and maintenance costs.

Special Requirements of the Project (Waiver, Technology Search)

Do the security requirements needed to support the investment require a security waiver from Cyber Security policies or Departmental Regulation 3140? At this phase in the CPIC Process, the security controls must be established. If a major change is made in system design after this phase a security waiver is required. Send security waiver requests to OCIO in accordance with established procedures.

Although an IT acquisition approval (acquisition waiver) request is normally separate from an IT investment package, approved investments still require acquisition waivers. An acquisition waiver should be requested early in the pre-acquisition process, preferably concurrent with the investment package, to allow sufficient review by the necessary offices within OCIO. The acquisition waiver package should clearly identify reason(s) for the request, include comprehensive cost comparisons, and contain a strong justification for waiver approval. It should be sent to the USDA Chief Information Officer. Information technology acquisition should only commence after written approval has been obtained from OCIO.

Technical Overview with Graphic Depiction The ISSPM will ensure that a technical overview of the entire security infrastructure for the system/application is included with the investment package. This depiction should detail the security hardware and software environment at all levels and their location. This can be included with the overall graphical depiction of the system/application. Explain in narrative how the security infrastructure will be deployed; the use of Commercial Off the Shelf (COTS) software; and planned technology refreshments. Discuss the security migration plan for the infrastructure from the existing to the proposed technology and major transition details that affect the provisioning.

Exit Criteria

Prior to exiting the Select Phase, investments must have:

- Established performance goals and quantifiable performance measures;
- Developed a project plan which details quantifiable objectives including an acquisition schedule, project deliverables, and projected and actual costs;
- Identified costs (including security costs), schedule, benefits, and risks (review of mitigations based on final design), and prepared the I-TIPS Security Backup Sheets;
- Completed a Select Security Analysis and prepared a Security Plan;
- Established security, telecommunications, Section 508 (IT accessibility), and architecture goals and measures;
- Established an EITIRB investment review schedule for the Control Phase;
- Form for how the Official Records will be maintained throughout the SDLC developed;
- Process of capture, maintaining, and disposal of records identified; and
- Obtained CIO and EITIRB approval to enter the Control Phase.

The Functional Manager may further develop IT investments not approved by the EITIRB for inclusion at a subsequent review.

Control Phase:

Purpose

The objective of the Control Phase is to ensure, through timely oversight, quality control, and executive review, that IT initiatives are conducted in a disciplined, well-managed, and consistent manner. Investments should be closely tracked against the various components identified in the Risk Assessment and Mitigation Plan developed in the Select Phase. This phase also promotes the delivery of secure quality products and results in initiatives that are completed within

scope, on time, and within budget. During this process, senior managers regularly monitor the progress/performance of ongoing IT investments against projected cost, schedule, performance, and delivered benefits.

The Control Phase is characterized by decisions to continue, modify, or terminate an investment. Decisions are based on reviews at key milestones during the program's development lifecycle. The focus of these reviews changes and expands as the investments move from initial concept or design and pilot through full implementation and as projected investment costs and benefits change. The reviews focus on ensuring that projected benefits are being realized; cost, schedule and performance goals are being met; risks are minimized and managed; and the investment continues to meet strategic needs. Depending on the review's outcome, decisions may be made to suspend funding or make future funding releases conditional on corrective actions.

Entry Criteria

Prior to entering the Control Phase, investments must have:

- Established performance goals and quantifiable performance measures;
- Developed a project plan which details quantifiable objectives, including an acquisition schedule, project
- deliverables, and projected and actual costs;
- Identified costs (including security costs), schedule, benefits, and risks (review of mitigations based on final design);
- Completed a Select Security Analysis and prepared a completed Security Plan;
- Established security, telecommunications, Section 508 (IT accessibility), and architecture goals and measures;
- Established an EITIRB investment review schedule for the Control Phase; and
- Obtained CIO and EITIRB approval to enter the Control Phase.

Once the investment enters the Control Phase, the IPT will monitor the investment throughout development and report investment status to the investment's sponsors and oversight groups.

Process

During the Control Phase, an investment progresses from requirements definition to implementation. Throughout the Phase, agency CIOs provide the OCIO with investment reviews to assist them in monitoring all investments in the portfolio. Investment reviews provide an opportunity for Project Managers to raise issues concerning the IT developmental process, including security, telecommunications, enterprise architecture alignment, E-government (GPEA compliance) and Section 508 concerns.

The ability to adequately monitor IT initiatives relies heavily on the outputs from effective investment execution and management activities. OCIO develops a master milestone review calendar for evaluation and approval by the EITIRB. The OCIO maintains a control review schedule for all initiatives in the Department's IT investment portfolio and monitors investments quarterly. The EITIRB reviews investments at their discretion or if the cost, schedule, or performance varies more than 10 percent from expectations.

The EITIRB reviews are based on factors including the strategic alignment, criticality, scope, cost, and risk associated with all initiatives. The Project Sponsor establishes milestones as part of the investment baseline against which performance will be measured throughout the Control Phase. Agencies are expected to uphold these milestones; OMB will hold agencies responsible for meeting milestones as originally indicated in the baseline. After establishing the milestones, the Project Sponsor revises the project plan as required to meet the approved milestones. It is recommended that the project plan include a system pilot during the Control Phase because piloting helps reduce risk and provides a better understanding of costs and benefits.

The following Security Analysis steps are required in the Control phase:

Security Cost Review. OMB Circular A-130 states in part that agencies should conduct Benefit Cost Analysis for each information system to support management decisions making to ensure realization of expected benefits. When preparing benefit cost analyses to support investment in information technology, agencies should seek to quantify the

improvements in agency performance results through measurement of program outputs. Proposed "major investment systems"…require detailed and rigorous analysis. While it is not necessary to create a new benefit cost analysis at each stage of the information system life cycle, it is useful to refresh this analysis with up-to-date information to ensure the continued viability of an information system prior to and during implementation. Appendix III, OMB Circular A-130 further specifies four controls: assigning responsibility for security, security planning, periodic review of security controls, and management authorization. Any Benefit Cost Analysis for IT Systems should include detailed security cost projections prepared in the SELECT phase. The security cost review in the Control Phase should compare the actual system security cost with those projected in the SELECT phase, the percentage of variance should be noted, and information included to support why the cost were different than those in the original projections.

Review of Security Risk Assessment/Mitigation Strategy A review of the risk mitigation strategies should be conducted by the Information Systems Security Program Manager to ensure that they have been included in the final design specifications of the system.

Comprehensive Information Systems/ Program Security Goals/Measures DM3140-1 requires that the Information Systems Security Program Manager (ISSPM) or their designate participate in the testing of security systems after installation. In order to adequately test security goals/measures must be developed and established during the control phase. Establish baseline performance measures for the security infrastructure that will be used to determine overall effectiveness and efficiency. These factors should be consistent with the levels of desired security formulated during the SELECT phase to ensure that system security benefits are realized by the system when it is operational during the post-implementation review.

System Rules The agency ISSPM and the System Administrator will establish a set of rules concerning use of and behavior within the application/system. The rules shall be as stringent as necessary to provide adequate security for the application/system and information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individual users with access to the application/system. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

Security Operating Procedures (SOP) The agency ISSPM will develop documentation specifying procedures that are to be carried out by system users (to include System Administrators, Network Administrators and operators) to uphold all aspects of security.

Specialized Training Before allowing individuals access to the system, the agency ISSPM will ensure that all individuals receive specialized training focused on their responsibilities and the system rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval system) to formal training (e.g., for an employee that works with a high-risk system.

Personnel Security The agency Information Systems Security Program Manager in coordination with the System Administrator will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. In cases where such controls cannot adequately protect the system or information in it, they will ensure that individuals are screened commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the system and periodically thereafter.

Special Requirements of the Project (Waiver, Technology Search)
Do the security requirements needed to support the investment require a waiver from Cyber Security policies or Departmental Regulation 3140? At this phase in the CPIC Process, the security controls should be established. If a major change is made in system design a security waiver is required. Send security waiver requests to OCIO in accordance with established procedures documenting efforts to ensure that the items in the prior phases have been reviewed and mitigations taken to limit risk.

Contingency Planning The agency ISSPM will establish a contingency plan in coordination with the system owner and IT Manager and periodically test the capability to perform the agency function supported by the system in accordance with appropriate guidance issued by NIST 800-18. Contingency planning includes development of

Continuity of Operations Plan (COOP), Disaster Recovery and Business Resumption Plans, as appropriate, based on identification of sensitive information or business owner requirements.

Security Test and Evaluation (ST&E) must be performed for all systems. If an ST&E is not performed, an Independent Verification and Validation (IV&V) is performed on the system. The ST&E is an examination and analysis of safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system. Ensure that costs for this testing have been included in the overall investment spreadsheet.

Authorize Processing The agency Information Systems Security Program Manager will ensure that a designated management official authorizes in writing use of the system/application by confirming that its security plan as implemented adequately secures the system. Results of the most recent review or audit of controls shall be a factor in management authorizations. The system/application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system/application.

Security Performance Measures In conjunction with the business owner and or developer, the ISSPM will establish system/application security performance measures that include at a minimum: redundancy, availability, data integrity, confidentiality and security plan effectiveness. The system must, wherever cost effective, operate with full redundancy to ensure no single point of failure could disable the system. The system must restrict disclosure of the information to designated parties, must be protected from errors or unauthorized modification, and must be available within some given timeframe. In addition, the effectiveness of the Security Plan in defining the protections in place should be measured. These measures will include goals for performance in each category.

Certification and Accreditation The authorization of an IT system to process, store, or transmit information, granted by a management official, provides a form of quality control. Some agencies refer to this authorization as accreditation. Accreditation, which is required under OMB Circular A-130, should be based on an assessment of the management, operational, and technical controls associated with an IT system. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. C&A costs should include the complete certification review and subsequent accreditation associated with the investment.

Disaster Recovery Plan Disaster Recovery Planning is a process of developing advance arrangements and procedures that enable an organization to respond to a disaster and resume the critical business functions within a predetermined period, minimize the amount of loss, and repair or replace necessary equipment or facilities. Disaster Recover Plan costs should include the complete costs to review the implemented system and develop the plan.

Exit Criteria

Prior to exiting the Control Phase, investments must have:

- Completed investment development;
- Confirmed the PIR schedule, Security Costs, Risk Assessment/Mitigations and Performance Measure Reviews;
- Completed the Security Test and Evaluation (ST&E) and development of the Disaster Recovery Plan
- Completed Contingency Plan and Certification/Accreditation of system; and
- Obtained CIO and EITIRB approval to enter the Evaluate Phase.

Evaluation Phase:

Purpose

The purpose of the Evaluate Phase is to compare actual to expected results after an investment is fully implemented. This is done to assess the investment's impact on mission performance, identify any investment changes or

modifications that may be needed, and revise the investment management process based on lessons learned. As noted in GAO's *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making*, "the Evaluation Phase 'closes the loop' of the IT investment management process by comparing actuals against estimates in order to assess the performance and identify areas where decision-making can be improved."

The Evaluate Phase focuses on outcomes:

- Determining whether the IT investment met its performance, cost, and schedule objectives; and
- Determining the extent to which the IT capital investment management process improved the outcome of the IT investment.

The outcomes are measured by collecting performance data, comparing actual to projected performance and conducting a Post Implementation Review (PIR) to determine the system's efficiency and effectiveness in meeting performance, financial and security objectives. The PIR includes a methodical assessment of the investment's costs, performance, benefits, documentation, mission, security, and level of stakeholder and customer satisfaction. The PIR is conducted by the agency, and results are reported to the OCIO and EITIRB to provide a better understanding of initiative performance and assist the Project Sponsor in directing any necessary initiative adjustments. Additionally, results from the Evaluate Phase are fed back to the Pre-Select, Select, and Control Phases as lessons learned. Normally, investments stay in this phase for a period no longer than 6 months.

Entry Criteria

The Evaluate Phase begins once a system has been implemented and the system becomes operational or goes into production. Any investment cancelled prior to going into operation must also be evaluated. Prior to entering the Evaluate Phase, investments must have:

- Completed investment development;
- Perform the Independent Verification and Validation (IV&V) as part of the PIR;
- Completed Control Phase Security Analysis, Standard Operating Procedures and the DR Plan;
- Completed Contingency Plan and Certification/Accreditation of system;

- Confirmed the PIR schedule; and
- Obtained CIO and EITIRB approval to enter the Evaluate Phase.

Process

In the Evaluate Phase, investments move from implementation or termination to a PIR and the EITIRB's approval or disapproval to continue the investment (with or without modifications). From the time of implementation, the system is continually monitored for performance, outages, maintenance activities, costs, resource allocation, defects, problems, and system changes. System stability is also periodically evaluated. During the PIR, actual performance collected is compared to performance projections made during the Select Phase. Then lessons learned for both the investment and the CPIC process are collected and fed back to prior CPIC phases.

The following Security Analysis steps are required in the Evaluation phase:

Detailed Post Implementation Security Review of System NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, specifies that during the implementation phase, the system's security features will be tested. The ISSPM will ensure that the security for the system/application is tested, installed, and authorized for processing. A security design review and systems test should be performed prior to placing the system into operation to assure that it meets security requirements. In addition, if new security controls are added to the application or support system, additional acceptance tests of those new controls must be performed. Since the installation of new major systems generally occur well after the initial design phase, the post implementation review becomes more significant. Care should be exercised when conducting this review to document the results and determine if the system still

meets the original security design. All design specifications for security should have been delivered and furnished to the new system administrator. Another review of the risk mitigation strategies should be done to ensure that they have been built into the system and are operational. If necessary, addition countermeasures should be identified and implemented to assure that the system will adequately protect the integrity, confidentiality, and availability of the data.

Specialized Training Before allowing individuals access to the system, the agency ISSPM will ensure that all individuals receive specialized training focused on their responsibilities and the system rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval system) to formal training (e.g., for an employee that works with a high-risk system.

Personnel Security The agency Information Systems Security Program Manager in coordination with the System Administrator will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. In cases where such controls cannot adequately protect the system or information in it, they will ensure that individuals are screened commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the system and periodically thereafter.

Special Requirements of the Project (Waiver, Technology Search)
Do the security requirements needed to support the investment require a waiver from Cyber Security policies or Departmental Regulation 3140? At this phase in the CPIC Process, the security controls should be established. If a major change is made in system design a security waiver is required. Send security waiver requests to OCIO in accordance with established procedures documenting efforts to ensure that the items in the prior phases have been reviewed and mitigations taken to limit risk.

Review of System Controls The agency ISSPM will have a process for (1) requesting, establishing, issuing, and closing user accounts (2) tracking users and their respective access authorizations; and (3) managing these functions. Mechanisms besides auditing and analysis of audit trails should be used to detect unauthorized and illegal acts.

Independent Verification and Validation (IV&V) will be performed as part of the PIR for purposes of CPIC to ensure the integrity of the system. Ensure that costs for this testing have been included in the overall investment cost.

Certification and Accreditation The authorization of an IT system to process, store, or transmit information, granted by a management official, provides a form of quality control. Some agencies refer to this authorization as accreditation. Accreditation, which is required under OMB Circular A-130, should be based on an assessment of the management, operational, and technical controls associated with an IT system. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. C&A costs should include the complete certification review and subsequent accreditation associated with the investment.

Disaster Recovery Plan Disaster Recovery Planning is a process of developing advance arrangements and procedures that enable an organization to respond to a disaster and resume the critical business functions within a predetermined period, minimize the amount of loss, and repair or replace necessary equipment or facilities. Disaster Recover Plan costs should include the complete costs to review the implemented system, develop and test the plan.

Exit Criteria

Prior to exiting the Evaluate Phase, investments must have:

- Conducted a PIR, including a Security Review of the System (Costs, Risk Assessment/Mitigations and Performance Measures);

- Completed Evaluation Phase Security Analysis;
- Completed Independent Verification and Validation (IV&V) and testing of the DR Plan
- Established an Operations and Maintenance (O&M) and operational performance review schedule; and
- Obtained CIO and EITIRB approval to enter the Steady-State Phase.

Steady State Phase:

Purpose

The Steady-State Phase provides the means to assess mature investments, ascertain their continued effectiveness in supporting mission requirements, evaluate the cost of continued maintenance support, assess technology opportunities, and consider potential retirement or replacement of the investment. The primary review focus during this Phase is on the mission support, cost, and technological assessment. Process activities during the Steady-State Phase provide the foundation to ensure mission alignment and support for system and technology succession management.

Entry Criteria

Prior to entering the Steady-State Phase, investments must have:

- Conducted a PIR, including a Security Review of the System (Costs, Risk Assessment/Mitigations and Performance Measures);
- Completed Independent Verification and Validation (IV&V)
- Completed Evaluation Security Analysis;
- Annual review of Certification and Accreditation for system
- Completed Testing of Disaster Recovery Plan
- Established an Operations and Maintenance (O&M) and operational performance review schedule; and
- Obtained CIO and EITIRB approval to enter the Steady-State Phase.

Process

During the Steady-State Phase, mission analysis is used to determine whether mature systems are optimally continuing to support mission and user requirements. An assessment of technology opportunities and an O&M Review are also conducted.

The following Security Analysis steps are required in the Steady State phase:

Upgrades, Updates & Patches Steady State is generally the longest phase of an investment and covers the maintenance and operation of the system/application in the production environment until disposal. In this phase system upgrades, updates, and patches are applied, all major system changes necessitate retesting of security controls, and overall security reviews are conducted periodically. Material reviewed in this phase includes the latest system/application review, agency responses to data calls for patch/upgrade information and the latest Summary Reports of Vulnerability Scans.

Specialized Training Before allowing individuals access to the system, the agency ISSPM will ensure that all individuals receive specialized training focused on their responsibilities and the system rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval system) to formal training (e.g., for an employee that works with a high-risk system.

Personnel Security The agency Information Systems Security Program Manager in coordination with the System Administrator will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. In cases where such controls cannot adequately protect the system or

information in it, they will ensure that individuals are screened commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the system and periodically thereafter.

Disposal/Disposition of system Describe how information is moved to another system, archived, discarded or destroyed. Has all electronic media and hardware been sanitized, cleared and purged from the system in accordance with departmental procedures on Classified and Sensitive But Unclassified Information?
Include the costs for disposal and disposition of the system.

Review of Security Controls OMB A130, Appendix III, requires a review of security controls for all systems, including the risk assessment, every 3 years or when there is a major change. This is an ongoing requirement during this phase and costs for the review should be planned accordingly as part of system maintenance.

Special Requirements of the Project (Waiver, Technology Search)
Do the security requirements needed to support the investment require a waiver from Cyber Security policies or Departmental Regulation 3140? At this phase in the CPIC Process, the security controls should be established. If a major change is made in system design a security waiver is required. Send security waiver requests to OCIO in accordance with established procedures documenting efforts to ensure that the items in the prior phases have been reviewed and mitigations taken to limit risk.

Certification and Accreditation The authorization of an IT system to process, store, or transmit information, granted by a management official, provides a form of quality control. Some agencies refer to this authorization as accreditation. Accreditation, which is required under OMB Circular A-130, should be based on an assessment of the management, operational, and technical controls associated with an IT system. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. If there is a major change in the system, it must be re-certified and re-accredited. C&A costs should include the complete certification review and subsequent accreditation associated with the investment. Major changes should be factored into costs for the system.

Disaster Recovery Plan Disaster Recovery Planning is a process of developing advance arrangements and procedures that enable an organization to respond to a disaster and resume the critical business functions within a Pre-determined period, minimize the amount of loss, and repair or replace necessary equipment or facility. Disaster Recover Plan costs should include the complete costs to review the DR Plan on an annual basis.

Exit Criteria

Prior to exiting the Steady-State Phase, investments must have obtained the CIO and EITIRB's direction whether to dispose, retire, or replace the system. All systems being disposed of will undergo sanitation of electronic media (tapes, disks, etc) and other hardware. Preservation of official records must be done prior to disposal or other action on the system in accordance with DR 3080-1, DR 3040-1, DR 3090-1 and other departmental policy.

Security Information Technology Investment Portfolio System (I-TIPS) Detailed Backup Sheets

The Detailed Backup Sheets (Tables 2 and 3) have been developed to reflect the Cyber Security Program Operations and Major IT System/Initiatives costs for Cyber Security infrastructure. These sheets will reside in the I-TIPS Reference Library and will be used to roll up costs. Detailed Backup Sheets are to be completed for the Cyber Security Program Operations even though they are not used in the Major IT Investment process. This information is captured to provide a more complete picture of the total Cyber Security Program cost by agency. Each of the spreadsheets will be part of the overall Cyber Security Portfolio for each agency in the I-TIPS Public Resource Library. The detailed backup sheets will reside in the I-TIPS Resource Library that is designed to be an electronic repository of agency information supporting the investments, projects or programs. The information that resides in the Resource Library is informal in organization, and permits the data captured in the library to be developed in categories that are not currently included in the regular capital planning process. In the case of travel and training, program managers can view this information separately in lieu of the costs being rolled up into their personnel costs. Portfolio Managers will

need to manually enter these costs into their overall personnel costs within I-TIPS to meet the official CPIC requirements. These spreadsheets have been created in Excel and can be downloaded from the library and updated following the normal I-TIPS guidelines.

The detailed backup spreadsheets will serve as a memory jogger for the agency and will allow program heads or other review levels the opportunity to see how costs were formulated at the working level. Further, they provide a permanent record of Cyber Security planning at the Cyber Security Program Operations and Major Cyber Security Initiatives working level costs for audit purposes. Permanent records can be kept of cost data by printing the sheets after entry and retaining them in a file or by saving the sheet as an Excel file for historical purposes.

Planned costs developed in Table 2, Cyber Security Program Operations, are not subject to review during the Pre-Select, Select, Control, Evaluate and Steady State processes. However, these figures will be used in evaluating each agency's Annual Cyber Security Program Plan and to satisfy regulatory reporting requirements to the General Accounting Office and the Office of Management and Budget. The information developed in Table 3, Major Cyber Security System/Initiatives will be used to evaluate the agency Cyber Security infrastructure review by OCIO during major IT investment call periods. It is perfectly acceptable to use the cost reported in accounting records as a beginning point for developing next year's projections. These spreadsheets can also be used for OMB Form 300 Reporting. However, each agency should factor into these costs all anticipated customer and major projects cyber security infrastructure requirements.

The general format has been outlined below:

Agency name should be provided in the space to the left.

Year should be reflected for the planned cost

Steady State are costs of maintenance and operations at current capability and performance level. This is the normal operational and maintenance costs involved in operating a program.

Development/Modernization/Enhancement (D/M/E) are costs for new systems, changes or modifications to existing systems that improve capability or performance, changes mandated by Congress of agency leadership, personnel costs for project management, and direct support.

Planned Costs are the total costs by category and sub-category for each item according to the operation or initiative they support. If the agency does not have significant costs in a subcategory, planned costs can be put in the "Other Security Equipment" subcategory as a general total. However, the intent of CPIC is to show that USDA is planning and managing our upcoming business. Updating subcategories of costs reflects the planning effort more clearly so agencies are encouraged to break down costs into as many subcategories as feasible.

Cost Categories

Cost Categories are the object class codes used for initial cost development. Since the development of Telecom Infrastructure costs is a new requirement under the Capital Planning and Investment Control (CPIC) Process, we are only looking at the first two digits of the Object Class code in terms of our breakdown. Agencies can certainly modify their own detailed backup sheets internally to provide the additional granularity, if desired. However they should only use the Universal Object Class Codes that have been established by OMB for this purpose. Each cost category is shown below:

Cost Categories Chart

I-TIPS DME or SS Category	Object Class	Object Class Definition

Equipment	31.0	Those equipment related costs under Object Class 31 - purchases of equipment, including software
Software	31.0	Those software related costs under Object Class 31 - purchases of equipment, including software
Services	23.1, 23.2, 23.3, 25.2	Rental payments to GSA; rental payments to other federal agencies; security, communications, utilities, and miscellaneous charges; and other contractual services not elsewhere reported
Support Services	25.2, 25.7*	Other contractual services (commercial), Operation and maintenance of equipment (commercial)
Supplies	25.2, 25.3, 26.0	Supplies and materials
Personnel	11.1 thru 12.2	Personnel compensation and personnel benefits
Other	DO NOT USE, RESERVED FOR DOD USE ONLY	DO NOT USE, RESERVED FOR DOD USE ONLY
Intra-Governmental Payments	23.3, 25.3, 41.0	Payments for all IT services within agencies, between executive branch agencies (e.g. FTS2001), and state and local governments. Includes grants, subsidies, and contributions.
Intra-Governmental Collections		Collections for all IT services within agencies, between executive branch agencies (e.g. FTS2001), and state and local governments. Includes grants, subsidies, and contributions.
Training	25.1, 25.2	Training related costs for personnel in support of program or initiative.

Travel	21.0	Travel related costs for personnel in support of program or initiative. This includes travel related to training courses or project management.

Figure 2

* Note: In all cases, obligations or estimated expenditures under object class 25.7, operations and maintenance of equipment should be reported as a SS cost.

31 Equipment - Include all planned costs by year for information technology equipment by sub-category (security, Video, Data hardware and Other). Additional items may be added, if necessary, within the Other sub-category or may be reflected in the Other Security Equipment cost as a total figure. Equipment costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Equipment costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

31 Software - include all cost for information technology software, custom and commercial off-the-shelf, regardless of cost. Rows may be added to break this software down by type, if desired. Software costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Software costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

23 Services - include costs for all GSA Contracts for Cyber Security Service by major type of service. Also in this category include all Cyber Security service provided by other federal activities to USDA by agency. Type of service provided can also be noted after the planned cost, if desired. Services cost for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Services cost for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

25 Support Services - include planned costs for Cyber Security services provided by private sources. For planning purposes this can be shown by type of service anticipated under the item. Support Service costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Support Services costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

26 Supplies -include planned costs for items ordinarily consumed or expended within one year. Supply costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Supply costs for and Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

10 Personnel -include planned costs for compensation directly related to duties performed for the Government by Federal Civilian and Non-Federal personnel. These costs may be further delineated by job title/series, if desired. Personnel costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Personnel costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

Intra-Government Payments - include planned costs for Cyber Security service provided by other agencies within or outside USDA for which you must pay a fee. Intra-Government Payments costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Intra-Government Payment costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

Intra-Government Collections - include planned fees for Cyber Security services provided to other agencies within or outside USDA. Intra-Government Collections for the Cyber Security Program include those associated with maintaining current capability and performance level. Intra-Government Collections costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

21 Travel & Transportation of Persons -include planned costs for the travel and transportation of persons while in authorized travel status. Travel for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Travel costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

25 Training - include the planned costs for training of personnel. Training costs for the Cyber Security Program includes those costs associated with maintaining current capability and performance level. Training costs for Major Cyber Security Initiatives include those costs associated with project management and direct support for the project as well as the cost associated with maintaining current capability and performance level.

Cyber Security Program Operations Backup Sheet
TABLE 1

Cyber Security Program Operations is the Detailed Backup Spreadsheet used to capture annual costs for the normal operations and maintenance of the total Cyber Security Program. The costs should be entered in I-TIPS during the normal yearly IT Budget cycle. Anticipated costs should be planned or projected based on prior year's accounting records, purchase orders, invoices from contractors or other reliable agency cost data. However, the final forecasts should be based in large part on the upcoming user security requirements or additional project support required for the upcoming year.

This sheet is designed to reflect the costs involved in the daily operation of your agency's Cyber Security Program. Planned costs for cyber security equipment and services that are not specifically tied to a specific cyber security major investment should be included below:

Cyber Security Program Operations Resources Base/Budget Requirements
DETAILED BACK UP SHEET
DATE

Agency_____ Year_____

31 Equipment:

Item	Steady State	D/M/E	Planned Cost
Firewall Hardware			
VPNs			
Public Key Infrastructure			
Intrusion Detection System (IDS) Hardware			
Vulnerability Testing			
Sniffers			
User Authentication Systems			
Content Smart Switches			
Layer I			
Layer II			
Layer III			
Layer IV			
Data Backup Equipment			
Hot Site System			
Redundancy Hardware			
Other Security Eqmt.			

Subtotal

31 Software:

Item	Steady State	D/M/E	Planned Cost
Firewall			
Intrusion Detection Sys. (IDS)			

Subtotal

23 Services:

* GSA Contracts for Cyber Security Service

Item	Steady State	D/M/E	Planned Cost
Risk Management Assessments			
Intrusion Detection Sys. Support			
Security Plan Preparation			
Disaster Recover Plan Prep.			
Firewall Support			
PKI Support			
Vulnerability Testing			

Subtotal

* Other Federal Contracts for Cyber Security Service

Item (By Agency)	Steady State	D/M/E	Planned Cost
Risk Management Assessments			
Intrusion Detection Sys. Support			
Security Plan Preparation			
Disaster Recover Plan Prep.			
Firewall Support			
PKI Support			

Subtotal

25 Support Services:

Non-Federal Contracts for Cyber Security Service

Item	Steady State	D/M/E	Planned Cost
Risk Management Assessments			
Intrusion Detection Sys. Support			
Security Plan Preparation			
Disaster Recover Plan Prep.			
Firewall Support			
PKI Support			

Subtotal

26 Supplies:

Item	Steady State	D/M/E	Planned Cost

Subtotal

10 Personnel:

Item	Steady State	D/M/E	Planned Cost

Subtotal

Intra-Gov't Payments:

Item	Steady State	D/M/E	Planned Cost

Subtotal

Intra-Gov't Collections:

Item	Steady State	D/M/E	Planned Cost

Subtotal

21 Travel & Transportation of Persons:

Item	Steady State	D/M/E	Planned Cost

Subtotal

25 Training:

Item	Steady State	D/M/E	Planned Cost
Security Awareness			
User Authentication			
Intrusion Detection Sys.			
Firewall & VPN			
Intro. Information Security			
Active Content Inspec. Sys.			
Vulnerability Testing			

Subtotal

Grand Total

The costs in this spreadsheet are updated as emergency or unanticipated costs occur or bi-annually to ensure they accurately reflect normal program operation.

Cyber Security Major Initiatives Backup Sheet
TABLE 2

Cyber Security Major Initiatives is the Detailed Backup Spreadsheet used to capture the planned costs developed to support Major Information Technology Investments. All cyber security requirements (equipment and services) identified to support a specific investment should be included on this spreadsheet. If other I-TIPS data has been developed to support other types of costs not related to IT, a reference should be made to the main investment portfolio location. In any case, the total security costs should be entered in the major portfolio for the investment. If this investment is made in partnership with another agency or agencies, a note should be included with the agency name to highlight the spreadsheet reflects pro-rated costs for the agency on that investment.

If the agency determines that the investment does not require additional cyber security support, a note reflecting this analysis should be included under this spreadsheet. In all cases, a security analysis should be performed for every major investment and appropriate documentation should be included below:

Major Security Initiatives Resources Base/Budget Requirements
DETAILED BACK UP SHEET
DATE

Agency_____ Year_____

31 Equipment:

Item	Steady State	D/M/E	Planned Cost
Firewall Hardware			
VPNs			
Public Key Infrastructure			
Intrusion Detection System (IDS) Hardware			
Vulnerability Testing			
Sniffers			
User Authentication Systems			
Content Smart Switches			
Layer I			
Layer II			
Layer III			
Layer IV			
Data Backup Equipment			
Hot Site System			
Redundancy Hardware			

Other Security Eqmt.

Subtotal

31 Software:

Item	Steady State	D/M/E	Planned Cost
Firewall			
Intrusion Detection Sys. (IDS)			

Subtotal

23 Services:

* GSA Contracts for Cyber Security Service

Item	Steady State	D/M/E	Planned Cost
Risk Management Assessments			
Intrusion Detection Sys. Support			
Security Plan Preparation			
Disaster Recover Plan Prep.			
Firewall Support			
PKI Support			
Vulnerability Testing			

Subtotal

* Other Federal Contracts for Cyber Security Service

Item (By Agency)	Steady State	D/M/E	Planned Cost
Risk Management Assessments			
Intrusion Detection Sys. Support			
Security Plan Preparation			
Disaster Recover Plan Prep.			
Firewall Support			
PKI Support			

Subtotal

25 Support Services:

Non-Federal Contracts for Cyber Security Service

Item	Steady State	D/M/E	Planned Cost
Risk Management Assessments			
Intrusion Detection Sys. Support			
Security Plan Preparation			
Disaster Recover Plan Prep.			
Firewall Support			

PKI Support

Subtotal

26 Supplies:

Item	Steady State	D/M/E	Planned Cost

Subtotal

10 Personnel:

Item	Steady State	D/M/E	Planned Cost

Subtotal

Intra-Gov't Payments:

Item	Steady State	D/M/E	Planned Cost

Subtotal

Intra-Gov't Collections:

Item	Steady State	D/M/E	Planned Cost

Subtotal

21 Travel & Transportation of Persons:

Item	Steady State	D/M/E	Planned Cost

Subtotal

25 Training:

Item	Steady State	D/M/E	Planned Cost
Security Awareness			
User Authentication.			
Intrusion Detection Sys.			
Firewall & VPN			

Intro. Information Security
Vulnerability Testing

Subtotal

Grand Total

Planned cost should be entered into the I-TIPS Resource Library along with other major investment supporting documentation during the preparation of the investment proposal by the agency. Updates should be made to costs based on the overall guidance provided on the Capital Planning and Investment Control (CPIC) process. Generally this is whenever costs change during the investment life cycle.