APPENDIX N—CYBER SECURITY INFRASTRUCTURE GUIDE

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 (OMB) recently updated OMB 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 Federal Information Security Management Act (FISMA)**,** has established a clear and convincing case for the 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 the Office of the Chief Information Officer (OCIO), in response to OMB, has pressed agencies and staff offices to take successive steps to demonstrate their ability to more clearly plan and articulate their 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. Security and privacy planning must proceed in parallel with the development of the system(s) to ensure IT security and privacy requirements, and costs are identified and incorporated into the overall lifecycle of the system(s).

Actions taken during the CPIC process support the Certification and Accreditation (C&A) process, FISMA reporting, and security administration within agencies and staff offices, throughout the Systems Development Life Cycle (SDLC). Each agency's Chief Information Officer (CIO), with their Information System Security Program Manager (ISSPM) must to take this opportunity to actively engage in this process, develop realistic security costs and establish an active C&A program for their IT investments. Implementation of an IT CPIC 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 OCIO Associate CIO for Cyber Security (ACIO-CS). For further information about this guide, please contact Cyber Security at cyber.communication@usda.gov.

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:

- To use new technologies to sustain, not erode, the privacy protections provided in statutes;
- To ensure the protection of Federal computer resources commensurate with the risk of harm resulting from misuse or unauthorized access to such systems;
- To manage security risks and incidents in a way that complements and does not unnecessarily impede agency business operations;
- To implement an overall strategy to manage security that is 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.

FISMA requires that all systems be certified and accredited which means the Agency Certifying Official (CO) and Designated Approving Authority (DAA) have to authorize, in writing, all systems to process information in a secure infrastructure. All systems must conduct a Privacy Impact Assessment (PIA) to determine and formally document if the system processes and/or stores Personally Identifiable Information (PII).

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 sensitivity and 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's 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 cost summary sheets are entered into the Capital Planning Investment Repository (CIMR). 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 (E-Board) 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 SDLC. OCIO has developed the following evaluation factors to be used in the CPIC cyber security infrastructure review and oversight process for new or existing investments in the USDA's investment 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 investment 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 security 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

5 Security and privacy issues for the investment are addressed, all questions are answered, and a PIA is provided in appropriate circumstances. Security/privacy detail is provided about the individual investment throughout the SDLC to include budgeting for security. **(GREEN)**

4 Security and privacy information for the investment is provided but there are weaknesses in the information that need to be addressed. **(GREEN)**

3 Security and privacy information for the investment is provided but fails to address the minimum requirements. (YELLOW)

2 Security and privacy information points to an overall Agency Security Process with little or no detail at this investment level. **(RED)**

1 There is no security or privacy information provided for the investment. **(RED)**

Tips: No investment can score above 3 until it has completed C&A, and the C&A must be less than 3 years old. OMB does not recognize interim authority to operate. Agencies must respond to these questions in a way that demonstrates that they understand (and are working to meet) the security requirements of the investment specifically. General statements are not helpful. For example, if the data in a system is sensitive, the security section should demonstrate that the agency knows this and is securing the data appropriately. OMB is also focusing more attention on the need for PIAs and System of Records Notice (SORNs).

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 System Security Plan (SSP) (Draft) has been completed User Requirements have been defined Preliminary Risk Assessment has been performed Data Sensitivity has been identified
Select Phase:	**Select Phase** Security Analysis has been completed Majority of SSP has been completed Risk Assessment/Mitigation has been completed PIA has been completed SORN (if required) has been completed
Control Phase:	**Control Phase** Security Analysis has been completed Security Cost and Performance Goals have been reviewed C&A of system has been completed Security Test and Evaluation (ST&E) has been completed Disaster Recover (DR) Plan has been completed
Evaluate Phase:	**Evaluate Phase** Security Analysis has been completed Post Implementation Review (PIR) with independent verification and validation (IV&V) has been completed

DR Plan has been tested

Steady State:

Upgrades/Patches have been applied as required
Maintenance/Production record has been maintained
Configuration Control/Management has been implemented
Re-certification and re-accreditation have been conducted
DR Plan has been tested
Annual Security Self-Assessment has been conducted
SSP has been updated annually
System Retirement and Disposal Activities have been completed (Not scored)

Security Evaluation Factors

Pre-Select Phase:

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

Select Phase:

Has a Select Phase security analysis been conducted?
Has an SSP been completed?
Are security risks identified and mitigation strategies proposed?
Has a PIA been completed?
Has a SORN been completed, if one is required?

Control Phase:

Has a Control Phase 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 completed?
Has the system completed C&A?

Evaluate Phase:

Has an Evaluate Phase 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 Phase security analysis been conducted?
Are system/application patches and upgrades being applied in a timely manner?
Are security controls being maintained?
Has the system been re-certified and re-accredited as required?
Has the SSP been updated annually?

Have retirement and disposal actions been taken, if necessary to protect sensitive data?

Rating Award Basis

Pre-Select Phase:

5 Pre-Select Phase Security Analysis has been completed. This includes draft SSP, Data/User Requirements, Preliminary Risk Assessment, Data Sensitivity determination and identification of system security officer. **[Green]**

4 Pre-Select Phase 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 A project plan has been developed showing the due and completion dates of all required Security Analysis documents that accompany 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 Phase Security Analysis has been completed to include information on all security analysis factors, SSP completed, appropriate risks identified, mitigation strategies sound, validated costs/benefit analysis (CBA) for security performed with constraints/assumptions, C&A strategy has been documented, funded, and security complements departmental architecture. PIA/SORN completed. **[Green]**

4 Select Phase 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 Select Phase Security Analysis has been completed 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]**

<u>Control Phase:</u>

5 Control Phase Security Analysis has been completed; security costs are accurately accounted for, controlled, and managed; original cost estimate is current; detailed performance goals/measures established; ST&E completed; C&A of system has been completed. **[Green]**

4 Control Phase 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 Phase Security Analysis has been completed 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]**

<u>Evaluate Phase:</u>

5 Evaluate Phase Security Analysis has been completed. Agency has done commendable job in conducting the PIR with an IV&V, annually tested DR Plan; PIR reports attainment of the goals, benefits, and expectations that were originally envisioned for the project. **[Green]**

4 Evaluate Phase 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 Evaluate Phase Security Analysis has been completed 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 Phase Security Analysis has been completed. System/application upgrades and patches are applied as required, security controls are maintained and high/medium vulnerabilities promptly corrected. Annual review of the Security Controls, C&A of System and DR Plan testing have been conducted for life of system.
[Green]

4 Steady State Phase 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 Phase Security Analysis has been completed 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 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 (see **Appendix K—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 ISSPM will work with the business owner to fully define the security requirements. Some of the questions to be answered: 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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems. A summary of the SSP shall be incorporated into the strategic Information Resources Management (IRM) plan, required by the Paperwork Reduction Act, and each CPIC Investment Proposal. At this point, a skeleton SSP 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, misuse, 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 emphasized that federal information required 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 used 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. 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. NIST’s Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, shall be used as guidance for determining sensitivity of systems and information.

Protecting sensitive information means providing security protection based on 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.

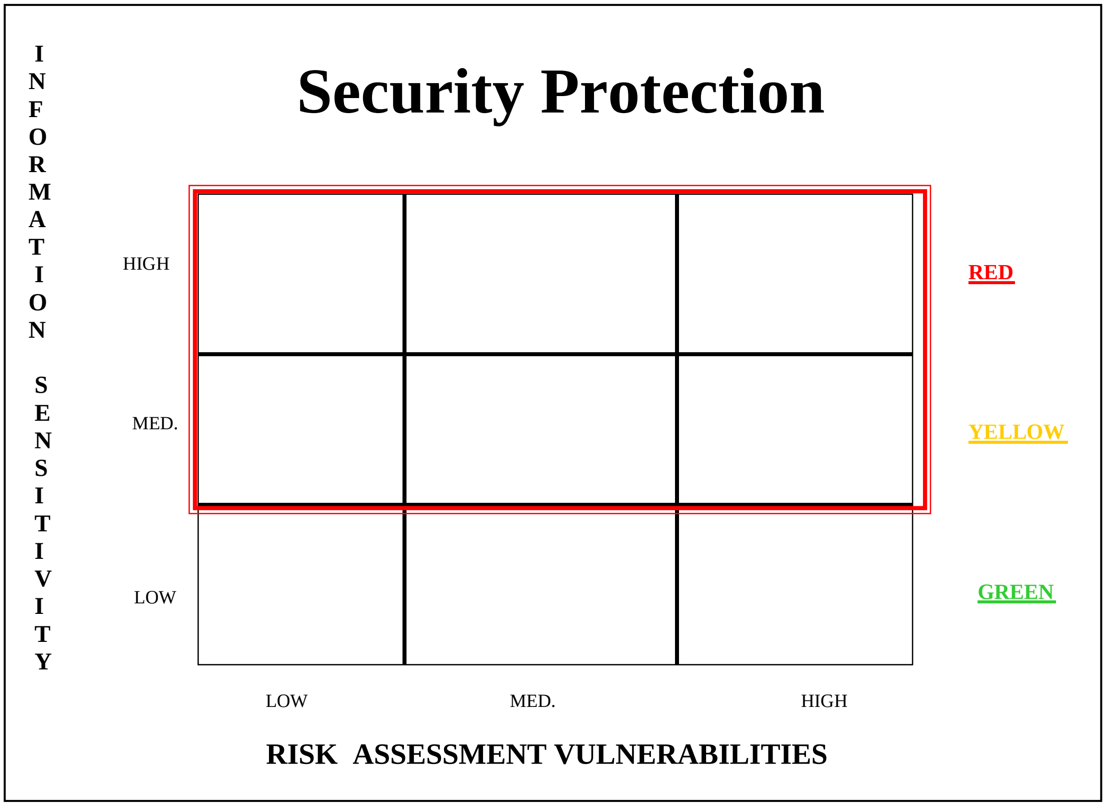

Figure 1

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 SSP.

Exit Criteria

Prior to exiting the Pre-Select Phase, investments must obtain CIO and E-Board 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 an SSP, determination of information sensitivity, Preliminary Risk Assessment**,** and selection of a Security Representative on the investment project team. An Agency Records Officer shall have been appointed for the system in accordance with the Electronic Records Management Program.

Select Phase:

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 E-Board selects which investments will be included in the Department's investment portfolio.

Entry Criteria

Prior to entering the Select Phase, investments must have obtained E-Board approval for the mission need and concept. The Pre-Select Security Analysis must have been completed, including the initiation of a draft SSP, 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, SSP**,** and project plan. By this time, the need for a PIA should have been determined. A Project Plan for certifying and accrediting the systems identified in this IT investment should have been formulated. 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 ensuring 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 ensure that security products and techniques are appropriately used in the system/application. The designated official will be contacted if 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 members to ensure appropriate security protection is proposed and/or in place for the new investment.

Security Risk Management Risk management addresses risks that arise from an organization's use of IT. 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 assessment results. The agency ISSPM is responsible for developing the appropriate risk assessment and mitigation strategies, including Plans of Actions and Milestones (POA&Ms) if necessary, 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 the 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; they are updated prior to implementation of the system and again 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 end-user 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 ISSPM, in coordination with the System Administrator (SA), will incorporate controls such as separation of duties, least privilege, and individual accountability into the system and system rules as appropriate. Employees’ managers must ensure that all individuals are screened commensurate with the risk and magnitude of the harm they could cause to a system and its information. Such screening shall be initiated 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 ISSPM will ensure that appropriate technical security controls are specified, designed into, tested, and accepted in the system in accordance with appropriate guidance issued by NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems.

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 SA 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 (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.

Certification and Accreditation This process has four phases: the Pre-certification or Initiation Phase; the Certification Phase, the Accreditation Phase, and the Post-accreditation or Continuous Monitoring Phase. The Pre-certification/Initiation Phase involves: making preparations, providing notification and identifying resources, delineating accreditation boundaries, providing SSP analysis, update and acceptance, reviewing the initial risk assessment, determining the security categorization, negotiating with participants and having CS confirm security categorization analysis. The Certification Phase involves: assessing security controls, documenting security certification, conducting ST&E, updating the risk assessment with the ST&E findings, updating the SSP, documenting the certification findings in the Security Analysis Report (SAR), forwarding the package to the ACIO-CS for a concurrency review, and forwarding the certification package to the DAA for an accreditation decision. The Accreditation Phase involves: obtaining the DAA security accreditation decision, providing security accreditation documentation and obtaining an ATO, IATO or Denial to Operate. The Post-Accreditation/Continuous Monitoring phase involves: providing configuration management and control, monitoring security controls, providing status reporting and documentation through POA&Ms and re-accrediting the system every three years or when a significant change occurs, updating the SSP annually, conducting annual security self-assessments, and periodic DR testing.

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 SSP 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 SSP in defining the protections in place should be measured. These measures will include goals for performance in each category.

Cost/Benefit Analysis In conjunction with the business owner and/or developer, the ISSPM will conduct a CBA, identify and quantify benefits and costs, and prepare cost estimates for the security to support the investment. Benefits should describe how the investment security enhances the agency's ability to meets its mission needs, and should outline functionality or cost savings. Benefits are defined as a profit, and 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. Costs that are unidentified in the planning phase frequently account for a large number of IT project cost overruns. This CBA 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 by using a self-assessment process. Costs developed must be captured for the projected SDLC and detailed in the Capital Planning Investment Repository (CIMR). SDLC costs include projected acquisition, installation, construction, operational and maintenance costs.

Special Requirements of the Project (Waiver, Technology Search)
At this phase in the CPIC Process, the security controls must be established; and it should be determined if security requirements needed to support the investment require a security waiver from Cyber Security policies or Departmental Regulation (DR) 3140-001 USDA Information Systems Security Policy. If a major change is made in system design after the Select 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 CIO. 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 physical location. This can be included with the overall graphical depiction of the system/application. The narrative explanation should include: how the security infrastructure will be deployed; the use of Commercial Off the Shelf (COTS) software; and planned technology refreshments; the security migration plan for the infrastructure from the existing to the proposed technology; and major transition details that affect the provisioning.

Privacy Impact Assessment This is designed to evaluate the impact on privacy of information stored in or processed by the information systems. The process is designed to guide system owners and developers in assessing privacy impact through the early stages of system development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and obtaining approval by the CS Privacy Act Officer in the OCIO. Additionally, if the investment/systems contains privacy data, a SORN may be required.

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);
- Completed a Select Phase Security Analysis and prepared an SSP ;
- Completed a PIA and SORN (if required), and a plan for C&A;
- Established security, telecommunications, Section 508 (IT accessibility) compliance, and architecture goals and measures;
- Established an E-Board investment review schedule for the Control Phase;
- Planned for maintenance of the Official Records throughout the SDLC;
- A process of capture, maintenance, and disposal of records identified; and
- Obtained CIO and E-Board approval to enter the Control Phase.

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

Control Phase:

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 project's SDLC. 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 Phase Security Analysis and SSP**;**
- Established security, telecommunications, Section 508 (IT accessibility) compliance, and architecture goals and measures;
- Established an E-Board investment review schedule for the Control Phase; and
- Obtained CIO and E-Board approval to enter the Control Phase.

Once the investment enters the Control Phase, the Investment Project Team (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, the agency CIO provides 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 compliance concerns.

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

The E-Board 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 CBA for each information system to support management decisions made to ensure realization of expected benefits. When preparing CBA to support investment in IT, 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 CBA at each stage of the information SDLC, 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. OMB Circular A-130, Appendix III, further specifies four controls: assigning responsibility for security, security planning, periodic review of security controls, and management authorization. Any CBA 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 costs with those projected in the Select Phase, the percentage of variance should be noted, and information included to support why the costs 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 ISSPM to ensure that they have been included in the final design specifications of the system.

Comprehensive Information Systems/Program Security Goals/Measures DM3545-002, USDA Information Systems Security Program, requires that the 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. Baseline performance measures for the security infrastructure that will be used to determine overall effectiveness and efficiency should be established. 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 during the PIR.

System Rules The agency ISSPM and the SA 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 The agency ISSPM will develop documentation specifying procedures that are to be carried out by system users (to include SAs, 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 ISSPM, in coordination with the SA, will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. Additionally, 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)
At this phase in the CPIC Process, the security controls must be functioning in a consistent and acceptable manner. If a major change is made in system design during this phase, the security controls must be re-evaluated using the C&A process. Security waiver requests should be sent to the OCIO in accordance with established procedures.

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 SP 800-34, Contingency Planning Guide for Information Technology Systems. Contingency planning includes development of Continuity of Operations Plan (COOP), Disaster Recovery (DR) and Business Resumption (BR) 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 ISSPM will ensure that a designated management official authorizes in writing use of the system/application by confirming that its SSP 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 acceptance of the risk of each system/application.

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. 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. Accreditation, which is required under OMB Circular A-130, Appendix III, is based on an assessment of the management, operational, and technical controls associated with an IT system. C&A costs should include the complete certification review and subsequent accreditation associated with the investment.

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 SSP 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 SSP in defining the protections in place should be measured. These measures will include goals for performance in each category.

Disaster Recovery Plan DR 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. DR Planning 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 ST&E and development of the DR Plan
- Completed Contingency Plan and C&A of the system; and

- Obtained CIO and E-Board approval to enter the Evaluate Phase.

Evaluate Phase:

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 Evaluate 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 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 E-Board 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;
- Performed the IV&V as part of the PIR;
- Completed Control Phase Security Analysis, Security Operating Procedures and the DR Plan;
- Completed Contingency Plan and C&A of the system;
- Completed PIA and SORN if required; and
- Obtained CIO and E-Board approval to enter the Evaluate Phase.

Process

In the Evaluate Phase, investments move from implementation or termination to a PIR and the E-Board'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 information is collected and 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 Evaluate Phase:

Detailed Post Implementation Security Review of System NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, specifies that during the Implementation Phase of the SDLC the system's security features will be tested. The ISSPM will ensure that the security for the system/application is installed, tested, and authorized for processing. A security design review and system test should be performed prior to placing the system into operation to ensure 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 occurs well after the initial design phase, the PIR 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 SA. An additional review of the risk mitigation strategies should be conducted to ensure that they have been built into the system and are operational. If necessary, additional countermeasures should be identified and implemented to ensure 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 ISSPM in coordination with the SA will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. Additionally, 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)

At this phase in the CPIC Process, the security controls must be functioning in a consistent and acceptable manner. If a major change is made in system design during this phase, the security controls must be re-evaluated using the C&A process. Security waiver requests should be sent to the OCIO in accordance with established procedures.

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 in addition to 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. 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. Accreditation, which is required under OMB Circular A-130, Appendix III, is based on an assessment of the management, operational, and technical controls associated with an IT system. C&A costs should include the complete certification review and subsequent accreditation associated with the investment.

Disaster Recovery Plan DR 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. DR Planning 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 PIA, and SORN (if required);
- Conducted a Security Review of the System (Costs, Risk Assessment/Mitigations and Performance Measures);
- Completed the Evaluate Phase Security Analysis;
- Completed IV&V and testing of the DR Plan;
- Established an Operations and Maintenance (O&M) and operational performance review schedule; and
- Obtained CIO and E-Board approval to enter the Steady State Phase.

Steady State Phase:

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 PIA, and SORN (if required);
- Conducted Security Review of the System (Costs, Risk Assessment/Mitigations and Performance Measures);
- Completed IV&V;
- Completed the Evaluate Phase Security Analysis;
- Conducted the tri-annual C&A of the system;
- Completed Testing of DR Plan;
- Established an O&M and operational performance review schedule; and
- Obtained CIO and E-Board 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 re-certification and re-accreditation of the system, and overall security reviews are conducted annually. 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 ISSPM in coordination with the SA will incorporate controls such as separation of duties, least privilege and individual accountability into the system and system rules as appropriate. Additionally, 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. Ensure that all electronic media and hardware has 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 Circular A-130, Appendix III, requires a formal 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)
At this phase in the CPIC Process, the security controls must be functioning in a consistent and acceptable manner. If a major change is made in system design during this phase, the security controls must be re-evaluated using the C&A process. Security waiver requests should be sent to the OCIO in accordance with established procedures.

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. 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. Accreditation, which is required under OMB Circular A-130, Appendix III should be based on an assessment of the management, operational, and technical controls associated with an IT system. C&A costs should include the complete certification review and subsequent accreditation associated with the investment.

Disaster Recovery Plan DR 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. DR Planning 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 E-Board's direction whether to dispose, retire, or replace the system. All systems being disposed of will undergo sanitization 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 3080-001, Records Management and other relevant departmental policy.