CHAPTER 15, PART 1
SECURITY CONTROLS IN THE SYSTEM LIFE CYCLE /SYSTEMS DEVELOPMENT LIFE CYCLE

1 BACKGROUND

USDA has traditionally depended upon diverse and rapidly changing commercially available IT resources to support its business practices and deliver services to the public. Often those resources have been implemented without consideration or implementation of minimum secure access controls and therefore, leaves sensitive information vulnerable to exploitation. The current heightened sense of national alert and the administration's focus on the security of Federal Information Technology (IT) assets requires that USDA take immediate action to secure our systems.

Including security early in the information System Life Cycle (SLC)/System Development Life Cycle (SDLC) will usually result in less expensive and more effective security than adding it after a system is operational. This guide presents a framework for incorporating security into all phases of the SLC/SDLC process, from inception to disposal. This document is a guide to help agencies select and acquire cost-effective security controls by explaining how to include information system security requirements in appropriate phases of the SLC/SDLC.

A general SLC/SDLC is discussed in this guide that includes the following phases: initiation, acquisition/development, implementation, operations/maintenance, and disposition. Each of these five phases includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SLC/SDLC described in this document or will have developed a tailored SLC/SDLC that meets their specific needs. In either case, it is recommended that organizations incorporate the associated IT security steps of this general SLC/SDLC found in Figure 1 into their development process:

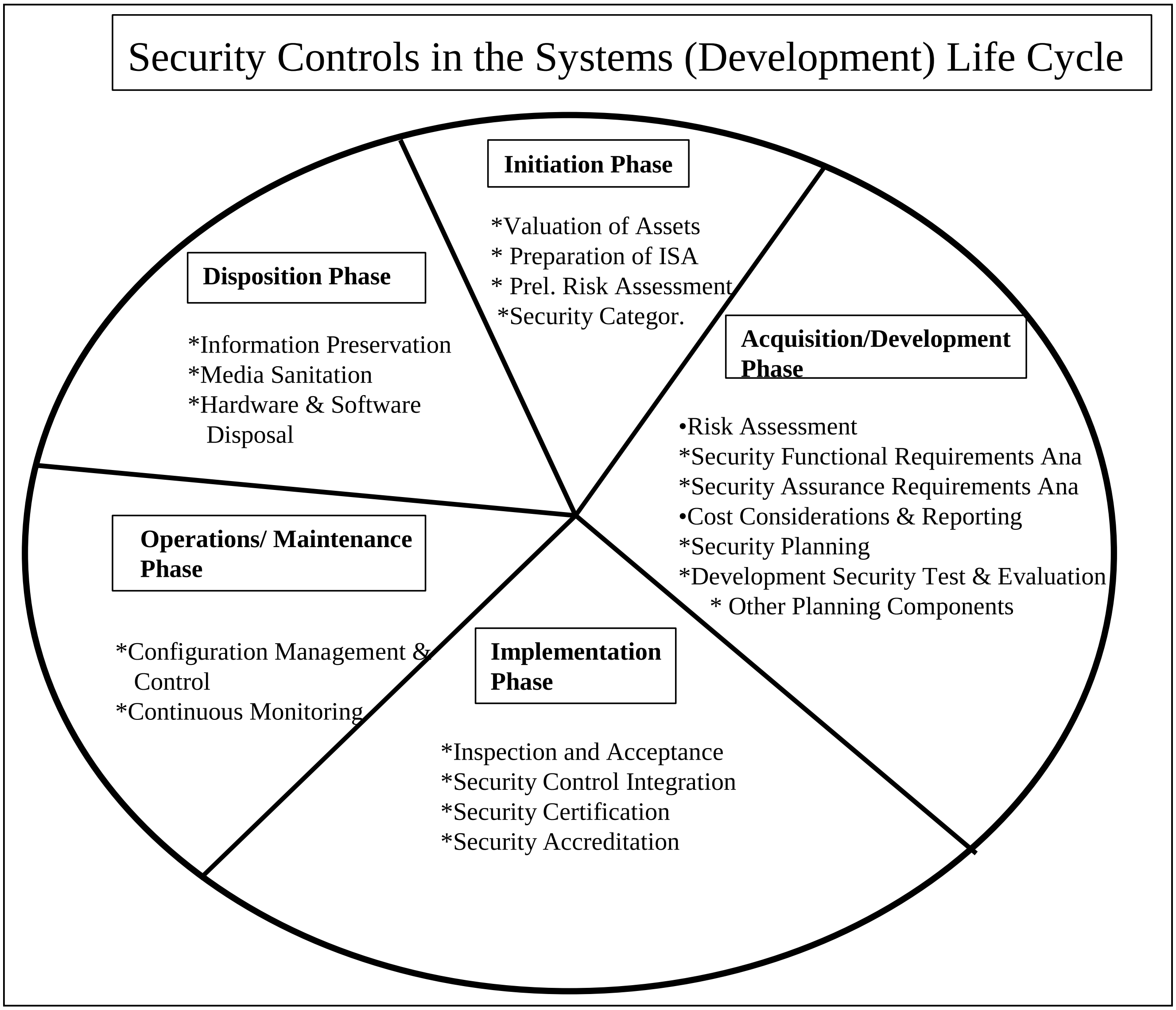
Security Controls in the Systems (Development) Life Cycle
Initiation Phase
*Valuation of Assets
* Preparation of ISA
* Prel. Risk Assessment
*Security Categor.
Acquisition/Development Phase
•Risk Assessment
*Security Functional Requirements Ana
*Security Assurance Requirements Ana
•Cost Considerations & Reporting
*Security Planning
*Development Security Test & Evaluation
* Other Planning Components
Implementation Phase
*Inspection and Acceptance
*Security Control Integration
*Security Certification
*Security Accreditation
Operations/ Maintenance Phase
*Configuration Management & Control
*Continuous Monitoring
Disposition Phase
*Information Preservation
*Media Sanitation
*Hardware & Software Disposal

Figure 1

t should be noted that this general model has been used for simplicity; there are other acceptable SLC/SDLC models that can be used for more complex IT systems. It is important for each agency to determine the appropriate SLC/SDLC at the beginning of work on the system to use as a framework for implementing the required actions. The number and types of appropriate security controls may vary throughout a particular SLC/SDLC and acquisition cycle. The relative maturity of an organization's security architecture may also influence the types of appropriate security controls. The blend of security controls is tied to the mission of the organization and the role of the system within the organization as it supports that mission. One way to identify the ideal mix of management, operational, and technical security controls is with the risk management process. To be most effective, information security must be integrated into the SLC/SDLC from its inception.

To assist organizations in making the appropriate selection of security controls for their information systems, the concept of baseline controls is introduced in NIST Special Publication 800-53. Baseline security controls are the minimum controls recommended for an information system based on the system's security categorization established in accordance with FIPS Publication 199.

FIPS Publication 199 security categories are typically considered during the risk assessment process to help guide the initial selection of security controls for an information system. The risk assessment process provides useful information and a procedural approach to examining the important factors that ultimately determine which security controls are necessary to protect the organization's operations and assets. The baseline security controls from Special Publication 800-53 associated with the security categories of FIPS Publication 199 serve as a starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. The baseline security controls can be tailored or adjusted based on the results of the risk assessments conducted by the organization. Modifications to the baseline controls should be documented (with supporting rationale for the changes) in the security plan for the information system.

The appropriate security controls are selected for the appropriate baselines. The security control baselines are intended to provide coverage for certain potential threats. The security controls selected for each baseline are at the recommended level of robustness to achieve the estimated threat coverage. In cases where the baselines do not provide sufficient coverage against certain types of threats, additional security controls may be needed. NIST Special Publication 800-53 provides more detailed information on appropriate security controls for each type of baseline.

Security is also built into an IT system from the beginning of its life cycle concurrent with the Capital Planning and Investment Control (CPIC) Process. Outlined below in Figure 2 is a chart depicting the relationship between the SLC/SDLC and CPIC phases. Many of the actions taken during the CPIC Phases support those required during the normal SLC/SDLC and can be used to support both requirements. An example of this is conducting a Risk Assessment which supports both the action required during the Initiation and Development/Acquisition Phase of the SLC/SDLC and is required by the Pre-Select and Select Phases of the Capital Planning Process.

SLC/SDLC	CPIC
Initiation	Pre-Select/Select
Development/Acquisition	Select
Implementation	Control
Operations/Maintenance	Evaluate/Steady State
Disposition	Steady State

Figure 2

During the Initiation Phase, Privacy impact implications need to be examined by agencies and staff offices. If privacy issues are identified, a Privacy Impact Assessment (PIA) and System of Records (SOR) Notice must be prepared.

2 POLICY

All USDA agencies and staff offices will select a SLC/SDLC and implement the appropriate baseline security controls during the life of all IT systems. In order to be most effective the security controls will be integrated into the SLC/SDLC from the system inception. Legacy systems will have the appropriate security controls established, where not cost prohibitive, at the current SLC/SDLC Phase. System owners will identify the Information System Security Officer (ISSO) and agency Information Systems Security Program Manager (ISSPM) when the system is in the Initiation Phase of the SLC/SDLC or the current SLC/SDLC phase for legacy systems.

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 timeframes; 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 a updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

The following section describes the roles of individuals in this process and provides more detail on each of the security control requirements in the SLC/SDLC.

a Key Roles and Responsibilities. Many participants can have a role in information system development depending on the nature and scope of the system. The names for the roles and titles will vary among organizations. Not every participant works on every activity within a phase; the determination of which participants need to be consulted in each phase is as unique to the organization as the development. With any development, it is important to involve the ISSPM, ISSO, Records Management Officer and Privacy Act Officer as early as possible, in the initiation phase.

A list of key roles is provided below. This list includes roles that are important to many information system acquisitions. In some small organizations, a single individual may hold multiple roles.

(1) Chief Information Officer (CIO) – The CIO is responsible for the organization's information system planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture.

(2) Contracting Officer (CO) – The CO is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

(3) Contracting Officer's Technical Representative (COTR) – The COTR is a qualified employee appointed by the CO to act as their technical representative in managing the technical aspects of a particular contract.

(4) Information Technology Investment Board (or equivalent) – The Information Technology (IT) Investment Board, or its equivalent, is responsible for managing the Capital Planning and Investment Control (CPIC) process defined by the Clinger-Cohen Act of 1996 (Section 5).

(5) Information Systems Security Program Manager (ISSPM) – The ISSPM is responsible for developing enterprise standards for information security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks to the organization. Information security program managers coordinate or perform system risk analyses, analyze risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats. They also support senior management in ensuring that security management activities are conducted as required to meet the organization's needs.

(6) Information System Security Officer (ISSO) – The ISSO is responsible for ensuring the security of an information system throughout its life cycle.

(7) Program Manager (owner of data)/Acquisition Initiator/Program Official – This official represents

programmatic interests during the acquisition process. The program manager, who has been involved in strategic planning initiatives of the acquisition, plays an essential role in security and is, ideally, intimately aware of functional system requirements. This manager also ensure that security control requirements are met during the entire life cycle.

(8) Privacy Act Officer – This individual is responsible for ensuring that the services or system being procured meet existing privacy policies regarding protection, dissemination (information sharing and exchange) and information disclosure.

(9) Legal Advisor/Contract Attorney – This person is responsible for advising the team on legal issues during the acquisition process.

(10) Records Management Officer – The Records Management Officer is responsible for working with the program/project manager to ensure that the business, system/application, data and project records are maintained according to agency-approved records control schedules. For those records deemed unscheduled, the Records Management Officer will work with the program manager to schedule those records as required by DR 3080-1. Records Disposition.

The list of roles in an information system development can grow with he complexity involved in acquiring and managing information systems. It is vital that all development team members work together to ensure that a successful development is achieved. Because the System Certifying Official (CO) and Designated Accrediting Authority (DAA), defined in CS guidance on Certification and Accreditation, must make critical decisions throughout the development process, they should be included as early as possible in the process. System users may assist in the development by helping the program manager to determine the need for the system and refine the requirements. Participants may also include personnel who represent IT, configuration management, design and engineering, and facilities groups.

b Expressing Security Needs. Articulation of the desired system security properties is necessary in order to integrate security into the SLC/SDLC. When an organization determines a system's security, those needs are referred to as "security requirements" and become part of the function requirements process. As explained below, the first phase in the SLC/SDLC is Initiation. During this phase, an organization determines its information security requirements that are often developed by successive refinement. The articulation of requirements starts at a high level of abstraction, often centered on the security objectives for the system. The high-level security requirements for the organization may include information security policy and enterprise security architecture. High-level requirements are the basis for more detailed functional requirements. Additional specificity is then added to the high-level security requirements.

Because a SLC/SDLC can extend many years or more, multiple different project personnel and supporting service providers could fulfill each role over the life of the system. The security characteristics of the system will evolve over this system lifecycle along with most other system characteristics. The system requirements documentation should be placed under configuration management control, from the inception of the system, as part of the total set of system documentation that evolves over the lifecycle.

c Detailed Data on SLC/SDLC Security Requirements. Each agency will follow the security control requirements outlined below during all stages of the system life cycle:

(1) *Initiation Phase*. This is the first phase in the SLC/SDLC. This section identifies security requirements such as valuation of the system assets, function requirements and the development of the Interconnectivity Security Agreement (ISA). In addition, a formal process of system change control begins.

(a) Valuation of System Assets – Each Business Owner needs to determine the value and sensitivity of data to meet program delivery requirements. This starts when a Business Case is developed for the system. The primary source of the business case information is the system owner and a secondary source is the system documents. USDA Risk Assessment Methodology defines this process in more detail and provides a model for identification of sensitive data.

(b) Preparation of the Interconnectivity Security

Agreement (ISA) - If this system will be connected to other IT systems, the business owner must discuss the requirements for connectivity with the other system's business owner and work to identify the security requirements for this connection. The ISA is started during this phase of the SLC/SLC/SDLC, is refined during the Acquisition/Development Phase but the ISA may not be completed until the actual system Implementation Phase. An ISA will be done for each system that will be connected to the new system.

(c) Privacy Implications – Each agency needs to determine the privacy implications to individuals at the inception of systems development. If there are privacy concerns, a Privacy Impact Assessment (PIA) is conducted and a System of Records (SOR) Notice is prepared for the system.

(d) Preliminary Risk Assessment – Conduct an assessment of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate. This assessment should result in a brief initial description of the basic security needs of the system, should define the threat environment in which the product or system will operate and define a potential set of countermeasures. This assessment is followed by an initial identification of required security controls that must be met to protect the product/system in the intended operational environment. The risk-based approach to information security is defined in NIST SP 800-30, Risk Management Guide for Information Technology Systems.

(e) Security Categorization – Define the level (i.e., low, moderate, or high) of potential impact on the agency or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, provides a standardized approach for establishing security categories for an organization's information and information systems. The security categories reflect the potential impact to an organization if events occur that jeopardize information systems necessary to accomplish the assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization by operating an information system. FIPS Publication 199 defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). These standards assist agencies in making the appropriate selection of security controls for their information systems.

(f) System Change Control – After completing all requirements of this phase, a system of change control should begin the Configuration Management (CM) Process and a formal CM Plan should be developed.

(2) *Acquisition / Development Phase*. This is the second phase in the SLC/SDLC during which the system is developed and acquired. This section identifies security requirements that need to be performed during this time. In order to enter this SLC/SDLC Phase, an ISA must be started, a valuation of system assets must have been completed and a Preliminary Risk Assessment must have been performed.

(a) Risk Assessment – Perform an analysis that identifies the protection requirements for the system through a formal risk assessment process. The first step in analyzing the security functional requirements is to identify the protection requirements for the system through the formal risk assessment process. This analysis will build on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific. In addition to considering the security perspective of the system being acquired, agencies should also consider that the system might affect other USDA systems to which it will be directly or indirectly connected. One way to incorporate the context is to have an enterprise security architecture. Without a USDA enterprise perspective, the acquisition could be sub-optimal, even to the extent of introducing vulnerabilities. If the enterprise context is not considered, there is a possibility that the system being acquired could compromise the other USDA systems.

Each USDA system should address several enterprise-wide security objectives:

(1) A specific system should not create vulnerabilities or unintended interdependencies in other enterprise systems.

(2) A specific system should not decrease the availability of other enterprise systems.

(3) The security posture of the set of all the enterprise systems should not be decreased because of this specific system.

(4) External domains not under enterprise control should be considered potentially hostile entities. The systems connected to such external domains must analyzed and attempts made to counter hostile actions originating from these domains.

(5) Security specifications should be appropriate for the given state of the system environment.

(6) Security specifications should be stated clearly to convey the desired functions and assurances to the enterprise system product team and the developers.

(7) Implemented specifications should sufficiently reduce the risks to the system and to the USDA mission that the system supports.

The security risk assessment should be conducted before the approval of design specifications. In addition, a security risk assessment can provide justification for specifications. The selection of appropriate types of safeguards or countermeasures should take into consideration the results of the security assurance requirements analysis.

(b) Security Functional Requirements Analysis – Perform an analysis of requirements that include the following components: (1) system security environment, (i.e., enterprise information security policy and enterprise security architecture) and (2) security functional requirements. This process should include an analysis of laws and regulations, such as the Privacy Act, FISMA, OMB circulars, agency enabling acts, NIST Special Publications and FIPS, and other legislation and federal regulations, which define baseline security requirements.

(c) Security Assurance Requirements Analysis – Conduct an analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal, privacy and security functional requirements, will be used as the basis for determining how much and what kinds of assurance are required. As with other aspects of security, the goal should be cost-effective assurance that meets the requirements for protection of agencies' information assets and legal mandates. In each situation, a balance should exist between the benefits to mission performance from system security and the risks associated with operation of the system without security.

(d) Cost Considerations and Reporting – Determine how much of the development cost can be attributed to information security over the life cycle of the system. The task of identifying costs attributable to security can be complex. The best input for this task comes from the risk management process. As previously described, the risk assessment results in recommended controls that will mitigate the identified vulnerabilities. In the second step, risk mitigation, agencies conduct a cost-benefit analysis on the recommended controls to determine whether they are cost effective given the likelihood of an incident and the potential impact to the organization. Once the controls are selected, the cost of each can be totaled for an overall security cost. Including security at the beginning of the SLC/SDLC is often considered the most cost effective approach for two reasons: (1) it is usually more difficult to add functionality into a system after it has been built; and (2) it is frequently less expensive to include the preventive measures to deal with the cost of a security incident.

(e) Security Planning – Ensure that agreed upon security controls, planned or in place, are fully documented in a system security plan. This plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program. FISMA requires agencies to have plans for information security programs to assure adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate. The security plan also provides a complete characterization or description of the information system. Attachments may include references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones). Evaluate and refine the ISA for this system with the other system owner (s) as needed.

(f) Security Control Development – Ensure that security controls described in the respective security plans are designed, developed, and implemented. Security plans for information systems currently in operation may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective.

(g) Developmental Security Test and Evaluation – Make certain that security controls developed for a new information system are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the information system is deployed. These controls are typically at the management and operation level. For those security controls that can be assessed prior to deployment, develop a Security Test and Evaluation Plan (STE). This plan guides the developmental security testing and evaluation of the security controls and provides important feedback to information system developers and integrators. The team performing the STE needs to be independent of the System Development Team.

(h) Other Planning Components – Ensure that all necessary components of the development process are considered when incorporating security into the life cycle. Several other parts of the Acquisition / Development phase contribute to IT security. Some components have been highlighted below; others can be found in NIST Special Publication 800-64.

1 Type of Contract- The type of contract (for example, firm fixed price, time and materials, cost plus fixed fee, etc.) can have significant security implications. Part of the considerations must include Background Investigations and Security Clearances required based on the value and sensitivity of the system. The IT security technical experts developing the specifications and the contracting officer should work together closely to select the contract type that will be most advantageous to the organization.

2 Review by Other Functional Groups- Depending on the size and scope of the system, a team or group of participants from various functional groups (for example, legal, human resources, information security, physical security, etc.) may be useful. For all IT systems, it is important to obtain assistance from the information security staff in terms of appropriate security controls early in the system life cycle.

3 Review by Certifying Official and DAA – OMB Circular A-130, Appendix III, requires that systems be approved, or authorized, to process data in specific environments. Management and operational security controls should be employed to protect the system. Additionally, the technical security functional and assurance security specifications must be contained in the contract with the developer. These security controls should be factored into the development of the technical specifications. The DAA can take these assumptions into account when deciding on the adequacy of the total set of security controls for reducing the residual risks to an acceptable level. The management and operational security controls can sometimes be outside the scope of the contract. In particular, the developer obviously cannot be responsible for the

organization's implementation of these security controls. In contrast, C&A testing also includes management and operational security controls implemented by the organization. Determination of the efficacy of these organization-implemented security controls is part of C&A testing. C&A processes should confirm that the assumptions in the system security requirements have been implemented as assumed and that the total set of security controls are adequate to reduce the residual risks to an acceptable level. Acceptance testing of the security properties of the contractor-developed system is a prerequisite to security testing as part of the C&A process. Because the DAA is responsible for the value and sensitivity of data, the C&A Process and accepting the risk of operating the system, they can advise the development team if the risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the DAA is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages. The development team and the DAA should also discuss the forms of evidence that they need to make a decision. This evidence may include system test results and other data. In addition, the acquisition initiator and the DAA should discuss how changes to the system and its environment would be addressed.

4 Continue System Change Control – System Change control takes on a significant role in the management of the development and acquisition tasks and during the requirements gathering and development. Once agreed to by all parties, the system requirements are baselined in the Change Control process. This baseline continues to be updated and maintained during the design and system development phase. The baseline and all changes must be reviewed, approved and tasks

completed prior to moving to the Implementation Phase.

(3) *Implementation Phase*. This is the third phase of the SLC/SDLC during which the system will be installed and evaluated in the operational environment of the organization. This section identifies security requirements that need to be performed during this time. In order to enter this SLC/SDLC Phase, the Risk Assessment, the STE and the ISA have to be completed and signed by the DAA, and all other requirements of the Acquisition/Development Phase must have been accomplished.

(a) Inspection and Acceptance – Ensure that the organization validates and verifies that the functionality described in the specification is included in the deliverables. Inspection and acceptance refers to the Government's decision to inspect, accept and pay for a deliverable. The Government should take care when accepting deliverables. Testing by the Government or an Independent Validation and Verification (IV&V) contractor to determine that the system does meet the specifications can be very useful. Testing should include the security of the system.

(b) Security Control Integration – Make certain that security controls are integrated at the operational site where the information system is to be deployed for operation. Integration and acceptance testing occurs after delivery and installation of the information system. Security control settings and switches are enabled in accordance with manufacturer instructions and available security implementation guidance, such as the Trusted Facility Manual (TFM) for the system.

(c) Security Certification – Ensure that the controls are effectively implemented through established verification techniques and procedures within the system certification process. Actions of the Certification Team give agency officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. FISMA requires periodic testing and evaluation of the security controls in an information system to ensure that the controls are effectively implemented. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures is a critical activity conducted by the agency. In addition to security control effectiveness, security certification also uncovers and describes the actual vulnerabilities in the information system. The determination of security control effectiveness and information system vulnerabilities provides essential information to authorizing officials to facilitate credible, risk-based, security accreditation decisions.

(d) Security Accreditation – Ensure that the necessary security authorization of an information system to process, store, or transmit information is obtained. OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information. This authorization (also known as security accreditation), granted by a senior agency official, is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations (including mission, functions, image, or reputation). The security accreditation decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process. An authorizing official relies primarily on: (i) the completed security plan; (ii) the security test and evaluation results; and (iii) the plan of action and milestones for reducing or eliminating information system vulnerabilities, in making the security accreditation decision on whether to authorize operation of the information system and to explicitly accept the residual risk to agency assets or operations.

(e) System Change Control – Change control continues during this time to ensure that the system has been designed and developed in accordance with the baseline and system requirements.

(4) *Operations / Maintenance Phase*. This phase is the fourth phase of the SLC/SDLC during which systems are in place and operating, enhancements and modifications to the system are developed and tested. Hardware and software is added or replaced. This section identifies security requirements necessary in during this time. In order to enter this SLC/SDLC Phase, the system must have been Certified

and Accredited by an authorized DAA who has granted authority for the system to operate or approved an Interim Authority To Operate and mitigation strategy for the system. All other requirements of the Implementation Phase must have been accomplished.

(a) Configuration Management and Control – Ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment of the system. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation. An effective agency configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

(b) Continuous Monitoring – Make certain that control continue to be effective in their application through periodic testing and evaluation. FISMA requires periodic and continuous testing and evaluation of the security controls in an information system to ensure that the controls are effective in their application. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits.

(5) *Disposition Phase.* Disposition is the final phase in the SLC/SDLC. In order to enter this phase, the DAA grants authority to retire the system after the Agency CIO approves the proposed system retirement and determine

that other USDA systems are not impacted. This section identifies security requirements that need to be performed during this time.

(a) Information Preservation – Electronic records created or received by USDA must be managed as federal records, as required by the Federal Records Act, to support USDA business and assure the public that USDA employees are accountable for their actions. Federal electronic records must be managed throughout the records life-cycle and ensure the reliability and authenticity of USDA's records as legal evidence of their actions and decisions. Electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States; agencies must consult with agency records office regarding retaining and archiving federal records.

(b) Configuration Management and Control – After the decision has been made to retire the system, the final system baseline is frozen and all CM documents are included in the information preservation process.

(c) Media Sanitization– Make certain that data is deleted, erased, and written over, as necessary. Protection of information system hardware usually requires that residual magnetic or electrical representation of data be deleted, erased, or written over and that any system components with nonvolatile memory are erased. This residual information may allow data to be reconstructed, providing access to sensitive information by unauthorized individuals. The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide various levels of protection. A distinction can be made between clearing information and purging information. Clearing information is removal of sensitive data from a storage device at the end of a processing period in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities. Purging is the removal of data from a storage device at the end of a processing period in such a way that there is assurance, proportional to the sensitivity of the data, and that the data may not be reconstructed except through open-ended laboratory techniques. Several commercially available software utilities are available to clear and purge information from an information system so that it cannot be later reconstructed except by very sophisticated and expensive laboratory techniques.

(d) Hardware and Software Disposal – Ensure that hardware and software is disposed of as directed by the ISSO. Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation. The disposition of software should comply with license or other agreements with the developer and with government regulations. There is rarely a need to destroy hardware, except for some storage media that contains sensitive information and that cannot be sanitized without destruction. In situations in which the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be sold or given away. Some systems may contain sensitive information after the storage media is removed. If there is doubt whether sensitive information remains on a system, the ISSO should be consulted before disposing of the system.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Establish policy and guidance for the inclusion of security controls in the SLC/SDLC for all USDA IT systems;

(2) Work with other agencies and staff offices to develop necessary security functionality;

(3) Perform compliance reviews of USDA IT systems to ensure that a SLC/SDLC has been established and security controls have been implemented as required by this policy;

(4) Based on review results evaluate if security controls for systems provide the proper level of security and work with agencies to resolve vulnerabilities; and

(5) Review, process and make security recommendations to the CIO for all IT Waiver requests.

b Agency Chief Information Officer (CIO) will:

(1) Implement internal procedures establishing requirements for an appropriate SLC/SDLC to be used for all agency IT systems beginning with system inception, wherever possible;

(2) Establish internal procedures that call for security controls to be implemented at each phase of the SLC/SDLC and ensure that systems do not move from one phase to another without meeting the mandated security requirements of the prior phase;

(3) Ensure that all system administrators, developers, IT personnel and security officials are familiar with the requirements of this policy;

(4) Ensure that all agency IT systems are Certified and Accredited;

(5) Perform routine reviews to determine that a SLC/SDLC is documented for all IT systems and that appropriate security controls have been validated based on the information contained in the system and impact to the agency mission;

(6) Ensure that legacy systems have security controls established based on the stage in the SLC/SDLC, security baseline and cost effectiveness;

(7) Assure that an ISSO and ISSPM have been formally established for all agency IT systems; and

(8) Ensure that a formal waiver has been requested for all non-compliant systems to provide additional time to conform to this policy.

c The agency Information Systems Security Program Managers(ISSPM) will:

(1) Read and become knowledgeable with the requirements of this policy;

(2) Ensure that all agency systems have an identified SLC/SDLC for all IT systems and that it is documented;

(3) Coordinate with agency System Developers, Administrators and other IT personnel to ensure that security functional requirements are developed and that controls are implemented based on the SLC/SDLC phase the system is currently in;

(4) Perform system validations of security controls on a periodic basis and report results to the agency CIO;

(5) Participate in new system development by identifying appropriate security controls based security baselines; and

(6) For changed systems, evaluate the implications on security and work with IT staff to ensure security is modified, as required.

- END -

TABLE 1
INTERCONNECTION SECURITY AGREEMENT

Purpose – The purpose of this Interconnection Security Agreement (ISA) is to identify and document to all signatories satisfaction:

- Existing risks and mitigation strategies for all of the systems being interconnected, regardless of whether they are General Support Systems (GSS) or Major Applications (MA). Note: Any automated process that relies on Information Technology (IT) must be considered either a GSS or a MA.

- Any additional risks and mitigation strategies introduced through the interconnection of these systems for all participating systems. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, "Security Guide for Interconnecting Information Technology Systems" states *"A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. The document describes various benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection."*

- Documentation of all systems impacted by the interconnection, regardless of their participation in this agreement. (In the event a MA or GSS is not a signatory to this agreement, their role in the interconnection must be documented and a separate ISA must be prepared.)

- Provide appropriate levels of assurance (appropriate is very subject, might be well to include specifics) in accordance with NIST SP 800-47 and to the satisfaction of all signatories that the documented risk and mitigation strategies are operating as stated and are effective.

INTERCONNECTION STATEMENT OF REQUIREMENTS – This section shall contain:

- a clear description of the systems covered by this agreement,

- each systems intended purpose and target community,

- data sensitivity (information to and from systems is ***Sensitive-but-Unclassified*** unless specified otherwise),

- a description of the interconnection, including a graphic representation of the interconnection, the purpose of the interconnection and a clear description of the authorities under which all of the systems operate. This can include statutory/regulatory requirements, project goals and should also clearly state the responsible management unit and system owner.

This agreement shall be reviewed and updated on an annual basis or should be amended whenever major changes to the systems concerned are planned and executed. A changelog and a new signature page should be attached whenever these events occur.

SYSTEM SECURITY CONSIDERATIONS – General information, data descriptions and data/work flows shall be documented in this section as well as risks and mitigation strategies so that a clear picture is presented to each participant of any residual risk. Any residual risks should be associated with either the business or mission component, administrative component or the customer component. To that end, the following documents shall be included (where data sensitivity allows) to the ISA:

- **Risk Assessments –** Risk Assessments for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended Risk Assessment shall become an attachment to this agreement. A copy of the Residual Risks accepted by the DAA should also be included.

- **System Security Plans –** System Security Plans for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended System Security Plan shall become an attachment to this agreement.

- **Configuration Management Plan –** Configuration Management Plans for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended Configuration Management Plan shall become an attachment to this agreement.

- **Trusted Facilities Manual –** Trusted Facilities Manuals for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended Trusted Facilities Manual shall become an attachment to this agreement. (isn’t the TFM a rather large document…might consider referencing it or parts of it that apply)

- **Security Test and Evaluation Plan/Report –** Security Test and Evaluation Plans and subsequent reports for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the Security Evaluation Report shall become an attachment to this agreement.

- **Miscellaneous Security Assurance –** Additional citations should be included to address any additional security concerns and any deviations from USDA or NIST Guidance and/or Policy. Additional citations should also be included for USDA policies that delegate specific security responsibilities to agencies/staff offices for execution. Examples include, but are not limited to:
    - **Incident Reporting**
    - **Employee/Contractor Trusted Behavior Expectations**
    - **Information Exchange Security**
    - **Maintenance and Review of appropriate records, logs and audit trails**
    - **Applicable Certification & Accreditation/Interim Authority to Operate**
    - **Any other agency/staff office policies or practices**

EXECUTIVE SUMMARIES/SIGN-OFF – An Executive summary shall be prepared that details all residual risks and is tied directly to the portion of the ISA that contains all appropriate signatures. Conditions for revocation of an ISA authority shall appear in this area as well. Once the ISA has the appropriate signatures, the original will be retained by the System Owner and copies will be provided to those whose systems are impacted by the interconnection. Cyber Security retains the right to review the ISA for compliance with the requirements of Table 1. The ISA will be retained by the system owner with the other system documentation for certifications and accreditation, compliance reviews and audit purposes. All changes to this official ISA will be executed whenever a major change to the system occurs.