



1400 Independence Ave., SW  
Washington, DC 20250

---

**USDA**  
INFORMATION SECURITY  
**EXECUTIVE BRIEFING HANDBOOK**

July 30, 2004

---

This page intentionally left blank.

# USDA Information Security Executive Briefing Handbook

## Table of Contents

---

Overview.....	1
Why Security Is Important.....	3
Security Legislation, Regulations & Guidance.....	5
Your Security Responsibilities .....	11
Certification and Accreditation.....	15
Security Program Requirements .....	21
Good Security Practices .....	23
Additional References.....	27

### Appendices

APPENDIX A - Certification and Accreditation.....	A-1
APPENDIX B - Categorizing Information & Information Systems .....	B-1
APPENDIX C - Risk Management.....	C-1
APPENDIX D - System Security Plans.....	D-1
APPENDIX E - Continuity of Operations/Disaster Recovery .....	E-1
APPENDIX F - Security Awareness and Training.....	F-1
APPENDIX G - Security Controls Review .....	G-1
APPENDIX H - Personnel Security .....	H-1
APPENDIX I - Configuration Management.....	I-1

This page intentionally left blank.

# USDA Information Security Executive Briefing Handbook

## Overview

---

### Introduction

As an Agency Head, Chief Information Officer, senior agency executive, or manager, you are responsible for providing adequate security for the information and information systems that support the operations and assets under your control. To successfully carry out that responsibility, you need to be aware of

- why security is important
- what the agency's security requirements are, and
- what your role is in meeting these requirements.

This handbook addresses each of these topics and seeks to heighten your overall security awareness and knowledge.

---

### Contents

This handbook contains the following topics:

Topic	See Page
Why Security Is Important	3
Security Legislation, Regulations & Guidance	5
Your Security Responsibilities	11
Certification and Accreditation	15
Security Program Requirements	21
Good Security Practices	23
Additional References	27

---

This page intentionally left blank.

# Why Security Is Important

---

## Why Security is Important

Appropriate security measures *ensure the ability of the agency to achieve its mission.*

Whether it be providing economic opportunities for farmers,



ensuring a safe food supply,



---

*Continued on next page*

## Why Security Is Important, Continued

---

**Why Security is Important**  
(continued)

or caring for forests and range lands,



the accomplishment of our mission depends on *accurate, available information and systems that are protected from potential disclosure, tampering, and harm*. Good security ensures the confidentiality, integrity, and availability of our information and systems so that we can fulfill our mandate of “enhancing the quality of life for the American people by supporting production of agriculture.”

---

**Example:  
Blaster &  
Welchia Worm  
Attacks**

Several agencies within the USDA learned the hard way just how important security is when they were hit by the Blaster and Welchia worms in the summer of 2003. The worms, which infiltrated PCs, servers, and the e-mail system, resulted in system outages that lasted *several weeks*. Such outages cost the USDA not only the time and money it took to eradicate the worms, but also the

- *loss of employee productivity,*
- *inability to provide products and services, and*
- *loss of public confidence and trust.*

Had better security measures and practices been in place (such as ensuring the latest system patches have been installed, blocking executables in e-mails, and educating users on good security practices), the spread of the Blaster and Welchia worms could have been avoided or, at the very least, more easily and quickly contained.

---

# Security Legislation, Regulations & Guidance

---

## Introduction

A number of laws and a great deal of regulations and guidance exist today regarding information security. For the purposes of this handbook, we will limit our review to those that more directly affect the USDA and from which your security responsibilities derive.

Keep in mind as you peruse these that they were enacted to make sure that you *are doing* the things you *should have been doing all along* to ensure the success of your Program and to protect those assets entrusted to you.

---

## Security Laws

The following table summarizes some of the more relevant security related laws and their associated requirements.

Title	Requirements
Federal Information Security Management Act of 2002 (FISMA) – [Title III of the E-Government Act of 2002]	Each government agency must <ul style="list-style-type: none"> <li>• develop, document, and implement an agency-wide information security program that includes:               <ul style="list-style-type: none"> <li>- periodic risk assessments</li> <li>- policies &amp; procedures</li> <li>- plans for providing adequate information security for networks, facilities &amp; systems</li> <li>- security awareness training</li> <li>- periodic testing &amp; evaluation of effectiveness of security plans, procedures, &amp; practices</li> <li>- process for planning, implementing, evaluating, &amp; documenting remedial actions to address deficiencies, and</li> <li>- plans &amp; procedures to ensure continuity of operations &amp; incident detection, reporting &amp; response.</li> </ul> </li> <li>• report annually to Congress on the adequacy and effectiveness of information security policies, procedures, and practices, and</li> <li>• ensure an independent evaluation of the agency’s information security program and practices is conducted annually.</li> </ul>

*Continued on next page*

## Security Legislation, Regulations & Guidance, Continued

---

### Security Laws (continued)

Title	Requirements
Privacy Act of 1974	<p>Each government agency must</p> <ul style="list-style-type: none"> <li>• establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.</li> </ul> <p>Allows individuals to</p> <ul style="list-style-type: none"> <li>• specify what information may be held by a government agency, and</li> <li>• obtain information held on them by the Federal Government.</li> </ul>
Clinger-Cohen Act of 1996	<p>Each government agency must</p> <ul style="list-style-type: none"> <li>• appoint a Chief Information Officer</li> <li>• implement a capital planning and investment control process, and</li> <li>• develop performance and risk-based management and measurement guidelines and methodologies for the use and procurement of information technologies.</li> </ul>

*Continued on next page*

## Security Legislation, Regulations & Guidance, Continued

### Security Laws (continued)

Title	Requirements
Paperwork Reduction Act of 1995	<p>Each government agency must</p> <ul style="list-style-type: none"> <li>• implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosures, and sharing of information collected or maintained by or on behalf of the agency</li> <li>• assume responsibility and accountability for compliance with the Computer Security Act and related information management laws, and</li> <li>• identify and afford security protections commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the agency.</li> </ul>
Government Paperwork Elimination Act of 1998 (GPEA)	<p>Each government agency must</p> <ul style="list-style-type: none"> <li>• allow individuals the option to submit information or transact with the agency electronically, and to maintain records electronically, when practicable.</li> <li>• not deny electronic signatures legal effect, validity, or enforceability.</li> </ul>

*Continued on next page*

## Security Legislation, Regulations & Guidance, Continued

### Security Regulations & Guidance

The following table summarizes some of the more relevant security related regulations, policies, and guidance and their associated purpose and/or intent.

Title	Purpose/Intent
OMB Circular No. A-130, Management of Federal Information Resources (Appendix III), 11/00	Establishes a minimum set of management controls for security programs, including <ul style="list-style-type: none"> <li>• assigning responsibility for security</li> <li>• developing a System Security Plan</li> <li>• screening &amp; training users</li> <li>• assessing risk</li> <li>• planning for disasters &amp; contingencies, and</li> <li>• reviewing security safeguards at least every 3 years.</li> </ul>
OMB Circular No. A-123, Management Accountability and Control, 6/95	<ul style="list-style-type: none"> <li>• Provides guidance to managers on improving accountability &amp; effectiveness of programs and operations.</li> <li>• Provides policy for management accountability &amp; management controls.</li> </ul>
OMB Circular No. A-127, Policies and Standards for Financial Management Systems, 7/93	<ul style="list-style-type: none"> <li>• Prescribes policies &amp; procedures for developing, operating, evaluating &amp; reporting on financial management systems.</li> </ul>
OMB Bulletin No. 90-08 (Appendix A) [Security Plans]	<ul style="list-style-type: none"> <li>• Provides guidance on the content and format of System Security Plans.</li> </ul>
FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 12/03	<ul style="list-style-type: none"> <li>• Establishes standards to be used to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.</li> </ul>

*Continued on next page*

## Security Legislation, Regulations & Guidance, Continued

### Security Regulations & Guidance (continued)

Title	Purpose/Intent
NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems	<ul style="list-style-type: none"> <li>• Establishes a baseline for the review of Information Technology (IT) security programs.</li> <li>• Presents basic security requirements applicable to most IT systems.</li> </ul>
NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems	<ul style="list-style-type: none"> <li>• Provides a guide for creating security plans for major applications and general support systems.</li> </ul>
NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems	<ul style="list-style-type: none"> <li>• Utilizes an extensive questionnaire containing specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured.</li> </ul>
NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems	<ul style="list-style-type: none"> <li>• Provides guidance for the development of an effective risk management program.</li> <li>• Provides guidance on the selection of cost-effective security controls.</li> </ul>
NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems	<ul style="list-style-type: none"> <li>• Provides guidance on the certification and accreditation process.</li> </ul>
NIST Special Publication 800-50, Building an Information Technology Security Awareness & Training Program	<ul style="list-style-type: none"> <li>• Provides guidance for building an effective information technology (IT) security program.</li> </ul>
NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems	<ul style="list-style-type: none"> <li>• Provides guidelines for selecting and specifying security controls for information systems.</li> </ul>

*Continued on next page*

## Security Legislation, Regulations & Guidance, Continued

---

### Security Regulations & Guidance (continued)

Title	Purpose/Intent
NIST Special Publication 800-60, Guide for Mapping Types of Information & Information Systems to Security Categories	<ul style="list-style-type: none"><li>• Provides guidelines for mapping types of information and information systems to security categories.</li></ul>
USDA Policies & Regulations [See the “Additional References” section for a listing of policies and guidance.]	<ul style="list-style-type: none"><li>• Establish policies and procedures for ensuring security and compliance with applicable laws &amp; regulations within the USDA.</li></ul>

---

### Additional References

A listing of additional pertinent security laws, regulations, and guidance, and the web sites where you can find them, is provided in the last section of this Handbook for your reference.

---

# Your Security Responsibilities

## Introduction

As an Agency Head, you are responsible for developing and maintaining a dedicated, independent security program. As a Chief Information Officer, senior agency executive, or manager, ***you play a key role*** in ensuring the security of the USDA’s information and assets. Through your ***direction and example***, sound information security procedures and practices will become standard within your agency. This section seeks to familiarize you with your security responsibilities so that you will be better able to fulfill them.

## Executive/ Management Responsibilities

The following table depicts your security responsibilities, along with the source from which that responsibility is derived. Where applicable, a summary of what the responsibility entails in terms of requirements (as extracted from its source/s) is also provided.

One of your ***key responsibilities*** is to ***manage and accept residual risk through the process of Certification and Accreditation (C&A)***. Given its importance and priority, additional guidance on C&A is provided in the next section.

**Note:** Specific requirements related to your responsibility to implement and maintain a Security Program are discussed in a separate section.

Security Responsibility	Source/s
Recognize that <b><i>risks to USDA’s environment CAN impact your mission!</i></b>	N/A
Maintain a dedicated independent <b><i>Security Program</i></b> in accordance with FISMA requirements that includes: <ul style="list-style-type: none"> <li>• System Security Plans (SSPs)</li> <li>• risk assessments</li> <li>• policies &amp; procedures to reduce risk</li> <li>• security awareness training</li> <li>• testing &amp; evaluation of plans, procedures &amp; security controls</li> <li>• security incident detection, reporting, &amp; response procedures</li> <li>• Continuity of Operations/Disaster Recovery Plans, and</li> <li>• remedial action plans for security deficiencies.</li> </ul>	FISMA, OMB A-130, DR 3440-2, CS-002, CS-015, CS-016, CS-021, CS-025, CS-028, CS-031

*Continued on next page*

## Your Security Responsibilities, Continued

**Executive/  
Management  
Responsibilities** (continued)

Security Responsibility	Source(s)
<p><b><i>Incorporate security costs in capital planning</i></b> in accordance with Clinger-Cohen Act and FISMA requirements, including</p> <ul style="list-style-type: none"> <li>• implement a capital planning &amp; investment control process</li> <li>• develop performance &amp; risk-based management &amp; measurement guidelines &amp; methodology for the procurement &amp; use of IT technology</li> <li>• implement, manage &amp; monitor IT security programs</li> <li>• maximize the benefits of IT investments through a three-phased process: Select, Control, and Evaluate, and</li> <li>• ensure that security is part of the management process throughout the life cycle of an investment.</li> </ul>	<p>Clinger-Cohen Act, FISMA, OMB A-11, OMB A-130, CS-026</p>
<p>Effectively <b><i>manage risks</i></b> through security planning, and training and awareness. Specific requirements include</p> <ul style="list-style-type: none"> <li>• System Security Plans (SSPs)</li> <li>• Security Awareness &amp; Training Program</li> <li>• periodic security controls testing &amp; evaluation</li> <li>• periodic risk assessments</li> <li>• Capital Planning &amp; Investment Control (CPIC)</li> <li>• Continuity of Operations Plan (COOP)</li> <li>• Configuration Management Plan (CMP), and</li> <li>• System Certifications &amp; Accreditations (C&amp;As).</li> </ul>	<p>FISMA, Privacy Act, OMB A-130, CS-002, CS-009, CS-015, CS-016, CS-019, CS-021, CS-026, CS-027, CS-028, CS-030, CS-031</p>

*Continued on next page*

## Your Security Responsibilities, Continued

**Executive/  
Management  
Responsibilities** (continued)

<b>Security Responsibility</b>	<b>Source/s</b>
<p><i>Implement cost-effective safeguards</i> and controls that</p> <ul style="list-style-type: none"> <li>• reduce risks to an acceptable level</li> <li>• ensure security throughout the information system life cycle</li> <li>• provide adequate security for networks, facilities, systems, and information</li> <li>• are periodically tested to ensure they are effectively implemented, and</li> <li>• comply with the requirements of FISMA, the USDA, &amp; other related policies, procedures, standards &amp; guidelines.</li> </ul>	<p>FISMA, Clinger-Cohen Act, Paperwork Reduction Act, OMB A-123, OMB A-130, DM 3200-2</p>
<p><i>Accept responsibility</i> for residual security risks by</p> <ul style="list-style-type: none"> <li>• conducting risk assessments</li> <li>• completing system Certifications &amp; Accreditations, and</li> <li>• authorizing processing.</li> </ul>	<p>FISMA, OMB A-130, CS-016, CS-030, CS-031</p>

This page intentionally left blank.

# Certification and Accreditation

---

## Introduction

In accordance with OMB Circular A-130 and CS-030, *all Major Applications (MAs) and General Support Systems (GSSs)*, including all information technology (IT) systems or applications owned, leased, operated, or connected to the USDA, *must be formally certified and accredited*. Certification and Accreditation (C&A) ensures that

- information systems operate with appropriate management review
- monitoring of security controls is ongoing, and
- re-accreditation occurs periodically and whenever a significant change occurs.

This section introduces the concepts of certification and accreditation and provides an overview of the C&A process.

*Note:* Additional information on the USDA C&A process is provided in Appendix A.

---

## Definition: Accreditation

*Accreditation* is the official management decision to authorize the operation of an information system.

This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the level of risk remaining to agency operations, assets, or individuals after the implementation of an agreed upon set of security controls.

---

## Definition: Certification

*Certification* is the comprehensive evaluation of management, operational, and technical security controls in an information system.

This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls.

---

*Continued on next page*

## Certification and Accreditation, Continued

---

**What's Involved in Accreditation?**

Accreditation involves determining residual risk to an agency's operations or assets and the acceptability of such risk given the confirmed vulnerabilities identified and the mission or business needs of the enterprise.

The accreditation decision is based on the results of the certification process, and is documented in an accreditation package consisting of

- the Accreditation Decision Letter signed by the authorizing official (known as the Designated Accrediting Authority (DAA), and
  - supporting documentation (which generally includes the certification package).
- 

**What's Involved in Certification?**

Certification involves evaluating the security controls of an information system to determine their effectiveness and identifying any remaining vulnerabilities. Certification results provide the factual basis for the authorizing official to render the accreditation decision.

At the completion of the certification process, a certification package is forwarded to the DAA with an accreditation recommendation. The certification package consists of the following documents:

- Security Controls Compliance Matrix
  - Security Test and Evaluation Report
  - Risk Assessment
  - System Security Plan
  - Security Evaluation Report
- 

**The C&A Process**

As outlined in the *USDA Certification and Accreditation Guide*, the C&A process is comprised of three phases:

1. Pre-Certification
2. Certification and Accreditation
3. Post-Accreditation

A brief description of each phase is provided in the table below. For more information on the steps involved in these phases, see Appendix A.

---

*Continued on next page*

## Certification and Accreditation, Continued

---

### The C&A Process (continued)

Phase	Description
1. Pre-Certification	Phase 1 involves <ul style="list-style-type: none"><li>• defining the scope of the C&amp;A effort</li><li>• identifying existing security controls</li><li>• reviewing the System Security Plan (SSP)</li><li>• reviewing the initial risk assessment, and</li><li>• negotiating with the participants.</li></ul>
2. Certification & Accreditation	Phase 2 involves <ul style="list-style-type: none"><li>• conducting system security testing and evaluation (ST&amp;E)</li><li>• updating the risk assessment with the ST&amp;E findings</li><li>• updating the SSP</li><li>• documenting the certification findings, and</li><li>• forwarding the certification package to the DAA for an accreditation decision.</li></ul>
3. Post-Accreditation	Phase 3 involves <ul style="list-style-type: none"><li>• managing the system configuration to ensure changes are monitored and do not adversely affect the security posture</li><li>• keeping the SSP current, including adding new security controls as they are implemented, and</li><li>• re-accrediting the system every 3 years or when a significant change occurs.</li></ul>

### What C&A Provides

The successful completion of C&A provides agency officials with the necessary assurances that the information system has appropriate security controls and that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing.

In essence, C&A provides a form of quality control that challenges managers and technical staff at all levels to implement the most effective security controls and techniques given technical constraints, operational constraints, cost and schedule constraints, and mission requirements.

---

*Continued on next page*

## Certification and Accreditation, Continued

---

### **C&A and the System Development Life Cycle**

Ideally, the C&A process should be integrated into the system development life cycle during the Capital Investment and Control Process (CPIC).

For systems in development, C&A activities should include writing the SSP and conducting the initial risk assessment. For operational and older systems, C&A may begin later in the life cycle. In either case, all C&A activities should be completed unless an exception has been granted by the USDA CIO.

---

### **C&A and the Risk Management Process**

C&A is a critical component of the overall risk management process. The following figure depicts the key activities in this process, which together combine to create a comprehensive information security program.

For each activity listed, National Institute of Standards and Technology (NIST) and/or USDA publications that provide specific direction and guidance on how to accomplish it are provided. Applying the guidance found in these publications will ensure a complete and comprehensive security program that meets USDA and federal requirements.

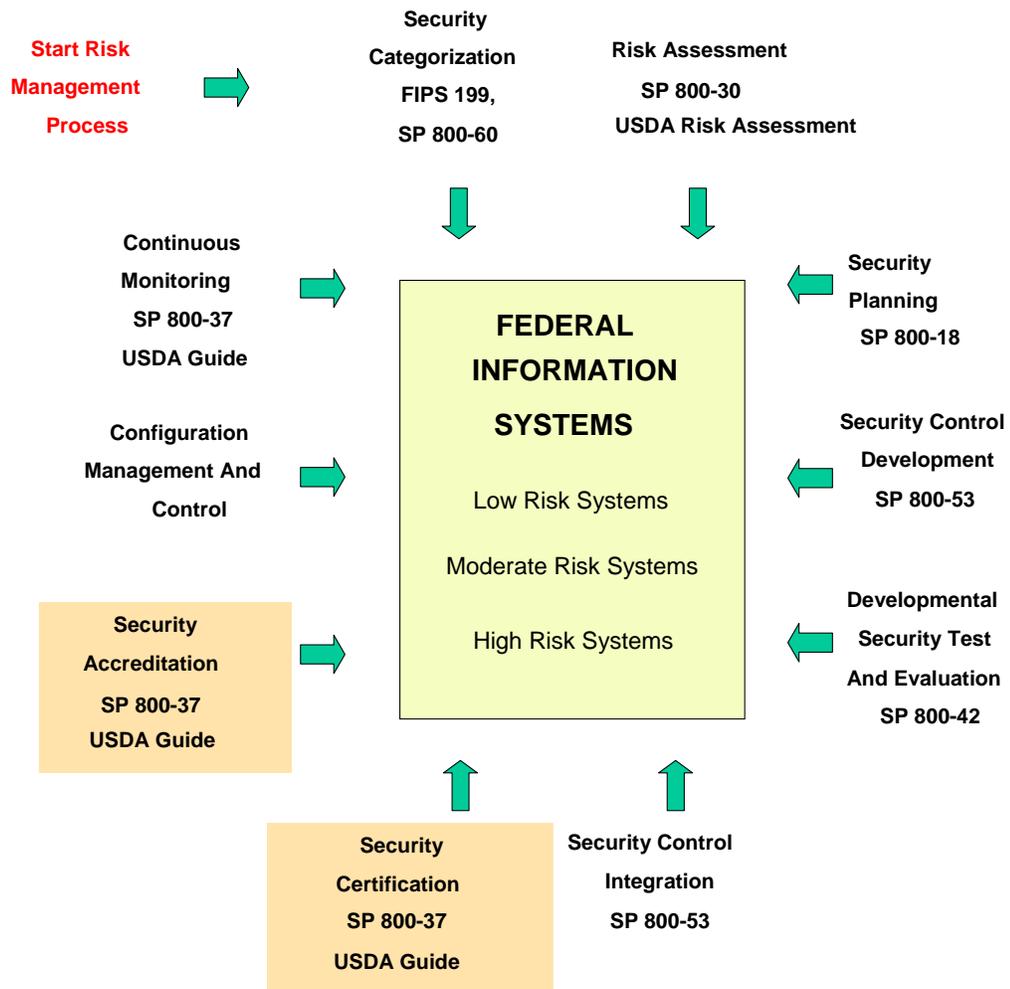
---

*Continued on next page*

# Certification and Accreditation, Continued

C&A and the Risk Management Process (continued)

## Information System Risk Management Process



This page intentionally left blank.

# Security Program Requirements

---

## Introduction

One of your biggest responsibilities is to *maintain a dedicated independent security program*. A comprehensive security program consists of policies, procedures, and plans that address the management, operational and technical security safeguards in place to protect your agency’s information and information systems. This section describes what you are required to include as part of your security program.

---

## Program Requirements & Components

The table below presents the requirements and associated components of your security program. To assist you in developing and maintaining your program, policies and guidance from NIST and the USDA Office of Cyber Security that offer information and procedural direction for each requirement are also provided. USDA Cyber Security policies are based on the NIST publications, which are in turn founded on security best practices and federal regulations such as FISMA.

More detailed information and guidance on program requirements and components is provided in Appendices B through H.

**Note:** A full listing and web location for each guidance publication mentioned can be found in the *Additional References* section.

Program Requirement/Activity	Program Component/s	Guidance
<i>Identify and categorize</i> sensitive systems	<ul style="list-style-type: none"> <li>• System Inventory</li> <li>• System Sensitivity Assessments/ Security Categorizations</li> </ul>	<ul style="list-style-type: none"> <li>• CS-019</li> <li>• FIPS PUB 199</li> <li>• NIST SP 800-18</li> <li>• NIST SP 800-37</li> <li>• NIST SP 800-60</li> </ul>
Conduct <i>periodic risk assessments</i> <ul style="list-style-type: none"> <li>• identify and mitigate ongoing or emergent threats</li> </ul>	<ul style="list-style-type: none"> <li>• System Risk Assessments</li> <li>• System Risk Mitigation Action Plans</li> </ul>	<ul style="list-style-type: none"> <li>• CS-016</li> <li>• CS-019</li> <li>• CS-031</li> <li>• FIPS PUB 31</li> <li>• NIST SP 800-30</li> <li>• NIST SP 800-37</li> </ul>

*Continued on next page*

## Security Program Requirements, Continued

### Program Requirements & Components (continued)

Program Requirement	Program Component/s	Guidance
Develop and maintain: <ul style="list-style-type: none"> <li>• System <i>Security Plans</i>,</li> <li>• <i>Continuity of Operations Plans</i></li> <li>• <i>Disaster Recovery Plans</i></li> <li>• <i>Security Awareness &amp; Training Program</i>, and</li> <li>• <i>Personnel security program</i> - coordinate with Human Resources &amp; Departmental Administration</li> </ul>	<ul style="list-style-type: none"> <li>• System Security Plans</li> <li>• Continuity of Operations Plans/Business Resumption Plans</li> <li>• Disaster Recovery Plans</li> <li>• Security Awareness &amp; Training Program Plan</li> <li>• Personnel Security Program</li> </ul>	<ul style="list-style-type: none"> <li>• CS-002</li> <li>• CS-015</li> <li>• CS-021</li> <li>• CS-025</li> <li>• CS-027</li> <li>• CS-028</li> <li>• FIPS PUB 87</li> <li>• NIST SP 800-16</li> <li>• NIST SP 800-18</li> <li>• NIST SP 800-26</li> <li>• NIST SP 800-34</li> <li>• NIST SP 800-50</li> <li>• NIST SP 800-53</li> </ul>
Implement, test, and review <i>security controls</i>	<ul style="list-style-type: none"> <li>• Security Control Development</li> <li>• Developmental Security Testing &amp; Evaluation</li> <li>• Security Control Integration</li> <li>• Annual Security Testing &amp; Evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• CS-006</li> <li>• NIST SP 800-14</li> <li>• NIST SP 800-18</li> <li>• NIST SP 800-26</li> <li>• NIST SP 800-37</li> <li>• NIST SP 800-42</li> <li>• NIST SP 800-53</li> <li>• NIST SP 800-53A</li> </ul>
<i>Certify &amp; Accredite</i> all Major Applications and General Support Systems	<ul style="list-style-type: none"> <li>• Certification Packages</li> <li>• Accreditation Letters</li> </ul>	<ul style="list-style-type: none"> <li>• CS-030</li> <li>• USDA C&amp;A Guide</li> <li>• NIST SP 800-37</li> </ul>
Implement and maintain <i>Configuration Management and change controls</i>	<ul style="list-style-type: none"> <li>• Configuration Management Program</li> </ul>	<ul style="list-style-type: none"> <li>• CS-009</li> <li>• NIST SP 800-12</li> <li>• NIST SP 800-14</li> </ul>
Continually <i>monitor your security program</i>	<ul style="list-style-type: none"> <li>• System Reviews</li> <li>• Re-accreditations</li> </ul>	<ul style="list-style-type: none"> <li>• CS-030</li> <li>• USDA C&amp;A Guide</li> <li>• NIST SP 800-37</li> </ul>

# Good Security Practices

---

## Introduction

Every user of the USDA's information systems has a responsibility to follow basic, good security practices such as those presented below. As you review these, keep in mind that *your behavior sets the example for your employees.*

---

## Good Security Practices: #1

Never share your userID and password!



## Good Security Practices: #2

Create strong passwords that are difficult to guess!



Combine upper and lower case letters with numbers and special characters.

---

## Good Security Practices: #3

Log out or lock your workstation before leaving it unattended!



---

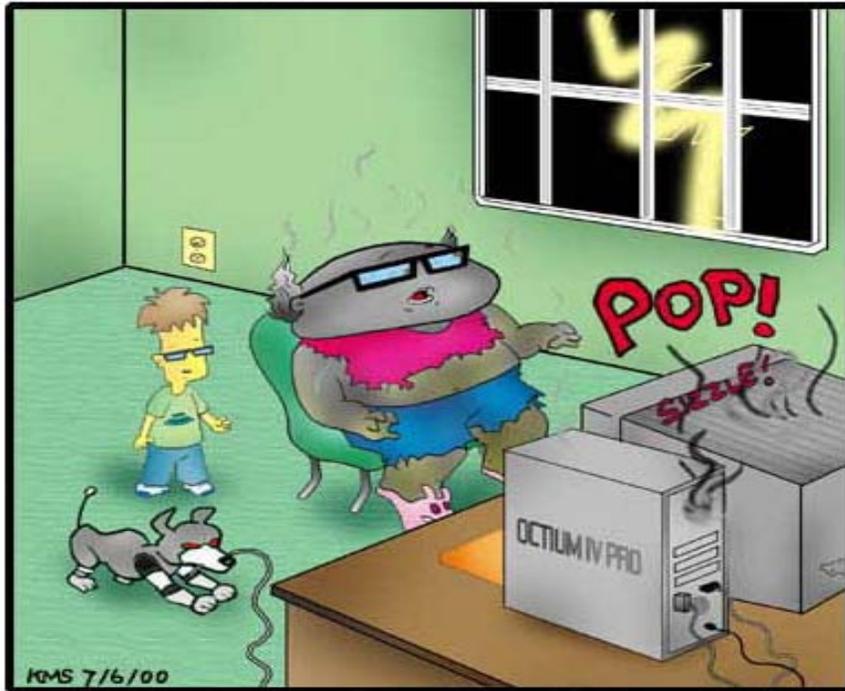
*Continued on next page*

## Good Security Practices, Continued

---

### Good Security Practices: #4

Backup your local hard drive!



In a bitter twist of irony, Bob suddenly realized he had forgotten to save his 250 page article on "Preventive Maintenance: The Importance of Making Back-ups"

---

### Good Security Practices: #5

Keep food and drink away from your system and keyboard!



*Continued on next page*

---

## Good Security Practices, Continued

---

### Good Security Practices: #6

Limit personal use of your system and services such as e-mail and the Internet.



### Good Security Practices: #7

Consider “Need to Know” before sharing information.



### Final Thought

While practicing good security can be inconvenient at times or somewhat burdensome, in the end it is what *ensures our ability to get the job done*. Because, as we all know, our systems are infallible, we never make mistakes, and ...

---

*Continued on next page*

## Good Security Practices, Continued

---

**Final Thought**  
(continued)



## Additional References

---

### Federal Laws

- **Privacy Act of 1974**, as amended, (5 U.S.C. 552a),  
[<http://www.usdoj.gov/04foia/privstat.htm>]
- **Computer Security Act of 1987**, P.L. 100-235  
[[http://crsc.nist.gov/secplcy/csa\\_87](http://crsc.nist.gov/secplcy/csa_87)]
- **Paperwork Reduction Act of 1995**, Title 44 Chapter 35  
[[http://www.archives.gov/federal\\_register/public\\_laws](http://www.archives.gov/federal_register/public_laws)]
- **Chief Financial Officers Act of 1990**, (31 U.S.C. 2512 et seq.)  
[[http://www.gao.gov/policy/12\\_19\\_4.pdf](http://www.gao.gov/policy/12_19_4.pdf)] and  
[<http://www.woirm.nih.gov/itmra/cfoact.html>]
- **Clinger-Cohen Act**, P.L. 104-106, Division E, Information Technology Management Reform Act of 1996 [<http://www.cio.gov/documents>]
- **Computer Security Enhancement Act of 1997**, H.R. 1903  
[[http://www.fas.org/irp/congress/1997\\_rpt/h105\\_243.htm](http://www.fas.org/irp/congress/1997_rpt/h105_243.htm)]
- **Government Paperwork Elimination Act of 1998**, P.L. 105-277, Title XVII [<http://www.cdt.org/legislations/105th/digsig/govnopaper.html>]
- **FY 2001 Defense Authorization Act (P.L. 106-398)** – Title X, subtitle G “Government Information Security Reform” (The Security Act)  
[<http://www.access.gpo.gov/nara/publaw/106publ.htm>]
- **Federal Information Security Management Act (FISMA)**, P.L. 107-347, Title III, December 2002  
[<http://www.fedcirc.gov/library/legislation/FISMA.html>]

---

### Executive Orders/ Presidential Decision Directives

- **Executive Order No. 12046 of March 27, 1978** [no electronic version available]
- **Executive Order No. 12472 of April 3, 1984** [no electronic version available]
- **Executive Order No. 13011 of July 16, 1996**  
[[http://www.nara.gov/fedreg/eo\\_clint.html](http://www.nara.gov/fedreg/eo_clint.html)]
- **Presidential Decision Directive – PDD 63** – Protecting America’s Critical Infrastructures (05/98) [<http://www.nipc.gov/about/pdd63.htm>]

---

*Continued on next page*

## Additional References, Continued

---

**Office of  
Management &  
Budget (OMB)  
Circulars,  
Bulletins and  
Memoranda)**

[<http://www.whitehouse.gov/omb>]

- **OMB Circular No. A-11** Preparation and Submission of Budget Estimates (05/03)
- **OMB Circular No. A-123** Management Accountability and Control (06/95)
- **OMB Circular No. A-127** Policies and Standards for Financial Management Systems (07/93)
- **OMB Circular No. A-130** Security of Federal Automated Information Resources (Appendix III) (11/00)
- **OMB Bulletin No. 90-08** (Appendix A) [Security Plans]
- **M-97-16** Information Technology Architectures (06/18/97)
- **M-99-05** Instructions on Complying with President’s Memorandum of May 14, 1998 “Privacy and Personal Information in Federal Records” (01/07/99)
- **M-99-18** Privacy Policies on Federal Web Sites (06/02/99)
- **M-99-00** Security of Federal Automated Information Resources (06/23/99)
- **M-00-07** Incorporating and Funding Security in Information Systems Investments (02/28/00)
- **M-00-10** OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (04/25/00)
- **M-00-13** Privacy Policies and Data Collection on Federal Web Sites (06/22/01)
- **M-00-15** OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (09/25/00)
- **M-01-05** Guidance on Inter-agency Sharing of Personal Data – Protecting Personal data (12/20/00)
- **M-03-19** Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (08/06/03)

---

*Continued on next page*

## Additional References, Continued

---

**National  
Institute of  
Standards &  
Technology  
(NIST) Federal  
Information  
Processing  
Standards  
Publications  
(FIPS)**

[<http://csrc.nist.gov/publications/fips/index.html>]

- **FIPS PUB 31** Guidelines for Automatic Data Processing Physical Security and Risk Management (06/74)
- **FIPS PUB 46-3** Data Encryption Standard (DES); specifies the use of Triple DES (10/99)
- **FIPS PUB 48** Guidelines on Evaluation of Techniques for Automated Personal Identification (04/77)
- **FIPS PUB 73** Guidelines for Security of Computer Applications (06/80)
- **FIPS PUB 74** Guidelines for Implementing and Using the NBS Data Encryption Standard (04/81)
- **FIPS PUB 81** DES Modes of Operation (12/80)
- **FIPS PUB 83** Guideline on User Authentication Techniques for Computer Network Access Control (09/80)
- **FIPS PUB 87** Guidelines for ADP Contingency Planning (03/81)
- **FIPS PUB 102** Guideline for Computer Security Certification and Accreditation (09/83)
- **FIPS PUB 112** Password Usage (05/85)
- **FIPS PUB 113** Computer Data Authentication (05/85)
- **FIPS PUB 140-1** Security Requirements for Cryptographic Modules (01/94)
- **FIPS PUB 140-2** Security Requirements for Cryptographic Modules (06/01)
- **FIPS PUB 171** Key Management Using ANSI X9.71 (04/92)
- **FIPS PUB 180-1** Secure Hash Standard (04/95)
- **FIPS PUB 181** Automated Password Generator (10/93)
- **FIPS PUB 185** Escrowed Encryption Standard (02/94)
- **FIPS PUB 186-2** Digital Signature Standard (DSS) (01/00)
- **FIPS PUB 188** Standard Security Labels for Information Transfer (09/94)
- **FIPS PUB 190** Guideline for the Use of Advanced Authentication Technology Alternatives (09/94)
- **FIPS PUB 191** Guideline for the Analysis of Local Area Network Security (11/94)
- **FIPS PUB 196** Entity Authentication Using Public Key Cryptography (02/97)
- **FIPS PUB 199** Standards for Security Categorization of Federal Information and Information Systems (12/03)

---

*Continued on next page*

## Additional References, Continued

---

### NIST Special Publications

[<http://csrc.nist.gov/publications/nistpubs/index.html>]

#### *Drafts:*

[<http://csrc.nist.gov/publications/drafts.html>]

### *800 Series*

- **NIST Special Publication 800-2**, Public-Key Cryptography
- **NIST Special Publication 800-3**, Establishing a Computer Security Incident Response Capability (CSIRC)
- **NIST Special Publication 800-4**, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials
- **NIST Special Publication 800-4A**, Security Considerations in Federal Information Technology Procurements
- **NIST Special Publication 800-5**, A Guide to the Selection of Anti-Virus Tools and Techniques
- **NIST Special Publication 800-6**, Automated Tools for Testing Computer System Vulnerability)
- **NIST Special Publication 800-7**, Security in Open Systems
- **NIST Special Publication 800-8**, Security Issues in the Database Language SQL
- **NIST Special Publication 800-9**, Good Security Practices for Electronic Commerce, Including Electronic Data Interchange
- **NIST Special Publication 800-10**, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls
- **NIST Special Publication 800-11**, The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security
- **NIST Special Publication 800-12**, An Introduction to Computer Security: The NIST Handbook
- **NIST Special Publication 800-13**, Telecommunications Security Guidelines for Telecommunications Management Network
- **NIST Special Publication 800-14**, Generally Accepted Principles and Practices for Securing Information Technology Systems
- **NIST Special Publication 800-15**, Minimum Interoperability Specification for PKI components (MISPC), Version 1
- **NIST Special Publication 800-16**, Information Technology Security Training Requirements: A Role- and Performance-Base Model (supersedes NIST Spec Pub. 500-172)
- **NIST Special Publication 800-17**, Modes of Operation Validation System (MOVS): Requirements and Procedures
- **NIST Special Publication 800-18**, Guide for Developing Security Plans for Information Technology Systems
- **NIST Special Publication 800-19**, Mobile Agent Security

---

*Continued on next page*

## Additional References, Continued

---

### NIST Special Publications (continued)

- **NIST Special Publication 800-20**, Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
- **NIST Special Publication 800-21**, Guideline for Implementing Cryptography in the Federal Government
- **NIST Special Publication 800-22**, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- **NIST Special Publication 800-23**, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- **NIST Special Publication 800-24**, PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
- **NIST Special Publication 800-25**, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
- **NIST Special Publication 800-26**, Security Self Assessment Guide for Information Technology Systems
- **NIST Special Publication 800-27**, Engineering Principles for IT Security
- **NIST Special Publication 800-28**, Guidelines on Active Content and Mobile Code
- **NIST Special Publication 800-29**, A Comparison of the Security Requirements of Cryptographic Modules in FIPS 140-1 and 140-2
- **NIST Special Publication 800-30**, Risk Management Guide for Information Technology Systems
- **NIST Special Publication 800-31**, Intrusion Detection Systems (IDS)
- **NIST Special Publication 800-32**, Introduction to Public Key Technology and the Federal PKI Infrastructure
- **NIST Special Publication 800-33**, Underlying Technical Models for Information Technology Security
- **NIST Special Publication 800-34**, Contingency Planning Guide for Information Technology Systems
- **NIST Special Publication 800-35**, Guide to IT Security Services (Draft)
- **NIST Special Publication 800-36**, Guide to Selecting IT Security Products
- **NIST Special Publication 800-37**, Guide for the Security Certification and Accreditation of Federal Information Systems
- **NIST Special Publication 800-38A**, Recommendation for Block Cipher Modes of Operation - Methods and Techniques
- **NIST Special Publication, 800-38B**, Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode

---

*Continued on next page*

## Additional References, Continued

---

### NIST Special Publications (continued)

- **NIST Special Publication, 800-38C**, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
- **NIST Special Publication 800-40**, Procedures for Handling Security Patches
- **NIST Special Publication 800-41**, Guidelines on Firewalls and Firewall Policy
- **NIST Special Publication 800-42**, Guideline on Network Security Testing
- **NIST Special Publication 800-43**, System Administration Guidance for Windows 2000 Professional
- **NIST Special Publication 800-44**, Guidelines on Securing Public Web Servers
- **NIST Special Publication 800-45**, Guidelines on Electronic Mail Security
- **NIST Special Publication 800-46**, Security for Telecommuting and Broadband Communications
- **NIST Special Publication 800-47**, Security Guide for Interconnecting Information Technology Systems
- **NIST Special Publication 800-48**, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
- **NIST Special Publication 800-50**, Building an Information Technology Security Awareness and Training Program
- **NIST Special Publication 800-51**, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
- **NIST Special Publication 800-53**, Security Controls for Federal Information Systems
- **NIST Special Publication 800-53A**, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems
- **NIST Special Publication 800-55**, Security Metrics Guide for Information Technology Systems
- **NIST Special Publication 800-60**, Guide for Mapping Information and Information Types to Security Objectives and Risk Levels
- **NIST Special Publication 800-61**, Computer Security Incident Handling Guide
- **NIST Special Publication 800-63**, Recommendation for Electronic Authentication

---

*Continued on next page*

## Additional References, Continued

---

### USDA Policies & Regulations

[[http://www.ocio.net.usda.gov/ocio/cyber\\_sec/index.html](http://www.ocio.net.usda.gov/ocio/cyber_sec/index.html)]

- **DR 3140-001**, USDA Information System Security Policy
- **DR 3140-2**, USDA Internet Security Policy
- **DR 3300-1**, Telecommunications & Internet Services & Use
- **DR 3410-1**, Information Collection Activity
- **DR 3080-1**, Records Disposition
- **DM 3200-2**, Management: A Project Managers Guide to Applications Systems Life Cycle Management
- **DM 3500**, USDA Cyber Security Manual
- **CS-002**, Annual Information Cyber Security Plan Call
- **CS-003**, Internet Access Security for Private Internet Service Providers
- **CS-004**, Policy on Reuse of User Logon Identification
- **CS-005**, Guidance on Physical Security in USDA Information Technology
- **CS-006**, Guidance on USDA Privacy Requirements and the Use of Cookie on Web Pages
- **CS-007**, Guidance on Vulnerability Scan Procedures
- **CS-008**, Interim Guidance on the Use of Public Key Infrastructure (PKI) Technology in USDA
- **CS-009**, Guidance on Configuration Management, Part I – Policy and Responsibilities
- **CS-010**, Guidance on Peer-To-Peer (P2P) Software and Copyright Protection, 2nd Review
- **CS-011**, Cyber Security Guidance on USDA IBM & IBM Compatible Mainframe Security Standards
- **CS-012**, Cyber Security Guidance Regarding Gateway and Firewall Technical Security Standards
- **CS-013**, Cyber Security Guidance Regarding C2 Controlled Access Protection
- **CS-015**, Cyber Security Guidance on Computer Security Awareness Training Programs
- **CS-016**, Cyber Security Guidance Regarding Risk Assessments and Security Checklists
- **CS-017**, Required Language for Agency Warning Banners
- **CS-018**, Cyber Security Guidance Memorandums
- **CS-019**, Cyber Security Guidance Memorandum Regarding Privacy Impact Assessments

---

*Continued on next page*

## Additional References, Continued

---

### USDA Policies & Regulations (continued)

- **CS-020**, Cyber Security Memorandum and Guidance Regarding Submission of Waiver Requests
- **CS-021**, 2003 Annual Security Plans for Information Technology Systems
- **CS-022**, Cyber Security Guidance Regarding Encryption of Sensitive But Unclassified (SBU) Information
- **CS-023**, Cyber Security Guidance Regarding Sensitive But Unclassified (SBU) Information
- **CS-025**, Cyber Security Guidance Regarding Annual Security Plans for Information Technology (IT) Systems and Security Programs
- **CS-026**, Cyber Security Guidance Regarding Security Policy for Capital Planning and Investment Control (CPIC)
- **CS-027**, Computer Security Awareness and Training Program Plan and Vendor and Product Survey
- **CS-028**, Cyber Security Guidance Regarding Disaster Recovery and Business Resumption Plans
- **CS-029**, Cyber Security Guidance Regarding Telework & Remote Access
- **CS-030**, Certification and Accreditation of Information Systems  
*USDA Certification and Accreditation Guide*
- **CS-031**, Cyber Security Guidance Regarding Risk Assessment Methodology
- **CS-032**, Cyber Security Guidance Regarding Establishing a Trusted Facility Manual (TFMS)
- **CS-033**, Cyber Security Guidance Regarding Establishing a Security Feature Users Guide (SFUG)
- **CS-034**, Cyber Security Guidance Regarding Portable Electronic Devices (PED) and Wireless Technology
- **CS-035**, Cyber Security Guidance Regarding Developing A Security Architecture Framework
- **CS-036**, Cyber Security Guidance Regarding Security Controls in the System Development Life Cycle (SDLC)
- **CS-037**, Portable Computers and Laptops Security (Planned May 2004)
- **CS-038**, Cyber Security Guidance Regarding Background Investigations, Suitability Determinations and Clearances for IT Personnel (Planned May 2004)
- **CS-039**, Cyber Security Guidance Regarding the Physical Security Checklist for IT Restricted Space (Planned May 2004)
- **CS-041**, Cyber Security Guidance Regarding Patch Management and System Updates (Planned May 2004)

---

*Continued on next page*

## Additional References, Continued

---

### Miscellaneous

- **DOD Directive 8500.1** Information Assurance (10/02)  
[<http://www.dtic.mil/whs/directives/>]
  - **GAO Federal Information System Control Audit Manual** (Exposure Draft) (FISCAM) (08/97) [[http://www.gao.gov/policy/12\\_19\\_6.pdf](http://www.gao.gov/policy/12_19_6.pdf)]
  - **Common Criteria** for Information Technology Security Evaluation (Ver. 2.1) (08/99) [<http://csrc.nist.gov/cc/ccv20/ccv2list.htm>]
  - **Federal CIO Council**, Securing Electronic Government (01/01)  
[<http://www.cio.gov>]
-

This page intentionally left blank.

**APPENDIX A**  
**Certification and Accreditation**

This page intentionally left blank.

# Certification and Accreditation

## Overview

---

### Introduction

Certification and accreditation (C&A) is the process whereby an information system is authorized to operate (i.e., process, store, or transmit information) at an acceptable level of risk [*accreditation*] based on an assessment of its management, operational, and technical controls [*certification*].

Performing system C&As is both a federal and USDA requirement.

---

### Federal C&A Requirements

The Federal Information Security Management Act (FISMA) of 2002, along with the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996, explicitly emphasize a risk-based policy for cost effective security.

In addition, OMB Circular A-130, Appendix III requires executive agencies within the federal government to

- plan for security
  - ensure that appropriate officials are assigned security responsibilities
  - periodically review the security controls in their information systems, and
  - **authorize system processing** prior to operations and, periodically, thereafter.
- 

### USDA C&A Requirements

In order to comply with federal requirements, CS-030, *Certification and Accreditation of Information Systems*, requires all USDA agencies and staff offices to formally certify and accredit all Major Applications (MAs) and General Support Systems (GSSs) by July 2004.

CS-031 and its companion, the *USDA Certification and Accreditation Guide*, provide policy and guidance regarding roles and responsibilities and the steps involved in the C&A process, and apply to all information technology (IT) systems or applications owned, leased, operated, or connected to the Department of Agriculture.

---

### In This Appendix

C&A, as outlined in the *USDA Certification and Accreditation Guide*, is a three-phase, multi-step process. This Appendix provides a general overview of that process, along with information regarding roles and responsibilities.

---

*Continued on next page*

## Overview, Continued

---

### Contents

This Appendix contains the following topics:

<b>Topic</b>	<b>See Page</b>
Roles and Responsibilities	A-3
The Certification and Accreditation Process	A-7

---

### References

The following documents were used in the development of this Appendix:

- CS-030, Certification and Accreditation of Information Systems
  - USDA Certification and Accreditation Guide
  - NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
-

# Roles and Responsibilities

---

## Introduction

Personnel in the following roles are involved in the USDA certification and accreditation (C&A) process:

- Designated Accrediting Authority (DAA)
- Certifying Official (CO)
- Certification Team
- Security Test and Evaluation Team
- Program Manager and System Owner
- Information System Security Officer

Descriptions of these roles and their respective responsibilities are provided below.

---

## Designated Accrediting Authority (DAA)

The Designated Accrediting Authority (DAA) is a USDA program area executive with the authority to evaluate the mission, business case, and budgetary needs for the system in view of the security risks present in the system's operating environment.

The DAA

- is the business owner of the general support system or major application being certified
  - has the authority to
    - formally approve the operation of an IT system at an acceptable level of risk within its environment
    - issue an Interim Authority to Operate (IATO) for an IT system based on the level of risk involved in system operation
    - deny approval for systems to operate
    - halt operations if unacceptable security risks are found to exist
  - assumes responsibility for the residual risks of operation of the system in a stated environment, and
  - approves security requirements documents, memoranda of agreement (MOA), memoranda of understanding (MOU), and any deviations from security policies.
- 

*Continued on next page*

## Roles and Responsibilities, Continued

---

### **Certifying Official (CO)**

The Certifying Official (CO) for the Department is the USDA Chief Information Officer (CIO).

Each agency CIO serves as the CO for his/her particular agency, and acts as the point of contact with regard to certification activities.

The mission of each agency CO is to

- evaluate the certification package from a technical perspective
  - evaluate the risk to the system
  - present a recommendation to the DAA with regard to the accreditation of the system as part of the accreditation package.
- 

### **Certification Team**

The certification team consists of the technical personnel from the business unit responsible for conducting the certification activities.

The certification team is responsible for

- identifying, assessing, and documenting the risks associated with operating the system, including:
    - assessing the vulnerabilities in the system
    - determining if the security controls are correctly implemented and effective
    - identifying the level of residual risk of the system
  - coordinating C&A activities, and
  - consolidating the final C&A package.
- 

### **Security Test & Evaluation Team**

The security test and evaluation (ST&E) team consists of personnel independent of the IT infrastructure and business function. The ST&E team must be approved by the CO prior to the commencement of the C&A process.

The ST&E team is responsible for

- performing the ST&E on the system
  - validating the results of the risk assessment, and
  - validating that the controls in the System Security Plan (SSP) are present and operating correctly.
- 

*Continued on next page*

## Roles and Responsibilities, Continued

---

### **Program Manager and System Owner**

The program manager and system owner represent the interests of the user community and the IT system throughout the system's life cycle.

The program manager is responsible for the system during initial development and acquisition, and the system owner assumes responsibility for the system after delivery and installation.

Both the program manager and system owner are responsible for

- ensuring the system is deployed and operated according to the security controls documented in the security plan
  - seeing that system users and security support personnel receive the requisite security training
  - coordinating the C&A effort
  - providing the necessary staff and information to the certification team, and
  - reviewing the certification package before it is presented to the CO.
- 

### **Information Systems Security Officer (ISSO)**

For operational systems, the Information Systems Security Officer (ISSO) is responsible for the day-to-day security of a specific IT system, including

- physical security
- personnel security
- incident handling, and
- security awareness, training, and education.

The ISSO, in conjunction with the Configuration Control Board (CCB), also

- identifies pending system or environment changes that may necessitate system re-certification and re-accreditation, and
  - serves as the principal technical advisor to the program manager on all security-related issues for developmental systems.
- 

*Continued on next page*

## Roles and Responsibilities, Continued

### Other Supporting Roles

Other individuals within USDA may play a role or have concerns or interests in the C&A process. The table below presents some of these roles and their potential interest or function in C&A.

Role	Interest/ Function
User Representatives	<ul style="list-style-type: none"> <li>• Assist in ensuring mission requirements are satisfied while meeting the security controls defined in the security plan</li> </ul>
Security Program Managers	<ul style="list-style-type: none"> <li>• Ensure a standard C&amp;A process is used throughout the agency</li> <li>• Provide internal C&amp;A guidance or policy</li> <li>• Review certification packages prior to DAA review, if appropriate</li> </ul>
Operations Managers	<ul style="list-style-type: none"> <li>• Oversee the security operations and administration of IT systems</li> </ul>
Facilities Managers	<ul style="list-style-type: none"> <li>• Oversee changes and additions to facilities housing IT systems</li> <li>• Ensure that changes in facility design or construction do not adversely affect the security of existing systems</li> </ul>

# The Certification and Accreditation Process

## Introduction

The C&A process is comprised of the following three phases:

1. Pre-Certification Phase
2. Certification and Accreditation Phase
3. Post-Accreditation Phase

This section describes the overall C&A process in terms of these phases, and summarizes the steps and activities involved in each.

## C&A Process Overview

The figure below provides an overview of the various phases and steps involved in the C&A process.

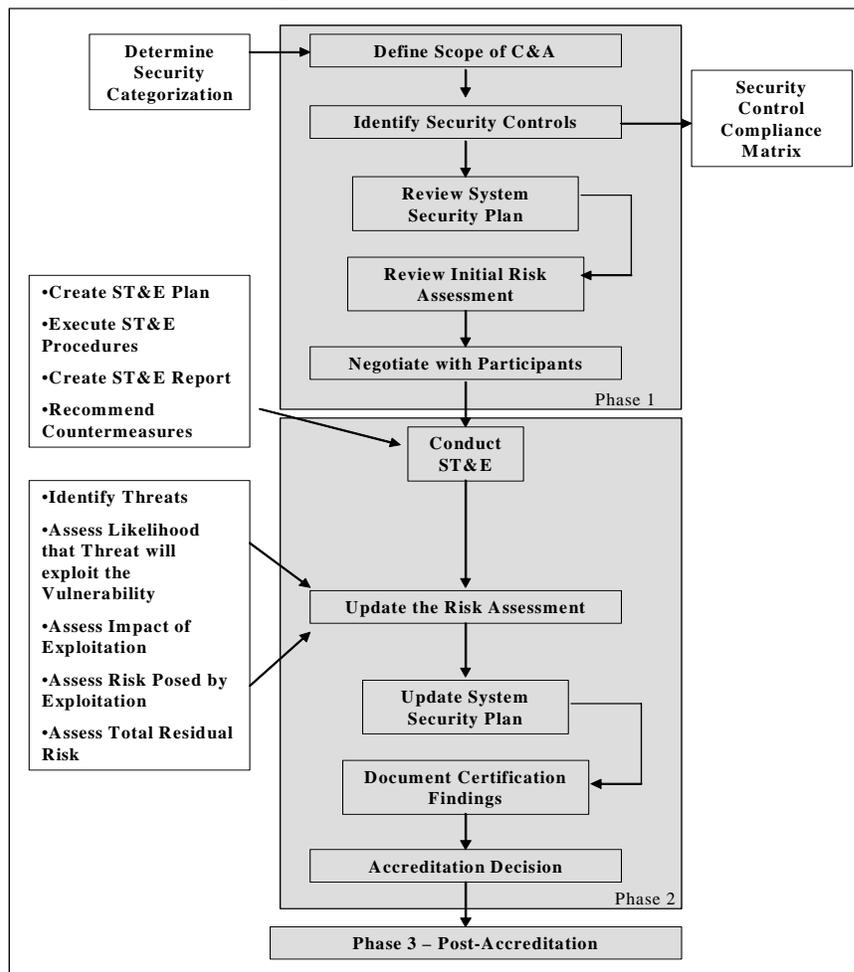


Figure 1 – The C&A Process

A discussion of the individual steps depicted for each phase follows.

*Continued on next page*

## The Certification and Accreditation Process, Continued

---

### Phase 1: Pre-Certification

Phase 1 involves five steps as described in the table below.

Step	Action
1	Define the system and scope of the C&A effort <ul style="list-style-type: none"><li>• Gather all available system information, including<ul style="list-style-type: none"><li>▪ Design documents</li><li>▪ System descriptions</li><li>▪ System Security Plans (SSPs)</li></ul></li><li>• Catalog system software, hardware, and communications equipment</li><li>• Determine security categorization for the system/application</li></ul>
2	Identify security controls and construct a security controls compliance matrix (SCCM) <ul style="list-style-type: none"><li>• List each control, its reference, and whether or not it has been implemented</li></ul>
3	Review the System Security Plan
4	Review the initial risk assessment
5	Negotiate with participants <ul style="list-style-type: none"><li>• Verify security categorization for system</li><li>• Review SCCM and ensure applicable security requirements are accurately reflected</li></ul>

---

### Key Participants in Phase 1

Key participants in Phase 1 include:

- DAA
  - CO
  - Program Manager
  - System Owner
  - Certification Team
  - ISSO
  - Other officials with an interest in the system
- 

*Continued on next page*

## The Certification and Accreditation Process, Continued

### Phase 2: Certification & Accreditation

In Phase 2, the certification team evaluates the effectiveness of the security controls on the system, and uses the results to update the risk assessment and SSP and to document the certification findings.

The table below presents the steps involved in this phase.

Step	Action
6	Conduct a Security Test & Evaluation (ST&E) <ul style="list-style-type: none"> <li>• Create an ST&amp;E Plan</li> <li>• Execute the test procedures</li> <li>• Document the results in an ST&amp;E Report</li> </ul>
7	Update the Risk Assessment <ul style="list-style-type: none"> <li>• Identify threats</li> <li>• Assess likelihood a vulnerability will be exploited</li> <li>• Assess impact of exploitation</li> <li>• Assess risk posed by vulnerability</li> <li>• Assess total risk to the system</li> <li>• Include updates as addendum to original Risk Assessment</li> <li>• Include risk determination in certification package</li> </ul>
8	Update the System Security Plan
9	Document certification findings <ul style="list-style-type: none"> <li>• Summarize findings in Security Evaluation Report (SER)</li> <li>• Compile certification package, to include:               <ul style="list-style-type: none"> <li>▪ SCCM</li> <li>▪ ST&amp;E Report</li> <li>▪ Risk Assessment</li> <li>▪ SSP</li> <li>▪ SER</li> </ul> </li> <li>• Forward certification package to CO</li> <li>• Forward CO Certification Statement and accreditation decision recommendation to DAA</li> </ul>
10	Accreditation decision <ul style="list-style-type: none"> <li>• DAA               <ul style="list-style-type: none"> <li>▪ Issues full accreditation, or</li> <li>▪ Denies accreditation</li> </ul> </li> <li>• Decision is documented in final accreditation package consisting of:               <ul style="list-style-type: none"> <li>▪ Accreditation Letter</li> <li>▪ Supporting documentation</li> </ul> </li> </ul>

*Continued on next page*

## The Certification and Accreditation Process, Continued

---

**Phase 3: Post-Accreditation Phase**

Phase 3 consists of managing the configuration of the system and re-accrediting it every three years.

The table below describes these activities.

<b>Activity</b>	<b>Description</b>
Configuration Management	<ul style="list-style-type: none"><li>• Monitor system modifications to ensure security posture is not threatened by changes to software or hardware</li><li>• Ensure any system changes are approved by the Configuration Control Board (CCB)</li><li>• Document implemented security changes in the SSP</li><li>• Determine if changes necessitate re-accreditation</li></ul>
Re-accreditation	<ul style="list-style-type: none"><li>• Re-accredit systems every three years or when significant system changes occur</li><li>• Ensure C&amp;A process for re-accreditation is begun in a timely fashion prior to three-year accreditation anniversary</li></ul>

---

## **APPENDIX B**

### **Categorizing Information & Information Systems**

This page intentionally left blank.

# Categorizing Information & Information Systems

## Overview

---

### Introduction

Categorizing information and information systems refers to the process of

- identifying those systems that support the operations and assets of the agency,
  - identifying the types of information that are processed, stored, or transmitted by those systems, and
  - determining the degree of protection required for each system based on the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification or destruction of the system and/or its information.
- 

### FIPS PUB 199

In accordance with FISMA, senior agency officials must determine the levels of information security appropriate to protect information and information systems under their control in accordance with standards promulgated by the National Institute of Standards and Technology (NIST). NIST has issued Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to assist agencies in categorizing information and information systems based on the objectives of providing appropriate levels of information security to a range of risk levels.

---

### In This Appendix

This Appendix provides an overview of the steps involved in categorizing information and information systems in accordance with FISMA and FIPS PUB 199.

---

### Contents

This Appendix contains the following topics:

Topic	See Page
Identifying Information Systems & Types of Information	B-3
Levels of Risk	B-5
Security Objectives	B-6
Security Categorization	B-7

---

*Continued on next page*

## Overview, Continued

---

### References

The following documents were used in the development of this Appendix:

- Federal Information Security Management Act (FISMA), P.L. 107-347, Title III, December 2002
  - NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
  - FIPS PUB 199, Security Categorization of Federal Information and Information Systems, 12/03
-

# Identifying Information Systems & Types of Information

---

## Introduction

Before an agency or organization can determine how much protection its information and information systems require, it must first identify

- the systems upon which it depends to accomplish its mission, and
  - the types of information that are processed, stored, and transmitted by each of those systems.
- 

## Identifying Information Systems

In accordance with NIST Special Publication (SP) 800-18, a “system” is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system. Each element of the system must

- be under the same direct management control
- have the same function or mission objective
- have essentially the same operating characteristics and security needs, and
- reside in the same general operating environment.

*Note:* All components of a system need not be physically connected (e.g., a group of PC’s placed in employees homes under defined telecommunication program rules, or a system with multiple identical configurations installed in locations with the same physical and environmental safeguards).

---

## Categorizing Systems as Major Applications or General Support Systems

Once all information systems that support the agency’s or organization’s operations and assets have been identified, each may be categorized as either a

- Major Application (MA), or
- General Support System (GSS).

These categorizations assist in the development of an appropriate System Security Plan based on the outlines provided in NIST SP 800-18. They do not reflect the *security* categorization of the system based on risk levels and security objectives.

---

*Continued on next page*

# Identifying Information Systems & Types of Information,

Continued

---

**Definition:  
Major  
Application**

A *Major Application (MA)* is a system that performs clearly defined functions for which there are readily identifiable security considerations and needs. A major application may be comprised of many individual programs and hardware, software, and telecommunications components, and may also consist of multiple individual applications if all are related to a single mission function.

**Examples:**

- Electronic funds transfer system
  - Payroll system
  - Personnel system
- 

**Definition:  
General  
Support System**

A *General Support System (GSS)* is comprised of interconnected information resources under the same direct management control which share common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications.

**Examples:**

- LANs
  - Communications networks
  - Backbones (agency-wide)
  - Shared information processing service organizations
- 

**Identifying  
Types of  
Information**

Once the agency's/organization's information systems have been distinguished, the types of information that each of those systems process, store, and/or transmit must be identified. Types of information may include:

- Privacy information
  - Medical information
  - Proprietary information
  - Financial information
  - Contractor sensitive information
-

# Levels of Risk

---

**What are the Levels of Risk?**

To safeguard information and systems cost-effectively, the degree of protection required must be established so that an appropriate level of security may be applied. In order to determine protection requirements, the level of risk to a system for each of the stated security objectives (confidentiality, integrity, and availability) must be determined. FIPS PUB 199 establishes the following three potential levels of risk:

- Low
- Moderate
- High

The levels of risk consider both impact and threat, but are more heavily weighted toward impact. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency/organization operations (including mission, functions, image or reputation), assets, or individuals (including privacy).

---

**Low Risk Level**

The level of risk is *low* if an event could be expected to have a *limited adverse effect* on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

---

**Moderate Risk Level**

The level of risk is *moderate* if an event could be expected to have a *serious adverse effect* on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.

---

**High Risk Level**

The level of risk is *high* if an event could be expected to have a *severe or catastrophic effect* on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

---

# Security Objectives

---

**Introduction** Security objectives are goals that must be achieved in order to appropriately protect a system and its information. The primary security objectives are:

- Confidentiality
- Integrity
- Availability

---

**Confidentiality** *Confidentiality* is a means of preserving authorized restrictions on information access and disclosure, including protecting personal privacy and proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

---

**Integrity** *Integrity* means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

A loss of integrity is the unauthorized modification or destruction of information.

---

**Availability** *Availability* means ensuring the timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or an information system.

---

# Security Categorization

---

**Introduction** Information and information systems can be categorized with respect to security based on the assignment of appropriate levels of risk (low, moderate, or high) to the security objectives of confidentiality, integrity, and availability.

---

**Categorization Formula** The standardized format for documenting the security category of a system is:

$$\text{Categorization} = [(\text{confidentiality}, \text{RISK-LEVEL}), (\text{integrity}, \text{RISK-LEVEL}), (\text{availability}, \text{RISK-LEVEL})]$$

The security categorization of an information system that processes, stores, or transmits multiple types of information shall be *at least* the *highest risk level* that has been determined for each type of information for each security objective of confidentiality, integrity, and availability – taking into account dependencies among these objectives.

**Example:**

The level of risk for confidentiality for systems that process information that requires no confidentiality protection (i.e., information that has a level of risk for confidentiality of zero) is NOT zero. In order to achieve integrity and availability, some information must be protected against disclosure (such as passwords, cryptographic keys, and any other information that would facilitate a successful attack).

---

**Categorization Summary Table** The following table (as extracted from FIPS PUB 199) summarizes the three levels of risk and associated descriptions for each security objective.

SECURITY OBJECTIVE	LEVEL OF RISK		
	LOW	MODERATE	HIGH
<b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	<ul style="list-style-type: none"> <li>Unauthorized disclosure of data could have a limited adverse effect on operations, assets, or individuals</li> <li>Loss of confidentiality could cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized disclosure of data could have a serious adverse effect on operations, assets, or individuals</li> <li>Loss of confidentiality could cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized disclosure of data could have a severe or catastrophic adverse effect on operations, assets, or individuals</li> <li>Loss of confidentiality could cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.</li> </ul>

*Continued on next page*

## Security Categorization, Continued

**Categorization Summary Table** (continued)

SECURITY OBJECTIVE	LEVEL OF RISK		
	LOW	MODERATE	HIGH
<p><b>Integrity</b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	<ul style="list-style-type: none"> <li>Unauthorized modification or destruction of information could have a limited adverse effect on operations, assets, or individuals.</li> <li>A loss of integrity could cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized modification or destruction of information could have a serious adverse effect on operations, assets, or individuals.</li> <li>A loss of integrity could cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized modification or destruction of information could have a severe or catastrophic adverse effect on operations, assets, or individuals.</li> <li>A loss of integrity could cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.</li> </ul>
<p><b>Availability</b> Ensuring the timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<ul style="list-style-type: none"> <li>Disruption of access to or use of information or an information system could have a limited adverse effect on operations, assets, or individuals.</li> <li>A loss of availability could cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.</li> </ul>	<ul style="list-style-type: none"> <li>Disruption of access to or use of information or an information system could have a serious adverse effect on operations, assets, or individuals.</li> <li>A loss of availability could cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.</li> </ul>	<ul style="list-style-type: none"> <li>Disruption of access to or use of information or an information system could have a severe or catastrophic adverse effect on operations, assets, or individuals.</li> <li>A loss of availability could cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.</li> </ul>

**APPENDIX C**  
**Risk Management**

This page intentionally left blank.

# Risk Management

## Overview

---

**Introduction** Risk management is the process of identifying, controlling, and mitigating information system related risks. The risk management process is ongoing and is used to determine adequate security for a system by analyzing threats and vulnerabilities and selecting cost-effective controls to achieve and maintain an acceptable level of risk. It includes risk assessment, cost-benefit analysis, and the selection, implementation, test, and security evaluation of safeguards.

---

**Purpose** The objective of performing risk management is to enable the agency/organization to accomplish its mission/s by

- better securing the information technology (IT) systems that store, process, or transmit information
- enabling management to make well-informed risk management decisions to justify expenditures, and
- assisting management in authorizing (or accrediting) IT systems based on supporting documentation from the performance of risk management.

---

**Risk Management Processes** Risk management encompasses three primary processes:

- Risk assessment
- Risk mitigation
- Risk evaluation and assessment

---

**In This Appendix** This Appendix provides an overview of risk management and the processes on which it is based, and describes how it fits into the system development life cycle.

---

*Continued on next page*

## Overview, Continued

---

### Contents

This section contains the following topics:

<b>Topic</b>	<b>See Page</b>
Risk Management & the System Development Life Cycle	C-3
Risk Assessment	C-6
Risk Mitigation	C-9
Risk Evaluation & Assessment	C-12

---

### References

The following documents were used in the development of this Appendix:

- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
  - NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems
  - DM 3500, Cyber Security Manual, Chapter 8, USDA Risk Management Program
  - DM 3500, Cyber Security Manual, Chapter 13, Cyber Security Plans
-

# Risk Management & the System Development Life Cycle

---

## Introduction

Effective risk management must be integrated into the entire system development life cycle (SDLC). Risk management is an iterative process that should be performed during each of the phases of a system's life cycle. This section summarizes the risk management activities associated with each phase of the SDLC.

---

## Five Phases of the SDLC

The life cycle of an information technology (IT) system has five phases:

- Initiation
- Development or acquisition
- Implementation
- Operation or maintenance
- Disposal

In some cases, a system may occupy several of these phases at the same time.

---

## Risk Management Activities During the Initiation Phase

The Initiation Phase is the starting point of any system and is where the need for an IT system is expressed and the purpose and scope of the system is documented. The primary focus of this phase of the life cycle is to gather information in preparation for the following stages.

Risk management activities performed during the Initiation Phase include

- completing a data sensitivity needs assessment
- developing a System Security Plan
- defining a Concept of Operation
- developing business and security requirements from federal laws, NIST guidelines, and USDA policy
- conducting a high-level threat analysis, and
- conducting a high-level mission impact analysis.

**Note:** The size and complexity of the system being initiated will determine to what extent and detail the above activities are conducted.

---

*Continued on next page*

# Risk Management & the System Development Life Cycle,

Continued

---

## **Risk Management Activities During the Development/Acquisition Phase**

It is during the Development/Acquisition Phase that the system is designed, purchased, programmed, developed, or otherwise constructed. Information gathered during the Initiation Phase is used in this phase to continue developing system and security requirements and to set system parameters and conditions.

Risk management activities performed during the Development/Acquisition Phase include

- defining the security architecture
- continuing development of security requirements
- updating the System Security Plan
- developing contingency and organizational security plans
- conducting a detailed threat analysis
- conducting a detailed impact analysis
- developing a high-level risk strategy & implementing countermeasures
- beginning system certification activities
- developing the Security Requirements document, and
- conducting a high-level risk assessment.

---

## **Risk Management Activities During the Implementation Phase**

In the Implementation Phase, the system security features are configured, enabled, tested and verified, and the system begins to perform its intended business function. The Implementation Phase includes all activities that occur prior to the system being placed into Production status.

Risk management activities performed during the Implementation Phase include

- implementing the security architecture
- assessing Management, Operational, & Technical controls
- conducting manual assessments, automated assessments, penetration tests, & system tests and evaluations
- conducting threat analysis
- conducting criticality analysis
- determining risk mitigations & implementing countermeasures
- completing the Certification package, and
- developing the Accreditation Statement.

---

*Continued on next page*

# Risk Management & the System Development Life Cycle, Continued

---

## **Risk Management Activities During the Operational/Maintenance Phase**

A system moves into production and continues to perform its stated mission during the Operational/Maintenance phase. Typically, the system is modified on an ongoing basis in this phase through the addition of hardware and software and by changes to organizational processes, policies, and procedures.

Risk management activities performed during the Operational/Maintenance Phase include

- monitoring security requirements
  - implementing a configuration management plan
  - continuing manual assessments & automated assessments
  - conducting penetration tests & system tests and evaluations after system changes
  - monitoring threat & impact to USDA mission, and
  - determining risk mitigations & implementing countermeasures, if required.
- 

## **Risk Management Activities During the Disposal Phase**

Normally, activities in the Disposal Phase consist of monitoring the state of the system. The only risk-related activity in this phase is to ensure that data is disposed of in a manner consistent with USDA policy. If the system's data is no longer required, then it can simply be destroyed by an approved means. Usually, the system will be upgraded or some part of the data will migrate to another system. In either case, it is important that adequate security controls have been implemented.

---

# Risk Assessment

---

**Introduction** Risk assessment is the first process in the USDA’s risk management methodology. Risk assessments are used to determine the extent of potential threats and the risks associated with an IT system throughout its system development life cycle (SDLC). The results of this process help to identify appropriate controls for reducing or eliminating risk, and also provide USDA management with the capability to make informed decisions when allocating IT program resources needed to fulfill business requirements.

---

**What is Risk?** *Risk* is a function of the *likelihood* of a given *threat-source* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the agency/organization.

---

**Threats & Vulnerabilities** A *threat* is the potential for a particular threat-source to successfully exercise a particular vulnerability. A *vulnerability* is a weakness that can be accidentally triggered or intentionally exploited.

In determining the likelihood (i.e., probability) that a potential vulnerability will be exploited by a threat, one must consider the motivation and capability of the threat-source, the nature of potential vulnerabilities, and the existence and effectiveness of existing controls.

---

**Threat-Sources** A *threat-source* is any circumstance or event with the potential to cause harm to an IT system. Threat sources can be:

- **Natural** – floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, etc.
  - **Human** – events that are either enabled by or caused by human beings, such as unintentional acts (e.g., inadvertent data entry) or deliberate actions (e.g., network based attacks and malicious software upload), and
  - **Environmental** – long-term power failure, pollution, chemicals, liquid leakage, etc.
- 

*Continued on next page*

## Risk Assessment, Continued

### Impact

Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and, in turn, produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).

### Risk Assessment Activities

The USDA risk assessment methodology consists of the following seven steps:

Step	Actions
Step 1: System Characterization	<ul style="list-style-type: none"> <li>• Identify system mission</li> <li>• Review system architecture &amp; determine system boundaries, interfaces &amp; data flow</li> <li>• Determine data categories and sensitivity</li> <li>• Consider system life cycle phase</li> <li>• Understand system users</li> <li>• Review system security policies</li> </ul>
Step 2: Conduct Vulnerability & Control Analysis	<ul style="list-style-type: none"> <li>• Conduct manual assessments</li> <li>• Conduct automated scans, penetration tests, and ST&amp;Es</li> <li>• Review previous security plans &amp; risk assessments</li> </ul>
Step 3: Conduct Threat Analysis	<ul style="list-style-type: none"> <li>• Determine threat types</li> <li>• Develop listing of threat-sources</li> <li>• Determine probability of threat occurrence</li> </ul>
Step 4: Conduct Impact Analysis	<ul style="list-style-type: none"> <li>• Consider data categories</li> <li>• Determine mission impact severity in terms of confidentiality, integrity, &amp; availability</li> </ul>
Step 5: Determine Risk Level	<ul style="list-style-type: none"> <li>• Determine threat probability of occurrence</li> <li>• Determine impact criticality</li> </ul>
Step 6: Develop a Risk Mitigation Strategy	<ul style="list-style-type: none"> <li>• Review threat list</li> <li>• Determine impact</li> <li>• Implement countermeasures</li> <li>• Develop a threat mitigation list based on available resources</li> </ul>
Step 7: Report the Residual Risk	<ul style="list-style-type: none"> <li>• Document remaining risk/s and a plan for future action</li> <li>• Include residual risk in Certification and Accreditation package</li> </ul>

*Continued on next page*

## Risk Assessment, Continued

---

**For Further  
Information**

More detailed information on how to perform each of the above steps in the USDA risk assessment process is provided in DM-3500, Cyber Security Manual, Chapter 8.

---

# Risk Mitigation

---

## What is Risk Mitigation?

**Risk mitigation** is the process of prioritizing, implementing and maintaining appropriate risk-reducing measures recommended as a result of a risk assessment.

---

## Risk Mitigation Activities

The information contained in the risk assessment leads to the following risk mitigation activities:

1. Prioritize actions
  2. Evaluate recommended control options
  3. Conduct cost-benefits analysis
  4. Select controls
  5. Assign responsibility
  6. Develop safeguard implementation plan
  7. Implement selected controls
- 

## Implementing Counter-measures

**Countermeasures** are actions that an organization can take to lessen or eliminate the threats or impacts of vulnerabilities identified in an IT system.

Typically, countermeasures are thought of in terms of security controls. When implementing recommended controls to mitigate risk, Technical, Management, and Operational controls (or a combination of such controls) should be considered in order to maximize their effectiveness. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an agency's/organization's mission.

---

## Security Control Categories

Security controls generally fall into one of the following three categories:

- Management Controls
  - Operations controls, and
  - Technical controls.
- 

*Continued on next page*

## Risk Mitigation, Continued

---

### **Management Controls**

Management controls focus on the management of the security system and the management of risk for a system. Management controls include:

- Risk assessment and management
  - Review of security controls
  - Rules of behavior
  - Planning for security in the system development life cycle
  - Authorize processing
- 

### **Operational Controls**

Operational controls focus on security methods and mechanisms that are primarily implemented and executed by people, as opposed to systems. Operational controls include:

- Personnel security
  - Physical and environmental protection
  - Production input/output controls
  - Contingency planning
  - Application software maintenance controls
  - Data integrity/validation controls
  - Documentation
  - Incident response capability
  - Security awareness and training
- 

### **Technical Controls**

Technical controls focus on security controls that the computer system executes. They consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls include:

- Identification & Authentication
  - Logical access controls
  - Public access controls
  - Audit trails
- 

*Continued on next page*

## Risk Mitigation, Continued

---

**Residual Risk** The risk remaining after the implementation of new or enhanced controls is the *residual risk*. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

Threats that are not immediately mitigated following a cost-benefit analysis, (thus representing residual risk to a system) are presented to the system's Designated Accrediting Authority (DAA) as part of the system's certification and accreditation package. It is then left to the DAA as to whether or not to allow the system to continue to operate while the risks are mitigated, accept the residual risk, or shut the system down.

---

# Risk Evaluation and Assessment

---

## **Introduction**

Over time, changes to IT systems and security policies, procedures, and practices will result in new risks surfacing and previously mitigated risks once again becoming a concern. Hence, the risk management process must continue and evolve.

---

## **Risk Assessment Requirements & Good Practices**

OMB Circular A-130 mandates that the risk assessment process be repeated at least every three years or whenever a significant system change occurs.

Regardless of federal requirements, risk management should be conducted and integrated into the system development life cycle as part of good security practices. A specific schedule for assessing and mitigating mission risks should be established, but remain flexible enough to allow changes where warranted (such as when a major change to a system occurs due to the emergence of new technologies).

---

## **Factors in Successful Risk Management**

In the end, a successful risk management program relies on

- senior management commitment
  - full support and participation of the IT team
  - competence of the risk assessment team
  - awareness and cooperation of members of the user community, and
  - ongoing evaluation and assessment of IT-related mission risks.
-

**APPENDIX D**  
**System Security Plans**

This page intentionally left blank.

# System Security Plans

## Overview

---

**Introduction** The completion of System Security Plans is a requirement of OMB Circular A-130, the Computer Security Act, and FISMA, as well USDA policy. Individual Security plans are required for all Major Applications (MAs) and General Support Systems (GSSs).

---

**What is a System Security Plan?** A *System Security Plan* (SSP) is a formal document that provides an overview of the security requirements of the information system and describes the security controls in place or planned for meeting those requirements.

---

**Purpose** The purpose of a System Security Plan is to

- provide an overview of the security requirements of the system
- describe the controls in place for meeting those requirements, and
- delineate responsibilities and expected behavior of all individuals who access the system.

---

**Main Parts of a Security Plan** There are two basic parts to a System Security Plan:

- System Identification
- System Security Controls

Each of these parts contains detailed information about the system and the controls that have been implemented to protect it.

---

**In This Appendix** This Appendix provides a general overview of the parts of a System Security Plan and the information that should be included in them.

---

*Continued on next page*

## Overview, Continued

---

### Contents

This Appendix contains the following topics:

<b>Topic</b>	<b>See Page</b>
System Types	D-3
System Identification	D-5
System Security Controls	D-6

---

### References

The following documents were used in the development of this Appendix:

- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
  - DM 3500, Cyber Security Manual, Chapter 13, Cyber Security Plans
-

# System Types

---

## Introduction

A System Security Plan (SSP) contains technical information about a system, its security requirements, and the controls implemented to provide protection against the system's risks and vulnerabilities. Before the plan can be developed, a determination must be made as to what type of plan is required based on the category of the system.

---

## System Categories

In accordance with NIST Special Publication 800-18, a system should be categorized as either a

- Major Application, or
- General Support System.

A security plan is required for all applications that fall under either category, and where a major application is supported by a general support system coordination of both plans is required.

---

## Definition: Major Application

A **Major Application (MA)** is a system that performs clearly defined functions for which there are readily identifiable security considerations and needs. A major application may be comprised of many individual programs and hardware, software and telecommunications components, and may also consist of multiple individual applications if all are related to a single mission function.

### *Examples:*

- Electronic funds transfer system
  - Payroll system
  - Personnel system
- 

*Continued on next page*

## System Types, Continued

---

**Definition:**  
**General Support System**

A *General Support System (GSS)* is comprised of interconnected information resources under the same direct management control which share common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications.

*Examples:*

- LANs
- Communications networks
- Backbones (agency-wide)
- Shared information processing service organizations

*Note:* A major application can run on a general support system. In such a case, the general support System Security Plan should reference the major application security plan.

---

**Security Plan Templates**

To facilitate the development of security plans for both system categories, the USDA has developed templates for a Major Application Security Plan and for a General Support System Security Plan based on NIST SP 800-18 and FISMA requirements. These templates may be found in DM 3500, USDA Cyber Security Manual, Chapter 13.

---

# System Identification

---

**Introduction** Once a system has been categorized as either a Major Application or a General Support System, the next step in the security plan development process is to provide basic identifying information about the system. This is accomplished in the first section of the plan titled *System Identification*.

---

**Purpose of System Identification Section** The content of the *System Identification* section of a security plan is the same for both MAs and GSSs. The purpose of this section is to provide general information about the system including

- who is responsible for the system
- the purpose of the system, and
- the sensitivity level of the system.

---

**System Identification Section Content** For both MA and GSS security plans, the *System Identification* section should cover the following topics:

- System Name/Title
- Responsible Organization
- Information Contact(s)
- Assignment of Security Responsibility
- System Operational Status
- General Description/Purpose
- System Environment
- System Interconnection/Information Sharing
- Sensitivity of Information Handled
  - Applicable Laws or Regulations Affecting the System
  - General Description of Information Sensitivity, and
- Configuration Management Information.

---

**Guidance on Completing System Identification Section** For guidance on how to complete the *System Identification* section of a System Security Plan, refer to the Security Plan Guidance presented in Attachment A of Chapter 13 of the USDA Cyber Security Manual (DM 3500), and NIST SP 800-18.

---

# System Security Controls

---

**Introduction** The second part of a System Security Plan describes the security controls in place for the MA or GSS. Controls are addressed within the following three major control categories:

- Management
  - Operational
  - Technical
- 

**Management Controls Section** The *Management Controls* section of a security plan describes the management control measures in place or planned that are intended to meet the protection requirements of the MS or GSS.

*Management controls* focus on the management of the computer security system and the management of risk for a system.

---

**Management Controls Section Content** The topics to be addressed in the *Management Controls* section of an MS plan or a GSS plan are the same, and include:

- Risk Assessment and Management
    - Performance Measures
  - Review of Security Controls
  - Rules of Behavior
  - Planning for Security in the Life Cycle
    - Initiation Phase
    - Development/Acquisition Phase
    - Implementation Phase
    - Operation/Maintenance Phase
    - Disposal Phase
  - Authorize Processing
    - Certification and Accreditation
    - Privacy
- 

*Continued on next page*

## System Security Controls, Continued

---

### Operational Controls Section

The *Operational Controls* section describes the operational control measures in place or planned that are intended to meet the protection requirements of the MS or GSS.

*Operational controls* focus on mechanisms that are primarily implemented and executed by people, as opposed to systems.

---

### Operational Controls Section Content

The content of the *Operational Controls* section varies slightly between an MS plan and a GSS plan, but, for the most part, addresses either all or a subset of the following topics:

- Personnel Security
  - Physical and Environmental Protection
  - Production, Input/Output Controls
  - Contingency Planning
  - Application Software Maintenance Controls
  - Hardware and System Software Maintenance Controls
  - Data Integrity/Validation Controls
  - Integrity Controls
  - Documentation
  - Security Awareness and Training
  - Incident Response Capability
- 

### Technical Controls Section

The *Technical Controls* section describes the technical control measures in place or planned that are intended to meet the protection requirements of the MS or GSS.

*Technical controls* consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

---

*Continued on next page*

## System Security Controls, Continued

---

### **Technical Controls Section Content**

The content of the *Technical Controls* section of an MS and GSS plan should address the following topics, as applicable:

- Identification and Authentication
  - Logical Access Controls
  - Public Access Controls
  - Audit Trails
- 

### **Guidance on Completing Security Controls Sections**

For guidance on how to complete the *Management, Operational, and Technical Controls* sections of a System Security Plan, refer to the Security Plan Guidance presented in Attachment A of Chapter 13 of the USDA Cyber Security Manual (DM 3500), and NIST SP 800-18.

---

## **APPENDIX E**

### **Continuity of Operations/Disaster Recovery**

This page intentionally left blank.

# Continuity of Operations/Disaster Recovery

## Overview

---

### Introduction

USDA depends upon numerous major critical systems and applications that support its day-to-day core business processes and enable the delivery of services to American farmers and the public. As a result, these systems and applications must be protected from disruptions such as power outages, water damage, fires, and viruses. While many vulnerabilities may be minimized or eliminated through the application of management, operational, and technical controls, it is virtually impossible to eradicate all risk. Thus, effective contingency planning (which includes business resumption plans, disaster recovery plans, and continuity of operation plans) and testing are essential to mitigate the risk of system and service unavailability.

---

### USDA Information Survivability Program

The USDA Information Survivability Program is managed by the Cyber Security Office and is predicated on the requirement that an IT contingency plan be developed and tested for each major system or application in accordance with federal mandates. Under this program, an agency/organization uses a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting IT systems, business processes, and facilities. At a minimum, the USDA requires the development of the following two plans to ensure that agencies and staff offices are able to effectively and efficiently reduce the adverse effects of a disastrous event:

- Business Resumption (BR) Plan
  - Disaster Recovery (DR) Plan
- 

### In This Appendix

This Appendix provides an overview of contingency planning and the processes involved.

---

### Contents

This Appendix contains the following topics:

Topic	See Page
Business Resumption Plans	E-3
Disaster Recovery Plans	E-4
Contingency Planning Process	E-5

---

*Continued on next page*

## Overview, Continued

---

### References

The following documents were used in the development of this Appendix:

- NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems
  - DM 3500, Cyber Security Manual, Chapter 14, IT Contingency and Disaster Planning
-

# Business Resumption Plans

---

## **Introduction**

As part of the contingency planning process, USDA IT and Business Program Managers must communicate and collaborate on how to continue business and recover losses if services are disrupted. By developing Disaster Recovery and Business Resumption Plans, agencies can focus on recovery solutions and cost-effective methods. This will ensure critical systems are recovered quickly and business is resumed within an acceptable timeframe.

---

## **What is a Business Resumption Plan?**

A *Business Resumption (BR) Plan* documents instructions or procedures that describe how the business will be restored after a significant disruption has occurred. A BR Plan does not address procedures to ensure continuity of critical processes throughout an emergency or disruption. However, agencies must coordinate critical processes during emergency disruptions, and detail those processes in their Disaster Recovery Plan and Occupant Emergency Plan.

---

## **BR Plan Requirements**

Each agency and staff office is responsible for developing, testing, implementing, and maintaining a BR Plan for all mission critical systems or applications in support of critical business functions. All plans must be well written, routinely reviewed, tested, and updated to provide for reasonable continuity of IT support in the event of a disruption or disaster. Such planning must also be incorporated and integrated into the system development life cycle process.

---

## **BR Plan Development Guidance**

USDA has provided Strohl Systems as the enterprise-wide software tool for use in the development of all BR Plans. Additional guidance on plan development is available in NIST SP 800-34 and CS-028, Cyber Security Guidance Regarding Disaster Recovery and Business Resumption Plans.

---

# Disaster Recovery Plans

---

**Introduction** In addition to a Business Resumption (BR) Plan, USDA requires a Disaster Recovery (DR) Plan for all mission critical systems and applications. As with BR Plans, DR Plans help to ensure that critical systems are recovered quickly and that business can resume within an acceptable timeframe.

---

**What is a Disaster Recovery Plan?** A *Disaster Recovery (DR) Plan* is an IT-focused plan designed to restore operability of the target system, applications, or computer facility at an alternate site after an emergency. The DR Plan usually applies to major, usually catastrophic, events that deny access to the normal facility for an extended period of time. The DR Plan is narrower in scope and does not address minor disruptions that do not require relocation.

---

**DR Plan Requirements** USDA requirements for a DR Plan are the same as those for a BR Plan. In essence, each agency and staff office is responsible for developing, testing, implementing, and maintaining a DR Plan for all mission critical systems or applications in support of critical business functions. All plans must be well written, routinely reviewed, tested, and updated to provide for reasonable continuity of IT support in the event of a disaster. Such planning must also be incorporated and integrated into the system development life cycle process.

---

**DR Plan Development Guidance** USDA has provided Strohl Systems as the enterprise-wide software tool for use in the development of all DR Plans. Additional guidance on plan development is available in NIST SP 800-34 and CS-028, Cyber Security Guidance Regarding Disaster Recovery and Business Resumption Plans.

---

# Contingency Planning Process

---

## Introduction

The development and maintenance of an effective contingency plan is a process involving several steps. These steps represent key elements in a comprehensive IT contingency planning capability, and the design should be integrated into each stage of the system development life cycle.

---

## Steps in the Contingency Planning Process

Each agency and staff office is responsible for accomplishing the following steps as part of the contingency planning process:

Step	Description
Conduct a Business Impact Analysis (BIA)	This analysis <ul style="list-style-type: none"> <li>• helps to identify and prioritize critical IT resources</li> <li>• determines the acceptable minimum level of system support necessary to restore mission critical core business functions, and</li> <li>• ranks business functions for restoration.</li> </ul>
Identify preventive controls	These are measures designed to <ul style="list-style-type: none"> <li>• reduce the effects of IT system disruptions</li> <li>• increase system availability, and</li> <li>• reduce contingency life costs.</li> </ul>
Develop recovery strategies	These strategies ensure that the system may be recovered quickly and effectively following an incident.
Develop DR and BR Plans	DR and BR Plans must include guidance and procedures for restoring the system and core business functions.
Maintain and update IT Contingency DR/BR Plans at least annually	Agencies and staff offices are required to update plans annually or following any significant change to their computing or telecommunications environment.

*Continued on next page*

## Contingency Planning Process, Continued

**Steps in the Contingency Planning Process**  
(continued)

Step	Description
Schedule testing for DR/BR Plans	<p>Agencies and staff offices are required to develop a testing program and schedule for tests with review by the Cyber Security Office. Deficiencies revealed must be corrected. The type of test and extent of testing will depend upon the</p> <ul style="list-style-type: none"> <li>• criticality of agency business functions</li> <li>• cost of executing the test plan</li> <li>• budget availability, and</li> <li>• complexity of information system and components.</li> </ul>
Train employees	Employees must be trained in order to execute recovery plans.
Participate in audit reviews	Informal and formal reviews of all plans will be conducted by the Cyber Security Office, the GAO, and the OIG to ensure that they are executable and in compliance with standards.

**For Additional Information and Guidance**

Additional, more detailed information and guidance on the contingency planning process and the development of contingency planning documents (such as BR and DR Plans) may be obtained from:

- NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems
- DM 3500, Cyber Security Manual, Chapter 14, IT Contingency and Disaster Planning
- CS-028, Cyber Security Guidance Regarding Disaster Recovery and Business Resumption Plans

**APPENDIX F**  
**Security Awareness and Training**

This page intentionally left blank.

# Security Awareness and Training

## Overview

---

### Introduction

Security awareness and training plays a critical part in ensuring the confidentiality, integrity, and availability of the USDA's systems and information. Since people tend to be one of the weakest links in attempts to secure systems and networks, a robust security awareness and training program helps to reduce this risk by ensuring that everyone involved in using and managing IT understand their security responsibilities, and properly use and protect the IT resources entrusted to them.

---

### What is Security Awareness & Training?

*Security awareness and training* creates user sensitivity to the threats and vulnerabilities of IT systems and the recognition of the need to protect information and the means of processing it, and teaches those who use, maintain, develop, or manage IT systems the security-related knowledge and skills that will enable them to do their job more effectively.

---

### Security Awareness & Training Program Requirements

The Computer Security Act, OMB A-130, and FISMA mandate periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of Federal computer systems. Accordingly, USDA requires that all agencies and staff offices develop, organize, implement, and maintain an IT systems security awareness training program to ensure the security of USDA information and IT resources, and to establish requirements for formal training to be conducted at least annually.

New employees are to be trained within 60 days of hire, and security awareness refresher training is required at least annually or whenever there is

- a significant change in IT direction
  - major system modifications
  - changes/upgrades in software utilized, or
  - change of duties for continued access to USDA IT systems.
- 

*Continued on next page*

## Overview, Continued

---

### Program Development Steps

There are three major steps involved in the development of a security awareness and training program:

- Design the program
  - Develop the program
  - Implement the program
- 

### In This Appendix

This Appendix provides a general description of the steps involved in developing a security awareness and training program.

---

### Contents

This Appendix covers the following topics:

Topic	See Page
Program Design	F-3
Program Development	F-5
Program Implementation	F-7

---

### References

The following documents were used in the development of this Appendix and should be referred to for further information and guidance as needed.

- NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program
  - NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
  - CS-015, Cyber Security Computer Security Awareness Training
  - CS-027, Computer Security Awareness and Training Program Plan and Vendor and Product Survey
-

# Program Design

---

## **Introduction**

An awareness and training program is the vehicle used to communicate security requirements across the USDA. The first step in the process of developing a program is to design it.

---

## **Designing the Program**

Awareness and training programs must be designed with the agency/organization mission in mind. It is important that the program support the business needs of the agency/organization and be relevant to the agency's/organization's culture and architecture. Designing the program consists of

- conducting a Needs Assessment, and
  - developing a plan.
- 

## **Conducting a Needs Assessment**

A needs assessment is a process that determines an agency's/organization's awareness and training needs. The results of a needs assessment provide justification to convince management to allocate adequate resources to meet those needs. Roles that require special training needs, such as Executive Management, System Owner, and System Administrators, should be addressed in a needs assessment.

A needs assessment can be accomplished by

- conducting interviews with key groups
  - surveys
  - reviews and assessments of current security awareness and training material, schedules, and attendees, and
  - reviews of the findings of audits and security reviews.
- 

*Continued on next page*

## Program Design, Continued

---

### **Developing a Plan**

A plan for implementing awareness and training within the agency/organization can be developed based on the information obtained in the needs assessment. A plan is a working document and should discuss the following elements:

- Existing national and local policy that requires awareness and training
- Scope of the program
- Roles and responsibilities of personnel who should design, develop, and maintain the training material and ensure appropriate employees attend or view it
- Goals to be accomplished for each aspect of the program
- Target audiences for each aspect of the program
- Mandatory courses or material for each target audience
- Learning objectives for each aspect of the program
- Topics to be addressed in each session or course
- Deployment methods to be used for each aspect of the program
- Documentation, feedback, and evidence of learning for each aspect of the program
- Evaluation and update of material for each aspect of the program
- Frequency that each target audience should be exposed to material

---

### **Implementation Priorities & Strategies**

Once the program has been developed and finalized, an implementation schedule must be developed. The needs assessment can be used at this point to determine what training needs to occur and within what timeframe. If implementation needs to occur in phases (e.g., due to budget constraints and resource availability), the factors to be used in determining which initiative to schedule first and in what order needs to be decided. Factors to consider include:

- Availability of material/resources
  - Role and organizational impact
  - State of current compliance
  - Critical project dependencies
-

# Program Development

---

## Introduction

Following the design of the awareness and training program, supporting material can be developed or obtained. The support material chosen should integrate into the audience's job function. The objective is to get and hold the audience's attention and inspire them to use what they see and hear in the program.

---

## Developing Program Materials

Training material should be developed or obtained with the following in mind:

- What behavior do we want to reinforce (awareness)?
- What skill or skills do we want the audience to learn and apply (training)?

Awareness material and training material have different goals in that

- an *awareness* program should make all individuals aware of their commonly shared IT security responsibilities, and
  - *training* material should include everything related to security that attendees need to know in order to do their jobs.
- 

## Developing Awareness Materials

When developing awareness materials, the agency/organization should focus on what it wants all personnel to be aware of regarding IT security. Topics that can be mentioned and briefly discussed include:

- Password usage
  - Protections from malicious code
  - Policy
  - Web usage
  - Data backup and storage
  - Incident response
  - Changes in systems environment & increases in risk
  - Inventory & property transfer
  - Personal use & gain issues
  - Encryption & transmission of sensitive information over the Internet
  - Laptop security
  - Personal digital assistant (PDA) security
- 

*Continued on next page*

## Program Development, Continued

---

### **Awareness Material Sources**

Potential sources of material on security awareness topics such as those described above include:

- E-mail advisories
  - Professional organization and vendors
  - Online IT security daily news websites
  - Periodicals
  - Conferences, seminars, and courses
- 

### **Developing Training Materials**

When developing training materials, the agency/organization should focus on what skill/s it wishes the audience to learn. Each audience that requires training tailored to their security responsibilities should be identified.

*Note:* NIST SP 800-16 presents a methodology that can be used to identify roles and training requirements and should be referenced for further assistance.

---

### **Training Material Sources**

Material for training courses can be developed in-house or can be outsourced. NIST SP 800-16 can be used to develop courses and material if in-house expertise exists and the necessary resources are available. In addition, training courses can be obtained from

- other federal agencies, and
  - vendors who offer “off-the-shelf” or tailored courses.
- 

### **USDA Security Awareness & Training Vendor and Product Survey**

The USDA Security Awareness & Training Vendor and Product Survey provides information on products that were surveyed and assessed by USDA in order to provide computer security awareness and training for its diverse and decentralized workforce. The survey provides information on potential vendors and products based on delivery mechanisms available and target audiences, and is included in the USDA Computer Security Awareness Training Program Plan.

---

# Program Implementation

---

## **Introduction**

The final step in the development of an awareness and training program is implementation. Implementation follows the successful completion of a needs assessment, the development of a program plan, and the development or selection/purchase of appropriate awareness and training material.

---

## **Program Acceptance**

Before the program can be implemented, it must be explained to and accepted by management. Senior executives and managers should be briefed as to the expected results of the program and its benefits in order to achieve support for its implementation and the necessary commitment of resources. In addition, those responsible for designing, developing, and implementing the awareness and training program (e.g., USDA Information System Security Program Managers) should be made fully aware of their roles and responsibilities.

---

## **Awareness Material Delivery Techniques**

There are a number of ways that awareness materials and messages can be presented and disseminated throughout an organization, including:

- Messages on trinkets (e.g., pens, key fobs, post-it-notes, etc.)
  - Posters
  - Screensavers and warning banner messages
  - Newsletters
  - Agency-wide e-mail messages
  - In-person, instructor-led sessions
  - IT security days
  - “Brown bag” seminars
  - Pop-up calendars
  - Crossword puzzles
- 

## **Training Material Delivery Techniques**

Techniques for effectively delivering training material include:

- Interactive video training (IVT)
  - Web-based training
  - Non-web, computer-based training
  - Onsite, instructor-led training
- 

*Continued on next page*

## Program Implementation, Continued

---

### **Post - Implementation**

An awareness and training program can quickly become obsolete if care is not taken to make sure that it is kept up-to-date and reflects current technologies, environments, and requirements. Hence, a process should be put in place post-implementation to periodically review program content as well as monitor compliance and effectiveness of the program. The use of an automated tracking system that captures key information regarding program activity (e.g., courses, dates, audience, cost, sources, etc.) is recommended. Such a system will facilitate enterprise-wide analysis and reporting regarding awareness, training, and education activities.

---

**APPENDIX G**  
**Security Controls Review**

This page intentionally left blank.

# Security Controls Review

---

**Introduction** A *security controls review* is an evaluation of the management, operational, and technical security controls in an information system to determine the effectiveness of those controls in a particular environment of operation and the remaining vulnerabilities in the system after implementation of such controls.

---

**Purpose** Reviews or assessments of information systems are conducted to

- determine if security controls are correctly implemented
- determine if security controls are effective in their application, and
- ensure that security-applicable laws, directives, regulations, and guidelines are met.

---

**Security Controls Review Requirements** OMB A-130 and FISMA require an annual independent evaluation of information security program and practices to determine their effectiveness. Evaluations are to include the testing of management, operational, and technical controls of all information systems. The type and rigor of a review or audit should be commensurate with the acceptable level of risk established for the system and the likelihood of learning useful information to improve security.

---

**Evaluation Methods** Methods that can be used to evaluate security controls include:

<b>Evaluation Method</b>	<b>Description</b>
Self-Assessments	A checklist approach that measures the existence & effectiveness of security controls based on an extensive questionnaire containing security objectives and suggested techniques.

---

*Continued on next page*

## Security Controls Review, Continued

### Evaluation Methods (continued)

Evaluation Method	Description
Security Testing & Evaluation (ST&E)	<p>An examination or analysis of protective measures once a system is fully integrated and operational with the following objectives:</p> <ul style="list-style-type: none"><li>• To uncover design, implementation and operational flaws that could violate security policy</li><li>• To determine the adequacy of security mechanisms</li><li>• To assess the degree of consistency between the documentation and its implementation</li></ul> <p>ST&amp;E addresses computer security, communications security, emanations security, physical security, personnel security, administrative security, and operations security.</p>
Penetration Testing	<p>Attempts to circumvent the security features of a system with the purpose of identifying methods of gaining system access using common tools and techniques developed by hackers.</p>
Vulnerability Scanning	<p>Identifies hosts, open ports, and associated vulnerabilities automatically instead of relying on human interpretation of the results.</p>

**Note:** Typically, several testing techniques are used in combination to gain a more comprehensive assessment of a system's overall security posture.

### References

The following documents were used in the development of this Appendix and should be referenced for additional and more detailed information regarding security control reviews and assessments.

- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST Special Publication 800-26, Security Self Assessment Guide for Information Technology Systems
- NIST Special Publication 800-42, Guideline on Network Security Testing
- NIST Special Publication 800-53, Security Controls for Federal Information Systems

**APPENDIX H**  
**Personnel Security**

This page intentionally left blank.

# Personnel Security

## Overview

---

### Introduction

In general, the greatest potential harm or disruption to a system comes from the actions of individuals, both intentional and unintentional. As a result, a broad range of security issues surround how individuals interact with computers and the access and authorities they need to do their job. Personnel security seeks to address these issues.

---

### Purpose

The purpose of personnel security is to reduce the risk of disruption, damage, loss, disclosure or other adverse impact to information and information systems due to individuals authorized to use or maintain such information and systems.

---

### Areas to Incorporate Personnel Security

Personnel security measures should be incorporated into the following areas:

- Position staffing
  - User administration
- 

### In This Appendix

This Appendix provides an overview of personnel security and how it should be incorporated into an agency's/organization's staffing and user administration efforts.

---

### Content

This Appendix contains the following topics.

Topic	See Page
Staffing	H-3
User Administration	H-5

---

*Continued on next page*

## Overview, Continued

---

### References

The following documents were used in the development of this section and may be referenced for further information:

- 5 CFR 731, 732, and 736
  - NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
  - NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook
  - CS-038, Cyber Security Guidance Regarding Background Investigations, Suitability Determinations and Clearances for IT Personnel (Planned May 2004)
-

# Staffing

---

## The Staffing Process

Staffing refers to the process of filling a job position based on specific requirements and the ability of an applicant to fulfill those requirements. In terms of personnel security, there are four steps in the staffing process during which security measures can be applied:

1. Defining the job
  2. Determining the public trust level and sensitivity of the position
  3. Filling the position (which involves screening applicants, determining suitability, and selecting an individual)
  4. Training
- 

## Defining the Job

Early in the process of defining a position, security issues should be identified and dealt with. Once a position has been broadly defined, the responsible supervisor should determine the type of computer access needed for the position. There are two general principles to apply when granting access:

- Separation of duties
- Least privilege

*Separation of duties* refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

*Least privilege* refers to the security objective of granting users only those accesses they need to perform their official duties.

---

## Determining Position Sensitivity

Knowledge of the duties and access levels that a particular position will require is necessary for determining the public trust level and sensitivity of the position. The responsible management official should correctly identify position sensitivity levels so that appropriate, cost-effective screening can be completed. Determining the appropriate level is based upon such factors as the type and degree of harm (e.g., disclosure of private information, interruption of critical processing, computer fraud) that an individual can cause through misuse of the computer system as well as more traditional factors, such as access to classified information and fiduciary responsibilities.

---

*Continued on next page*

## Staffing, Continued

---

### Filling the Position

Once a position's level of public trust and sensitivity has been determined, the position is ready to be staffed. At this point, a screening process may be employed as a security measure. Background screening helps determine whether a particular individual is suitable for a given position.

Within the federal government, the most basic background screening technique involves checking

- for a criminal history
- FBI fingerprint records, and
- other federal indices.

The exact type of screening that takes place depends upon the level of public trust and sensitivity of the position and applicable federal and agency regulations.

*Note:* In general, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening to reduce the risk to the organization.

---

### Training

Even after a candidate has been hired, the staffing process is not considered to be complete until employees have been trained to do their job, which includes computer security responsibilities and duties. Such security training can be very cost-effective in promoting security. Organizations may provide introductory training prior to granting a user system access, and follow-up with more extensive training.

---

# User Administration

---

## Introduction

Effective administration of users' computer access is essential to maintaining system security. User Administration deals with

- user account management, and
  - auditing.
- 

## User Account Management

User account management involves

- the process of requesting, establishing, issuing, and closing user accounts
- tracking users and their respective access authorizations, and
- managing these functions.

To address security issues involved in user account management, processes and procedures should be in place to ensure that

- user accounts are established and maintained for authorized users only
  - users understand their responsibilities prior to being given system access
  - appropriate access restrictions are assigned to users based on the principles of least privilege and separation of duties, and
  - user accounts no longer needed are removed in a timely manner.
- 

## Auditing

From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine

- the levels of access assigned to each individual
  - conformity with the concept of least privilege
  - whether all accounts are still active
  - whether management authorizations are up-to-date, and
  - whether required training has been completed.
-

This page intentionally left blank.

**APPENDIX I**  
**Configuration Management**

This page intentionally left blank.

# Configuration Management

---

## **Introduction**

Information systems are typically in a constant state of migration due to continual upgrades to hardware, software, or firmware, and possible modifications to the surrounding environment where the system resides. To ensure potential security impacts of specific changes to an information system or its surrounding environment are considered prior to their implementation, an effective configuration management and control policy and associated procedures are required.

---

## **What is Configuration Management?**

Configuration Management (CM) is a control activity applied to the components of an Information Technology (IT) system throughout its life to provide assurance that the system components are well defined and cannot be changed without proper justification and full knowledge of the consequences.

CM ensures that the system state can be accurately determined for the following components:

- Hardware
- Software
- Communications services
- Documentation

Configuration management procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system, and subsequently controlling and maintaining an accurate inventory of any changes to the system.

---

## **Benefits of CM**

Applying configuration management to an IT system can enhance its cost-effectiveness and security. Benefits of CM include:

- Changes are less error prone and, therefore, less costly to complete
  - Results in better-designed changes due to early identification of the impact of a modification on other components
  - Results in better developed and properly justified changes due to formal approval of change requests
- 

*Continued on next page*

## Configuration Management, Continued

---

### Benefits of CM *(continued)*

- Reduces risk of malicious changes by making each change visible and ensuring full accountability and audit
  - Simplifies trouble shooting and recovery from a loss or disaster by having a clear statement of each system component and its configuration state
- 

### CM is a Requirement for System Accreditation

All USDA General Support Systems (GSSs) and Major Applications (MAs) must undergo a certification and accreditation process and be accredited by a Designated Accrediting Authority (DAA) prior to being placed in operation. *One of the requirements for system accreditation is the implementation of a formal configuration management process.*

The documentation maintained for CM also provides the necessary evidence to the DAA that the security aspects of each change since the system's last accreditation review has been properly evaluated. These procedures significantly simplify the re-accreditation process.

---

### USDA CM Policy

USDA requires all offices and agencies to implement an effective CM program for all IT systems under their control. IT Program Offices are responsible for providing overall CM guidance and procedures for their subordinate organizations.

#### ***Configuration Control Board***

Configuration management baselines (and recommendations for subsequent changes to those baselines) are to be established by a Configuration Control Board (CCB). Each CCB must be chaired by a Change Control Authority (CCA), a senior manager (often the project manager or system owner) who can authorize the expenditure of resources and make decisions.

#### ***Configuration Management Plan***

Agencies that manage large computing facilities must develop and implement site Configuration Management Plans and procedure documents. Agencies with systems that do not utilize large computing facilities are required to create individual CM plans and procedures to augment those developed at the agency-wide level.

---

*Continued on next page*

## Configuration Management, Continued

---

### Five Major Functions of CM

CM consists of the following five major functions:

- Configuration Management Planning and Management
  - Configuration Identification
  - Configuration Change Control
  - Configuration Status Accounting
  - Configuration Audit and Verification
- 

### CM Planning & Management

CM begins with the planning process. CM planning includes

- planning
- coordinating, and
- managing

all of the tasks necessary to implement and conduct CM activities, and occurs throughout all life-cycle phases of a system. Documentation of the planning process and development of the CM Plan (CMP) formalizes individual roles and ensures continuity of CM practices at all levels of management.

*All offices, agencies, programs, teams, organizations, contractors, and consultants that develop or maintain USDA systems must develop and implement a CM plan.*

---

### Configuration Identification

The configuration identification process is the foundation for all other CM processes. It documents the products of system engineering and the approved configuration of the physical and functional characteristics of the system/product.

In the configuration identification process, any piece of hardware, software, or both that satisfies an end use function and is designated for separate configuration management becomes a Configuration Item (CI). The number and composition of CIs designated in a system is a design decision.

**Example:** For a system containing several software application programs, each program and its related documentation and data might be designated a configuration item.

---

*Continued on next page*

## Configuration Management, Continued

---

**Configuration Change Control** The configuration change control process manages the current configuration baseline that was obtained from the results of the configuration identification process. The types and levels of documentation subject to Government configuration control authority are defined in the Configuration Management Plan (CMP), or by a contractor if the system is being outsourced.

Proposed changes to system baselines must be submitted to the appropriate CCB where they are approved or disapproved by the CAA. Upon implementation of a change, all documentation (e.g., operation manuals, training, materials, etc.) must be updated and released concurrently.

---

**Configuration Status Accounting** Each of the above CM processes provides information to the configuration status accounting (CSA) database. CSA tracks configuration documentation changes and the configuration of items. These records should include both current and historical information to ensure traceability from the initial requirements or previous baseline.

Metrics (i.e., performance measurements) can be obtained from the information in the CSA database and used to monitor and improve the CM process.

---

**Configuration Audit and Verification** The configuration audit and verification process is used to verify that a product's performance requirements have been achieved by the product/system design, and that the product/system design has been accurately documented.

Verification is based on

- information from the CSA database
- results of product/system testing
- physical hardware or software (or its representation), and
- the software engineering environment.

Successful completion of verification and audit activities results in a verified product/system and documentation set that may be confidently considered a Product/System baseline.

---

*Continued on next page*

## Configuration Management, Continued

---

### References

The following documents were used in the development of this section and may be referenced for further information:

- NIST Special Publication 800-53, Security Controls for Federal Information Systems
  - CS-009, Guidance on Configuration Management, Part I – Policy and Responsibilities
-