NISTIR 4378

AUTOMATED INFORMATION SYSTEM SECURITY ACCREDITATION GUIDELINES

Edward Roback
NIST Coordinator

U.S. Department of Transportation
Federal Aviation Administration

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4378

AUTOMATED INFORMATION SYSTEM SECURITY ACCREDITATION GUIDELINES

U.S. Department of Transportation
Federal Aviation Administration

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

August 1990

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents the Federal Aviation Administration's Automated Information System Security Accreditation Guidelines. This document provides procedures for the preparation of documentation for the security accreditation of automated information systems.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this methodology. However, as this material may be of use to other organizations, the report is being reprinted by NIST to provide for broad public dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the Federal Aviation Administration, U.S. Department of Transportation, for their permission to publish this report.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, National Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

AUTOMATED INFORMATION SYSTEM
SECURITY ACCREDITATION GUIDELINES

30 November 1989

DEPARTMENT OF TRANSPORTATION

FEDERAL AVIATION ADMINISTRATION

CONTENTS

CONTENTS

PAGE

FIGURES

PURPOSE

This guideline is directed to the FAA Automated Information System (AIS) Security Officers (AISSO) and AIS Security Managers (AISSM). It establishes procedures for preparation of documentation required for accreditation of the security of the FAA's AIS. It makes the accreditation process as straight-forward as possible for any FAA system, whatever its purpose or complexity.

DEFINITION

Accreditation is the "formal declaration that the appropriate AIS security countermeasures have been properly implemented." (Federal Aviation Administration Automated Information System Security Program, Order 1600.54B; February 7, 1989; page 263)

RESPONSIBILITY

The AISSM is responsible for identifying the Data Processing Activities (DPAs) in the Data Processing Installation (DPI) for which he or she is responsible. The AISSM is also responsible for supervising AISSOs. The AISSOs are responsible for preparing the documentation required for accrediting DPAs. "DPA" is defined on page 2 of these guidelines.

The AISSO is responsible for completing the forms and other materials in this guideline for each assigned DPA. The AISSO is also responsible for assembling the Accreditation Report, which consists of the forms and other materials. The report describes the DPA, assesses the extent to which it is at risk from threats to its security, and recommends an accreditation action. The AISSO sends the completed report to the AISSM.

THE REQUIREMENT

The requirement for accreditation, established in FAA Order 1600.54B, applies to all FAA DPAs. These include air traffic control and administrative systems now in operation, and those under development or planned.

Accreditation requires the AISSM to identify the DPAs in the DPI, and the AISSOs to complete the forms and other materials in these guidelines. Designated Approving Authorities (DAA) then sign accreditation statements that formally accept risks to each DPA. The Appendix to these guidelines outlines the DAA's action.

DPI AND DPA IDENTIFICATION

The AISSM is required to identify the DPI and all of the DPAs in the DPI. The definitions and instructions in this section are for the AISSM to follow to accomplish this task.

A DPI is a facility, office, service, division or branch.

A DPA is "an assembly of computer equipment, facilities, personnel, software and procedures configured for the purpose of storing, calculating, computing, summarizing, and retrieving data and information with a minimum of human intervention."(FAA Order 1600.54B; I-2).

To identify the DPI and all of the DPAs in the DPI, the AISSM completes the DPI and DPA Identification Form in Figure 1 on page 4. Send copies of the completed form to the AISSC, and to the AISSOs who are responsible for preparing Accreditation Reports for the DPAs identified on the form.

The AISSC uses the form to establish the DPAs that are part of the DPI.

The AISSOs use the form to determine the DPAs for which they are responsible. However, they do not include it in the Accreditation Report.

Follow these instructions to complete the DPI and DPA Identification Form:

Item 1: Report the DPI's official title. The DPI's title is the same as the title of your facility, office, service, division or branch.

Item 2: Report your name and title.

Item 3: Report your routing symbol, phone number and office address.

Item 4: Summarize the official function or purpose of the facility, office, service, division or branch that you report as the DPI.

Item 5: List all of the DPAs located in the DPI, the name of the DPA and its address (if different from the DPI's address). Identify, by name, the AISSO for each DPA. Add continuation pages as necessary.

- DPAs are mainframes, minicomputers, personal computers, or networks of computers. A DPA may include CPUs, disk or tape drives, switching and control units, printers, etc. They may be configured as office automation systems composed of multiple pieces of equipment.
- DPAs are the administrative property of the DPI. They are physically located in the DPI's offices, or dispersed in the field (e.g., remote radars, navigation and weather sensing equipment).
- DPAs may be remotely accessed by users from other DPAs.
- DPAs may consist of connected equipment that serves one function (e.g., the Aviation Weather Observing System (AWOS) sensors connected to an AWOS Data Acquisition System (ADAS) at an airport).
- If the equipment that makes up the DPA is located at one site, report the address of that site. If the equipment is dispersed to more than one site, enter "dispersed to" and briefly describe the locations (e.g., "dispersed to airport surface").

Figure 1
DPI AND DPA IDENTIFICATION FORM

The AISSM completes this form to identify the Data Processing Installation (DPI) and the Data Processing Activities (DPAs) that are part of the DPI.

---

1. DPI Title: _____
(Facility, Division, Branch, Program Office or other)

2. AIS Security Manager: _____
(name) (title)

3. Address: _____ Phone: _____
(routing symbol)

_____
(street No.)

_____
(city) (state) (zip)

4. Functions (the official purpose of the facility, division, branch or other organization that comprises the DPI).

_____

_____

_____

5. List the DPAs in the DPI: (Add continuation pages.)

1. Title: _____
Address: _____
AISSO: _____

2. Title: _____
Address: _____
AISSO: _____

3. Title: _____
Address: _____
AISSO: _____

To make sure the AISSOs know the titles and locations of the specific DPAs for which they are responsible, write a memo to each AISSO. In this memo, clearly identify the title(s) and address(es) of the DPA(s) for which the AISSO is responsible. Also identify the name, title and organization of the Designated Approving Authority (DAA) for each DPA. Attach a copy of the DPI and DPA Identification Form to this memo.

SCHEDULE

The instructions in this section are for the AISSO to follow to complete the schedule in Figure 2 on page 7.

Use the schedule to propose dates for accomplishing each of the tasks required to complete the Accreditation Report. Also use the schedule to report the actual date each task is completed. Send the schedule to the AISSM. The AISSM will use it to track the accreditation process.

1. PROPOSED DATES

Figure 2 presents a list of the tasks involved in completing the Accreditation Report. Propose a date for completing each task. The date will depend on the amount of work required. This will vary with the size and complexity of the DPAs and the resources available to accomplish the work. For example, it may take a half-hour for one person to complete the risk assessment for a stand-alone office automation system. However, it may take over a labor-week to complete this task for an IBM 3084.

If necessary, consult with the AISSM or the AISSC to estimate the work required for each task and to identify the resources that are available to complete the tasks by the proposed dates.

2. ACTUAL COMPLETION DATES

In addition to proposed dates, the schedule includes a column for entering the dates that the requirements for the report are actually completed. Enter these dates as they occur.

3. REVISIONS

Submit a revised schedule, with changes in proposed and actual completion dates to the AISSM on a monthly basis. The AISSM will review the schedule to determine if additional resources are necessary for timely completion of the Accreditation Report and will send a copy of the revised schedule to the AISSC.

Figure 2: SCHEDULE

REQUIREMENT	DATE PROPOSED	DATE COMPLETED
1. TITLE PAGE		
2. TABLE OF CONTENTS		
3. FORM 1: DPA SECURITY PROFILE		
4. FORM 2: OFFICE AUTOMATION RISK ASSESSMENT OR LAVA		
5. FORM 3: CONTINGENCY PLAN OR WAIVER		
6. FORM 4: SENSITIVE APPLICATION CERTIFICATION OR WAVER		
7. SUMMARY		
8. FORM 5: ACCREDITATION REQUEST		
9. FORM 6: DRAFT ACCREDITATION STATEMENT		

THE ACCREDITATION REPORT

The instructions in this section are for the AISSO. Before conducting the tasks required in this section, review the responsibilities for accreditation established in Order 1600.54B, Chapter 1, Paragraph 10. Also review the requirements for accreditation specified in Order 1600.54B, Chapter 15.

Then follow these instructions to complete a separate Accreditation Report for each DPA assigned to you. They explain how to prepare the six forms and the other materials identified in the schedule and listed below:

1. Title Page;
2. Table of Contents;
3. Form 1: DPA Security Profile;
4. Form 2: Office Automation DPA Risk Assessment, or Los Alamos Vulnerability and Risk Assessment (LAVA);
5. Form 3: Contingency Plan or waiver;
6. Form 4: Sensitive Application Certification Statements or waiver;
7. Summary;
8. Form 5: Accreditation Request; and
9. Form 6: Draft Accreditation Statement.

The following sections of the guidelines include these forms and instructions for completing each form or other requirement. To make it easier to complete the forms, leave them in the guidelines while you fill them out. When you finish, remove the completed forms from the guidelines. Then staple or bind them together to make up the Accreditation Report.

1. TITLE PAGE

The AISSM will send you a memorandum with a DPI and DPA Identification Form (Figure 1 on page 4) that identifies one or more DPAs for which you are responsible. This memo also identifies the name, title and organization of the Designated Approving Authority (DAA) for each DPA. Contact the AISSM if you have not received this information, because you will need it to complete the Accreditation Report title page.

Figure 3
DPA ACCREDITATION REPORT
TITLE PAGE

FEDERAL AVIATION ADMINISTRATION

(DPI TITLE)

(DPA TITLE)
SECURITY ACCREDITATION REPORT

Prepared By:
(Name and Title of AISSO)
(Organization)

Prepared For:
(Name and Title of DAA)
(Organization)

Conveyed By:
(Name and Title of AISSM)
(Address)

Conveyed on: (Month, Day, Year)

FOR OFFICIAL USE ONLY

Public availability to be determined by 5 U.S.C. 552.

Before you complete the DPA Accreditation Report, retype the title page to include this information and also your name and the name and title of the AISSM. Do not include the date the report is conveyed. See Figure 3 on page 9.

2. TABLE OF CONTENTS

After you have completed the applicable forms for the Accreditation Report, retype the Table of Contents (on page 8 of these Guidelines) to show the proper page numbers. Insert the Table of Contents after the Title Page in the finished report.

3. DPA SECURITY PROFILE

Form 1: DPA Security Profile, begins on page 13. Consult with the system manager, users, programmers, maintenance and procurement personnel, and any other associated persons to become familiar with the DPA and its operations before filling out this form.

The form includes instructions for filling it out. Some additional instructions are:

Item 1: DPA Identification. Report your name, routing symbol and telephone number and copy the DPA's title and address from the DPI and DPA Identification, Figure 1, No. 5 on page 4.

Item 2: Configuration. The definition of "DPA" is on page 2 of these guidelines. There is additional information for identifying the DPA on page 3. Review this information and then check one of the six boxes on the form that most closely describes the particular DPA. If none of the types apply, check the box marked "Other" and write a brief description of the DPA. Later, you will use your answer to this item as the basis for selecting a method for assessing risks to the DPA. (See pages 17 and 28.)

Item 3: Hardware Inventory. List the DPA's hardware. If the hardware is already listed in the System Inventory Directory maintained by AMS-300, the Personnel Property Management Information System (PPMIS), or in another listing, check the appropriate box(es) and attach current print-outs.

Otherwise, do the inventory yourself by reporting the name and providing a brief description of each component, (e.g., IBM 3084 mainframe, DG MV-1500 minicomputer, IBM PC-AT, LaserJet II

Printer, etc.), list the manufacturer's name, and the model and serial numbers of each unit (these are usually on the backs of the components).

Item 4: Software Inventory. List the name and manufacturer of each software package that is physically resident on the DPA. Include the operating system.

Item 5: Storage Media. Check one or more of the box(es) to describe the DPA's storage media. If none of the five types apply, check the box marked "Other". Then write a brief description of the type of storage media used by the DPA.

Item 6: Owner. Attach FAA Form 1600-56 (2-88), "Agreement for Use of Privately Owned Computers Accessing Government Data," for privately owned components of the DPA. Get these forms from the AISSC.

Item 7: Use. Check the box to report if direct or remote access to the DPA is restricted to normal business hours or if the DPA is available for use 24 hours a day.

Item 8: Users. Follow the instructions on the form for completing this item to identify the DPA's users.

Item 9: Cost. Follow the instructions on the form to estimate the cost of the DPA.

If your basis is the original cost of the equipment, use the table provided on the form to follow the OMB and GSA requirements that replacement cost estimates include income lost because the money spent on the DPA is not invested in income-producing assets. (Office of Management and Budget Circular A-94, Revised March 27, 1972. Also see General Services Administration, Federal Information Resource Management Regulation: Acquisition Policies, 201-24.207, 1984)

Item 10: Sensitivity. Consult with the AISSC if necessary to determine the sensitivity levels of the information that the DPA processes. Then check the box(es) on the form to report if the DPA processes classified National Security Information (Level I); unclassified sensitive data (Level II) - including Privacy Act data; or unclassified non-sensitive data (Level III). Use the following information to make this determination:

> Level I: Classified information is officially classified by an original classification authority as either Top Secret, Secret or Confidential.
>
> "The Department of Transportation has no Top Secret original classification authority and only the Secretary and those positions designated by the Secretary have original classification authority for Secret and Confidential material."(Information Security Do's and Don'ts in the Department of Transportation,

DOT/OST; 2, also see Classification, Declassification, and Control of National Security Information, DOT Order 1640.4C).

Level II: Unclassified sensitive data are defined by the Computer Security Act of 1987 (Public Law 100-235) as:

"any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

Unclassified sensitive data are also defined by OMB Circular A-130 as:

"data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act."

In summary, sensitive data include information:

1. Protected under the Privacy Act;
2. Exempt from public release under the Freedom of Information Act;
3. Labeled For Official Use Only; and information whose
4. Loss disclosure, or misuse could adversely affect the national interest or the ability of the agency to accomplish its mission.

Level III: Unclassified non-sensitive data include information that is neither classified nor sensitive.

Item 11: Comments. Provide any additional information or clarification in this item. Also provide comments on the clarity and completeness of the form.

FORM 1
DATA PROCESSING ACTIVITY (DPA) SECURITY PROFILE

Please complete and include this Security Profile Form in the Accreditation Report for each DPA.

1. **DPA IDENTIFICATION**

Fill in the following information:

A. **AISSO:** _____
(Name) (Title)

B. **Routing Symbol:** _____

C. **Phone:** (FTS) _____

D. **DPA Title:** _____

E. **Address:** _____
(Street No.) (City) (State) (Zip)

2. **CONFIGURATION**

This item categorizes DPAs by type.

Check the box that most closely describes the configuration of the DPA:

A. [ ] **Office Automation (OA) System.**
(Examples are desk-top PCs and dedicated word processors that do not interface with other devices.)

B. [ ] **OA system with Remote Capability.**
(Primary processors that may be remotely accessed from terminals.)

C. [ ] **Network.**
(A set of processors that interface through communications media and switching devices so that users may share applications and data.)

D. [ ] **Minicomputer**

E. [ ] **Terminal**
(These are separate DPAs if they are administered independently of other equipment with which they interface.)

F. [ ] **Mainframe**

G. [ ] **Other:**

_____

_____

_____

FORM 1
DATA PROCESSING ACTIVITY (DPA) SECURITY PROFILE

3. HARDWARE INVENTORY

A. Is the DPA's hardware identified in the System Inventory Directory maintained by AMS-300?

[ ] Yes [ ] No

B. Is its hardware identified in the Personnel Property Management Information System (PPMIS)?

[ ] Yes [ ] No

C. What other inventory system identifies the hardware?

_____

(Name of the system. Write "none" if not identified in other inventory.)

D. Is all of the DPA's hardware located at the address identified in Item 1E?

[ ] Yes [ ] No

E. If the hardware is identified in an inventory system, attach a current inventory listing and go to Item 4. Otherwise, complete 3F.

F. Complete the following Hardware Inventory.

If you checked the "No" box for 3D, identify the location (by address) of each component, otherwise do not indicate the location.

(If reporting more than ten components, please provide a continuation page.)

HARDWARE REPORTED FOR THIS DPA SHOULD NOT BE REPORTED FOR ANY OTHERS.

ITEM	DESCRIPTION	MANUFACTURER	MODEL NO.	SERIAL NO.	LOCATION
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

4. SOFTWARE INVENTORY

Please attach a current listing of all software that is physically resident on components listed in Item 3. Attach authorizations for public domain or personally owned software.

FORM 1
DATA PROCESSING ACTIVITY (DPA) SECURITY PROFILE

5. STORAGE MEDIA

Check the boxes for all of this DPA's storage media.

A.	[ ]	Floppy Disk	E.	[ ] Fixed Hard Card
B.	[ ]	Fixed Hard Disk	F.	[ ] Other Media:
C.	[ ]	Removable Hard Disk		_____
D.	[ ]	Tape Drive		_____
				_____
				_____

6. OWNER:

IF COMPONENTS OF THE DPA ARE OWNED BY INDIVIDUALS, ATTACH COPIES OF Agreement for Use of Privately Owned Computers Accessing Government Data, FAA FORM 1600-56 (2-88).

7. USE

Check the box to report if the DPA is available for direct or remote access:

[ ] only during normal business hours [ ] on a 24 hour basis.

8. USERS

Check the box to report if the DPA is used (directly and/or remotely) by:

[ ] DPI personnel only. [ ] DPI personnel and others.

FORM 1
DATA PROCESSING ACTIVITY (DPA) SECURITY PROFILE

9. COST

To estimate the DPA's cost obtain current vendor quotations, or determine the original costs of hardware and software and use the Present Worth Factor (Table 1) to adjust these costs by 10% per year to account for lost returns on investment, as follows:

1. Determine the original cost of each hardware and software component listed in Items 4 and 5.
2. Determine the number of years since acquisition of each component;
3. Multiply the original cost of each component by the Present Worth Factor for the number of years;
4. Add the resulting values;
5. Enter this total on the following line.

Total Cost: $ _____

Table 1
10% Compound Interest
Present Worth Factor

Years	Original Cost		Present Worth Factor		Current Value
1	$00.00	x	1.1	=	$00.00
2			1.21		
3			1.331		
4			1.4641		
5			1.6105		
6			1.7716		
7			1.9487		
8			2.1436		
9			2.3579		
10			2.5937		
11			2.8531		
12			3.1384		
13			3.4523		
14			3.7975		
15			4.1772		
16			4.5950		
17			5.0545		
18			5.5599		
19			6.1159		
20			6.7275		

10. SENSITIVITY

Classified (Level I) data is official Top Secret, Secret or Confidential information.

Unclassified sensitive (Level II) data is either protected by the Privacy Act of 1974, national security information designated "For Official Use Only", proprietary information, such as pre-award procurement data, or otherwise defined as sensitive by the Computer Security Act of 1987.

Unclassified, non-sensitive data are all data that are not officially classified and are not Unclassified sensitive data as defined by this Act.

Check the box(es) to report the sensitivity level(s) of the data processed:

[ ] Classified [ ] Unclassified Sensitive [ ] Unclassified non-sensitive

11. COMMENTS

4. OFFICE AUTOMATION DPA RISK ASSESSMENT

FAA Order 1600.54B requires you to identify risks to the DPA from environmental and human threats. The Order requires that you use one of two methods to accomplish this task:

1. The Office Automation DPA Risk Assessment; or
2. The Los Alamos Vulnerability and Risk Assessment (LAVA).

Review Form 1, Item 2 on page 13 to determine whether to use the Office Automation DPA Risk Assessment in Form 2 on page 19, or to use LAVA. If you checked box A, B, or E, on Form 1 Item 2, use the Office Automation DPA Risk Assessment. If you did not check one of these three boxes, go to page 28, which provides guidelines for LAVA. If you use LAVA, include a copy of the printed LAVA report in the Accreditation Report instead of Form 2.

If you don't use LAVA, follow these instructions to complete the Office Automation DPA Risk Assessment in Form 2.

Items 1 through 7 in Form 2 require estimating whether the risk from exposure to each of seven threats is high, medium or low. Form 2 also requires reporting safeguards that now protect the DPA from these threats and safeguards that are planned. Item 8 of Form 2 is an evaluation of the DPA's risks and vulnerabilities that will help you determine if present or planned safeguards are adequate to protect it.

Before completing this form, consult with technical and administrative personnel, if necessary, to:

1. Make sure you understand the configuration of the DPA, know all of its components and their locations, and understand its operations.
2. Familiarize yourself with the construction and condition of the DPA's components and the facility or facilities that house these components.
3. Know about environmental and human hazards that potentially threaten the DPA, and actual incidents that have threatened the DPA in the past.

4. Evaluate the extent to which the DPA is exposed to threats from:
    1. Fire;
    2. Unstable Power Supply;
    3. Water;
    4. Loss of Data Integrity;
    5. Electrical Hazards;
    6. Unauthorized Use or Misuse; and
    7. Physical Penetration.

5. Identify safeguards that protect the DPA. These may involve physical, electronic, administrative, procedural and other mechanisms.

Then read the instructions in Form 2 and complete each item.

FORM 2
OFFICE AUTOMATION DPA RISK ASSESSMENT

Complete this form for each Office Automation (OA) DPA.

First fill in the following information, then read the instructions on this page and complete each item.

Title of DPA: _____ **Date:** ____/____/____/

AISSO: _____ **PHONE:** _____
(name) (title)

AISSM: _____ **PHONE:** _____
(name) (title)

DPA Address: _____
(routing symbol)

_____
(Street Number) (City) (State) (ZIP)

INSTRUCTIONS

To complete this form:

A. Review the brief description provided for each of the seven threats: 1) Fire, 2) Unstable Power Supply, 3) Water, 4) Loss of Data Integrity, 5) Electrical Hazard, 6) Unauthorized Use or Misuse, and 7) Physical Penetration;

B. Review available documentation, such as system specifications, handbooks, emergency plans, etc., interview individuals who are familiar with the DPA's operations, and informally survey its environmental and human threat exposures;

C. Based on these reviews, for each threat check the box that, in your judgement, represents the risk to the DPA - High, Medium, or Low.

D. Follow the instructions to report present and planned safeguards.

E. Follow the instructions in Item 8 to determine if the safeguards provide adequate security for the DPA and to recommend additional safeguards, if necessary.

FORM 2
OFFICE AUTOMATION DPA RISK ASSESSMENT

1. FIRE

THREAT

The DPA may be at risk from fire if:

1. Combustible materials, such as paper, magnetic media, flammable plastics, etc., are present. The hazard from paper and magnetic media may be greater if they are placed on open shelves or stored in enclosures that are not fire-resistant than if they are stored in fire resistant enclosures.
2. It is located where there are defective electrical outlets and cables, hot appliances, or where there are open or smoldering flame sources, such as in areas where smoking is permitted;
3. The facility is undergoing construction;
4. The installation is located in proximity to clothing, textile, chemical, plastic, paint and petroleum processing or storage facilities, electrical appliance assembly, foundry, paper manufacturing or storage and warehouse operations;
5. The facility's structure is not fire resistant. In this respect, there are five construction grades:

   A. **Fire Resistive:** Framing, floors, walls and roof are constructed of noncombustible materials and insulated to protect against loss of strength as a result of fire;
   B. **Heavy Timber:** Exterior walls are non-combustible with a 2-hour rating and columns, beams, floors and roof are heavy timber, which is slow to burn;
   C. **Noncombustible:** While a fire in a non-combustible structure will not draw fuel from the structure itself, the heat from the fire may cause the structure to collapse;
   D. **Ordinary Construction:** The dimensions of the timber portions of the structure are too small to qualify as heavy timber; and
   E. **Wood Frame:** This typifies residential structures constructed of two inch thick framing and one inch boards. It provides the least resistance to fire.

Risk to the DPA from fire also depends on the extent to which the facility and equipment are protected by fire walls, fire-rated partitions, stairwells, dampers or shutters, on the extent to which low-flame-spread materials are used for floors, walls and furnishings, and on its own composition and proximity to flammable materials.

ESTIMATED RISK FROM FIRE: [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE
☐	SPRINKLERS	____/____/____
☐	HALON	____/____/____
☐	HAND HELD FIRE EXTINGUISHERS	____/____/____
☐	FIRE BELL	____/____/____
☐	SMOKE DETECTORS	____/____/____

PRESENT		PLANNED DATE
☐	FIRE ALARM	____/____/____
☐	NON-COMBUSTIBLE STRUCTURE	____/____/____
☐	WRITTEN EMERGENCY PLAN	____/____/____
☐	OTHER: (briefly describe: _____ _____ _____	____/____/____

2. UNSTABLE POWER SUPPLY

THREAT

The DPA may be at risk from fluctuations in or loss of electrical power if:

1. DC line voltage is 90% or less of nominal for more than four milliseconds, or 120% or more of nominal for more than 16 milliseconds. This could result in logic errors, erroneous data transfers or, in extreme cases, damage to hardware. Such transients may result from lightening strikes on exposed power distribution cables and switching equipment, from power company operations, and from power supply fluctuations within the facility; or
2. There are excessive demands on the power supply, or generating or transmission equipment failures. This could also result in loss of service and data.

ESTIMATED RISK FROM UNSTABLE POWER SUPPLY [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE	PRESENT		PLANNED DATE
☐	BACK UP POWER SUPPLY	____/____/____	☐	POWER SURGE PROTECTION	____/____/____
☐	NONVOLATILE MEMORY	____/____/____	☐	OTHER: (briefly describe: _____ _____ _____	____/____/____
☐	AUTO RESTART	____/____/____			

---

3. WATER

THREAT

The DPA may be at risk of damage from water if it is:

1. Located in a basement facility in a low lying area subject to flooding. Executive Order 11296, August 1966 requires federal agencies to evaluate flood hazards in planning for the use of these areas, and to implement flood-proofing measures where practical and economically feasible.
2. Subject to leaks from plumbing in risers, air conditioning units, and other water sources within the facility; or if it is
3. Connected to power sources or peripherals through cables subject to submersion under a raised floor;

Water from automatic sprinklers may also damage a DPA. However, damage caused by water from sprinklers is usually less than the damage that would otherwise result from a fire.

ESTIMATED RISK FROM WATER: [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE	PRESENT		PLANNED DATE
☐	COMPUTER LOCATED ABOVE GRADE	____/____/____	☐	WATERPROOF EQUIPMENT COVERS	____/____/____
☐	RAISED FLOOR	____/____/____	☐	CLOSED METAL FILES AND CABINETS	____/___/____
☐	PROTECTED CABLES AND CONNECTORS	____/____/____	☐	OTHER: (briefly describe: _____ _____ _____	____/____/____
☐	HUMIDITY RECORDING DEVICES OR INDICATORS	____/____/____			

FORM 2
OFFICE AUTOMATION DPA RISK ASSESSMENT

4. ELECTRICAL HAZARDS

THREAT

Equipment and applications may be damaged by electrical discharges if defective components, connectors, worn cables, human or environmental hazards can cause short circuits. Electrical hazards may include:

1. Unsound installation or maintenance procedures;
2. Spilling of beverages or other careless acts.
3. Damp cables or enclosures;
4. Conductive dust; or
5. Other conditions.

ESTIMATED RISK FROM ELECTRICAL HAZARDS: [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE	PRESENT		PLANNED DATE
☐	EQUIPMENT GROUNDED	____/____/____	☐	FIRE EXTINGUISHERS	____/____/____
☐	POWER OFF CONTROLS	____/____/____	☐	OTHER: (briefly describe: _____ _____ _____	____/____/____

---

5. LOSS OF DATA INTEGRITY

THREAT

The accuracy of data processed by the DPA may be degraded if:

1. A security policy does not control access to the DPA's equipment, applications and data to prevent malicious or accidental modification;
2. Operating controls, such as data entry verification procedures, do not minimize errors;
3. Files are not frequently backed-up;
3. Air conditioning does not adequately remove dirt, dust, smoke and other destructive particles and does not maintain humidity sufficient to prevent static charges from accumulating on furnishings and equipment; and
4. Static discharges from personnel are not inhibited.

ESTIMATED RISK OF LOSS OF DATA INTEGRITY: [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE	PRESENT		PLANNED DATE
☐	ENFORCEMENT OF SECURITY POLICY	____/____/____	☐	ANTISTATIC MEASURES (Chemical sprays, humidifiers, etc.	____/____/____
☐	IMPLEMENTATION OF OPERATING CONTROLS	____/____/____	☐	OTHER: (briefly describe: _____ _____ _____	____/____/____
☐	EFFECTIVE AIR CONDITIONING	____/____/____			

6. UNAUTHORIZED USE OR MISUSE

THREAT

The DPA may be at risk of damage from unauthorized use or misuse if it supports applications that employees or others may use for malicious purposes or personal gain, and if physical, administrative, hardware or software controls do not restrict and audit access to the system, applications or data.

Unauthorized use or misuse may involve direct access or access through interfaces. For example, DPAs that interface with public communications networks or which use public domain software may be exposed to virus attacks. Public domain software, and inadequate software development controls may also expose the DPA to Trojan horse, time or logic bomb attacks that could disrupt its operations.

ESTIMATED RISK OF UNAUTHORIZED USE OR MISUSE: [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE
☐	INDIVIDUAL IDENTIFIERS AND PASSWORDS REQUIRED FOR SYSTEM ACCESS	____/____/____
☐	INDIVIDUAL IDENTIFIERS AND PASSWORDS REQUIRED FOR APPLICATION AND FILE ACCESS	____/____/____
☐	ACCESS CONTROLS AND AUDIT LOGS PROTECT THE OPERATING SYSTEM AND ALL APPLICATIONS	____/____/____
☐	SOFTWARE INSPECTION AND VERIFICATION	____/____/____
☐	ACCESS ROSTERS	____/____/____
☐	INPUT/OUTPUT RECEIPT SYSTEM	____/____/____
☐	END-OF-DAY CHECKOUT PROCEDURES	____/____/____
☐	OTHER: (briefly describe: _____ _____ _____	____/____/____

7. PHYSICAL PENETRATION

THREAT

The DPA may be exposed to physical penetration resulting in damage to components and applications if potential adversaries have opportunities to access the facility where the DPA is located, the motive and capability for theft, malicious modification or destruction of equipment, applications and data, or unauthorized disclosure of information. Attempts at physical penetration may involve taking advantage of:

1. The condition and accessibility of the premises;
2. Poor surveillance and employee absences;
3. Inadequate maintenance and inventory controls;
4. Accidents or natural hazards;
5. Carelessness and errors; and
6. Other circumstances that provide opportunities.

ESTIMATED RISK OF PHYSICAL PENETRATION: [ ] HIGH [ ] MEDIUM [ ] LOW

SAFEGUARDS

Check the boxes for safeguards that currently protect this DPA. Provide the implementation date for planned safeguards.

PRESENT		PLANNED DATE
☐	CIPHER LOCKS, AND IMPLEMENTATION OF WRITTEN CONTROL PROCEDURES	____/____/____
☐	PERSONAL RECOGNITION ACCESS CONTROLS	____/____/____
☐	VISITOR LOGS AND ESCORT PROCEDURES	____/____/____
☐	INTRUSION-RESISTANT PARTITIONS, DOORS, WINDOWS, ETC.	____/____/____

PRESENT		PLANNED DATE
☐	SECURITY AWARENESS TRAINING	____/____/____
☐	KEY CONTROL PROCEDURES	____/____/____
☐	LOCKED EQUIPMENT COVERS AND CABINETS	____/____/____
☐	WRITTEN EMERGENCY SITUATION CONTROL PLANS AND PROCEDURES	____/____/____
☐	OTHER: (briefly describe: _____ _____ _____)	____/____/____

FORM 2
OFFICE AUTOMATION DPA RISK ASSESSMENT

8. EVALUATION

This section evaluates the risks and the safeguards reported in the previous seven items. It is intended to help you judge the adequacy of the DPA's security.

Follow the instructions below to calculate a score. This score combines the risk and safeguard ratings from the Office Automation DPA Risk Assessment with the cost and sensitivity information from the DPA Security Profile. The score is the **"Unprotected Risk"**, expressed as a percent. The higher this percent, the more the DPA needs additional protection.

First follow the instructions for steps 1 through 4 which explain how to use the table on this page. Then use the information from the table to do the calculations explained in the instructions for steps 5 through 10 on the following page. These calculations will result in the score for **Unprotected Risk** Then follow the instructions for steps 11 and 12. These instructions explain how to calculate a score for **Projected Risk**. Calculating this score will help you decide whether or not to recommend additional protection for the DPA.

Instructions

1. For each threat listed in the table on this page, check the column under Degree of Threat that represents the risk from the ratings reported in the Office Automation DPA Risk Assessment - (H)igh, (M)edium or (L)ow. Count the number of checks under each rating, and write the numbers in the totals row under each of the columns marked H, M and L

2. Count the number of safeguards reported for each threat. Write that number in the column titled **Current**. Do this for **Planned** safeguards as well.

3. Count the total number of current safeguards. Write this number in the **TOTAL** row and **Current** column. Divide this total by 48. Write the resulting percent to the left of the "%" sign. This is the percent of the safeguards identified in the seven risk assessment items that now protect the DPA. Also count the number of planned safeguards and write this number in the **TOTAL** row and **Planned** column.

	DEGREE OF THREAT			SAFEGUARDS	
				CURRENT	PLANNED
THREAT	**H**	**M**	**L**		
1. FIRE					
2. POWER SUPPLY					
3. WATER					
4. ELECTRICAL HAZARDS					
5. DATA INTEGRITY					
6. UNAUTHORIZED ACCESS					
7. PHYSICAL PENETRATION					
	H	**M**	**L**		
TOTAL:				/48 =	%

4. When you have completed steps 1 through 3, use the following formula to calculate the Total Threat. To do this, multiply the number of (H) by 3, the number of (M) by 2 and the number of (L) by one. Then add the results as follows:

$$\underline{\quad H \times 3 \quad} + \underline{\quad M \times 2 \quad} + \underline{\quad L \quad} = \underline{\quad \text{Total Threat} \quad}$$

FORM 2
OFFICE AUTOMATION DPA RISK ASSESSMENT

5. Next, subtract the percent of **Current** safeguards that you calculated in the table from 100 percent. This results in the percent of the total safeguards that are not currently protecting the DPA. Since the DPA is not protected by these safeguards, it is vulnerable. This percent represents the DPA's **Vulnerability**.

100% - _____% = _____%
safeguards vulnerability

Figure 4
RELATIVE COST

RANGE	RELATIVE COST
Less than $5K	1
$5K to 10K	2
$10K to 15K	3
$15K to 20K	4
$20K to 25K	5
$25K to 30K	6
OVER $30K	7

6. Use the table in Figure 4 to determine the **Relative Cost** of the DPA on a scale of 1 to 7. Look up the cost reported on Form 1, Item 9 on page 16, find its range and look across to the Relative Cost column. Write the number below, as indicated.

$_____ =
cost

_____
Relative Cost (on scale of 1 to 7)

7. Look up the highest sensitivity of the data processed by the DPA from Form 1, Item 10 on page 16 and find its **Sensitivity Score** below:

SENSITIVITY	SCORE
Classified:	[3]
Sensitive:	[2]
Non-Sensitive:	[1]

Sensitivity Score = [ ]

8. Multiply the **Total Threat** from Step 4 by the **Relative Cost** from Step 6 and the **Sensitivity Score** from Step 7 to get the **Total Risk**.

Item 4 x Item 6 x Item 7 = Total Risk

_____ x _____ x _____ = _____
Total Threat Relative Cost Sensitivity Total Risk

9. Next multiply the **Total Risk** that you calculated in Step 8 by the **Vulnerability** that you calculated in Step 5. The answer is the percent of the Total Risk that the DPA is not protected against. This is called the **Unprotected Risk**.

_____ x _____ = _____
Total Risk Vulnerability Unprotected Risk

Figure 5
UNPROTECTED RISK

A RANGE	B PERCENT
0 to 20	0%
20 to 40	5%
40 to 60	10%
60 to 80	15%
80 to 100	20%
100 to 120	25%
120 to 140	30%
140 to 160	35%
160 to 180	40%
180 to 200	45%
200 to 220	50%
220 to 240	55%
240 to 260	60%
260 to 280	65%
280 to 300	70%
300 to 320	75%
320 to 340	80%
340 to 360	85%
360 to 380	90%
380 to 400	95%
over 400	100%

10. Use the table in Figure 5 to convert the **Unprotected Risk** to a percent from 0% to 100% First find the range in Column A that the **Unprotected Risk** score falls within. Then look across to find the percent in Column B.

Unprotected Risk = _____

Percent = _____%

The higher the percent, the more the DPA is at risk from and vulnerable to the threats.

11. If the answer in Step 10 is greater than 50%, recalculate the **Vulnerability** (Step 5) using the sum of the **Current** and **Planned** safeguards (divided by 48) and recalculate the **Unprotected Risk** (Steps 9 and 10) to get the percent of **Projected Risk**.

FORM 2
OFFICE AUTOMATION DPA RISK ASSESSMENT

12. If the **Projected Risk** from step 11 is less than 50%, recommend adding the **Planned** safeguards in the Accreditation Request, Form 5 on page 37.

13. If the **Projected Risk** is greater than 50%, the DPA needs more safeguards than those already planned. In this case, evaluate the risk from each threat and the adequacy of the current safeguards and the planned safeguards reported in the Office Automation DPA Risk Assessment. Plan to add even more safeguards to protect the DPA against the threats from which the risk is high and for which the current safeguards and safeguards already planned are insufficient. Then recalculate the **Projected Risk**.

Repeat this process until the **Projected Risk** is less than 50%.

14. Recommend adding all of the originally planned and the additionally planned safeguards in the Accreditation Request, Form 5 on page 37.

5. LAVA

Use LAVA if you checked box D, F or G in Form 1, Item 2 on page 13. Include a LAVA Report in the Accreditation Report for these DPAs instead of Form 2.

Obtain the IBM-PC compatible LAVA software from the AISSM. It can be installed on personal computers using Intel 8088, 80286 and 80386 microprocessors. The software requires a minimum of two floppy disk drives or one hard and one floppy disk drive and 512 Kilobytes of memory. It does not require modification for use at different sites.

LAVA is a comprehensive method for assessing vulnerabilities and risks. If you are using LAVA, read the manual that comes with the software and follow its instructions. Also, distribute copies of this manual to all persons involved in the risk assessment.

A. RESULTS

The LAVA software contains algorithms that analyze the responses to 1,000 questions. From this analysis, the software produces a report on the DPA's exposure and vulnerability to threats, on the potential consequences of its exposure and vulnerability, and on the adequacy of its safeguards.

THREATS

Both natural and human hazards may threaten a DPA. LAVA calculates the extent to which the DPA is exposed to these threats by scoring responses to questions on its location, construction and condition and on adversaries' motives, capabilities and opportunities.

VULNERABILITIES

LAVA scores the effectiveness of the protection provided to the DPA by its current safeguards in terms of vulnerability scores. A higher score indicates greater vulnerability.

CONSEQUENCES

LAVA assesses the potential consequences of a DPA's exposure and vulnerability to threats by comparing the extent of exposure to its vulnerability and to the value of its assets. Potential consequences are greater if valuable assets are exposed to threats to which the DPA is vulnerable.

LAVA also estimates potential monetary and non-monetary losses from:

1. legal action, lost time, and interim operation;
2. repair, recovery, and hardware and software replacement;
3. employee replacement and training;
4. damage and destruction, waste, fraud and embezzlement;
5. adverse public reaction, embarrassment, and potential degradation of reputation;
6. organizational disruption;
7. employee discouragement and poor morale; and the
8 intangible cost associated with unsafe or restrictive working conditions.

LAVA analyzes these losses to suggest safeguards that would reduce the potential costs from exposure to the threats.

B. USING THE LAVA REPORT

LAVA produces a printed report on the extent to which the DPA is vulnerable to and at risk from threats, and on potential consequences of its vulnerability to those threats. The report also suggests additional safeguards to reduce the DPA's vulnerability.

Use these results, to determine if additional safeguards are needed to protect the DPA. If additional safeguards are needed, recommend them in the Accreditation Request, Form 5 on page 37.

6. CONTINGENCY PLAN

Contingency plans provide documentation used to assure "reasonable continuity of data processing support should events occur that prevent normal operations of the DPA." (OMB Circular A-130).

FAA Order 1600.54B requires contingency plans "for all DPAs which house computer equipment used to support FAA operational or administrative missions for which unplanned disruption of service would have a critical impact on mission accomplishment. If unplanned disruption of services would not have a critical impact on mission accomplishment, the AISSM shall inform the regional AISSC, and no contingency plan is required." (FAA Order 1600.54B; 201).

If you are required to prepare a contingency plan, refer to Order 1600.54B, Chapter 10, page 201 through 210. Additional information is provided in Appendix 4 of Order 1600.54B. Appendix 4 reviews the contents of Contingency Plans for Air Route Traffic Control Centers (ARTCC). FIPS PUB No. 87, Guidelines for ADP Contingency Planning also provides instructions for developing contingency plans.

If a contingency plan is not required for the DPA, include a waiver, Form 3, on page 31 in the Accreditation Report.

FORM 3
CONTINGENCY PLAN WAIVER

Memorandum

Date:_____/_____/_____/ Reply to Attn of:

Subject: Contingency Plan Requirement:

_____
(Title of DPA)

From:_____
(AISSM)

To: _____
(AISSC)

I have reviewed the services provided by the subject Data Processing Activity (DPA).

Unplanned disruption of these services would not have a critical impact on accomplishment of the FAA operational or administrative missions. Therefore, a contingency plan for this DPA is not required for its accreditation.

#

7. SENSITIVE APPLICATION SECURITY CERTIFICATION STATEMENTS

An application is a computer program and data developed as a system to perform a particular function. It may be used on one or more connected or unconnected AIS. The application is sensitive if its misuse could adversely affect the FAA's ability to accomplish its mission. Examples are the Advanced Automation System (AAS), Remote Maintenance Monitoring System (RMMS), Voice Switching and Control System (VSCS), Health Information Subsystem (HIS), Substance Abuse Information Subsystem (SAIS), and Aircraft Registration System (ARS).

Certification of sensitive applications is required for accreditation of the DPAs upon which the software and data for the applications reside.

Obtain a copy of the Security Certification Statement for every sensitive application that resides on the DPA. Get these Statements from the office responsible for development or distribution of the application or from application managers. Contact the AISSC to identify these offices. Insert copies of the Certification Statements for each sensitive application that resides on your DPA at this point in the Accreditation Report.

Two conditions under which you are not required to include sensitive application certification statements are:

1. Your DPA does not host any sensitive applications. You do not need certification statements for sensitive applications that are remotely accessed from the DPA as long as the software and data for those applications reside elsewhere. Computer programs such as word processors, spread sheets and data-base management programs, and files that these programs access are not by themselves applications and do not require sensitive application certification.
2. Access to sensitive applications that reside on the DPA is restricted solely to users within the facility, office, service, division or branch that comprises the DPI; those users have the background investigations or

security clearances required for access to that information; there is no capability for remote access to the DPA; and there are no copies of the applications on any other DPAs.

If either of these conditions apply, complete the Sensitive Application Security Certification Waiver, Form 4 on page 34.

A Provisional Accreditation may be granted at the DAA's discretion if the required certification statements are not available. The instructions for completing the Accreditation Request, Form 5, on page 37, include directions for requesting provisional accreditation.

8. SUMMARY

The AISSO prepares a narrative summary of the Accreditation Report that describes the DPA's security and recommends an accreditation action. In this summary, review:

1. The DPA's configuration, purpose and organizational context;
2. The sensitivity level of the DPA's applications and data;
3. The importance of the DPA for the FAA's mission;
4. Major risks and vulnerabilities revealed by the risk assessment;
5. Deficiencies that the results of the risk assessment indicate should be remedied;
6. Your recommendations for additional safeguards as a result of the evaluation in Item 8 of the Office Automation DPA Risk Assessment, Form 2 on page 25 of these guidelines, or the LAVA report; and
7. Possible operational restrictions for conditional accreditation of the DPA.

9. ACCREDITATION REQUEST

Complete Form 5 on page 37 to request an accreditation action. Base your recommendation on the extent to which the DPA is adequately protected. Attach an explanation if a contingency plan and sensitive application certification statements are

FORM 4
SENSITIVE APPLICATION
SECURITY CERTIFICATION WAIVER

Memorandum

Date:_____/_____/_____/ Reply to Attn of:

Subject: Sensitive Application Security Certification: (Title of DPA)

From:_____
(AISSM)

To: _____
(DISTRIBUTION)

Review of the applications hosted by the subject Data Processing Activity (DPA) suggests that Security Certification Statements for Sensitive Applications are not required for its accreditation, because (check one):

[ ] The subject DPA does not host sensitive applications as defined by the criteria for Level II data in the FAA Security Program, Order 1600.54B, paragraph 15.

[ ] The following sensitive applications are hosted by the subject DPA but access to these applications and to the data that they process is restricted to operators of only this single DPA or, if more than one DPA, to operators within only one DPI.

(List Sensitive Applications)

_____

_____

_____

_____

required for this DPA but are not included in the Accreditation Report. Also propose dates for providing these materials and request provisional accreditation.

Include Form 5 in the Accreditation Report. It must be signed by the AISSO and the AISSM. If the DPA hosts classified (Level I) or sensitive (Level II) applications, the AISSC must also sign a concurrence statement on this form.

Also complete the Accreditation Statement, Form 6 on page 38, except for the signature. Include it in the Accreditation Report.

TRANSMITTAL

You have now completed all of the documentation required for accreditation of this DPA. Remove the Forms from the guidelines and prepare a Table of Contents, as instructed on page 10. Assemble and bind all of the completed forms and other materials required to make up the Accreditation Report. Make sure you include:

1. The Title Page;
2. The Table of Contents;
3. Form 1: DPA Security Profile;
4. Form 2: Office Automation DPA Risk Assessment; include a LAVA report instead of Form 2 if you used LAVA;
5. a Contingency Plan or Form 3: Contingency Plan Waiver;
6. Sensitive Application Security Certification Statements or Form 4: Sensitive Application Security Certification Waiver;
7. The Summary;
8. Form 5: Accreditation Request; and
9. Form 6: Accreditation Statement.

Send the complete report to the AISSM.

ACCREDITATION ACTION

Official accreditation occurs when the Accreditation Statement in the Accreditation Report is signed by the DAA.

The AISSM is the DAA who signs the Accreditation Statement if the DPA is non-sensitive (Level III). For these DPAs, the

AISSM retains the Accreditation Report, including the signed Accreditation Statement, and sends a copy of the entire report to the AISSC.

The AISSM does not sign the Accreditation Statement for a Level I or Level II DPA, because he or she is not the DAA for these DPAs. Instead, the AISSM sends the entire Accreditation Report for Level I and II DPAs to the AISSC. The AISSC signs the concurrence with the Accreditation Request, Form 5, and sends the entire Accreditation Report to the DAA. The DAA signs the Accreditation Statement.

FORM 5

ACCREDITATION REQUEST

Having complied with the requirements for documenting its sensitivity and value, assessing risks and vulnerabilities, identifying safeguards, and preparing a contingency plan, I recommend granting this DPA (Check one):

[ ] Provisional Accreditation with Approval to Operate pending submission of Sensitive Application Certification Statements.

[ ] Accreditation with Approval to Operate.

[ ] Accreditation with Approval to Operate under the condition that the following additional safeguards be planned or restrictions enforced:

_____

_____

_____

_____

[ ] Other than Approval to Operate (Explain):

_____

_____

_____

AISSO: _____
Signature Date

==========

CONCURRENCE

Based on review of documentation prepared for accreditation of this DPA, I (check one):

[ ] concur with the recommendation.

[ ] do not concur.

Exceptions (if none, so state):

_____

_____

_____

AISSM: _____
Signature Date

I (check one): [ ] concur with the recommendation.

[ ] do not concur.

Exceptions (if none, so state):

_____

_____

_____

AISSC: _____
Signature Date

FORM 6

ACCREDITATION STATEMENT

I HAVE EXAMINED THE MATERIALS SUBMITTED TO SUPPORT SECURITY ACCREDITATION OF:

_____ IN THE
(TITLE OF DPA)

_____
(TITLE OF DPI - SERVICE, DIVISION, BRANCH, ETC)

LOCATED AT: _____
(ADDRESS)

BASED ON THIS EXAMINATION, I AUTHORIZE THIS SYSTEM TO PROCESS INFORMATION RATED:

[ ] LEVEL I - CLASSIFIED
[ ] LEVEL II - SENSITIVE
[ ] LEVEL III - NON SENSITIVE

SUBJECT TO THE FOLLOWING CONDITIONS:

_____
(SIGNATURE) (DATE)

_____
(TITLE)

APPENDIX

This appendix briefly summarizes accreditation responsibilities of the AISSM, AISSC and DAA established in FAA Order 1600.54B.

AISSM

The position of AISSM is established at the service, office, division staff or branch level, with one AISSM for each Data Processing Installation (DPI). In addition to supervising the preparation of Accreditation Reports by AISSOs, the AISSMs are the DAAs for all DPAs processing unclassified, non-sensitive (Level III) data in their Services or Branches.

Appendix Figure 1
DRAFT ACCREDITATION TRANSMITTAL MEMORANDUM

Memorandum

Date:____/____/____/Reply to Attn of:

Subject: Accreditation:: (Title of DPA)

From: _____
(AISSC)

To: _____
(DAA)

The enclosed Accreditation Report for the subject Data Processing Activity (DPA) is submitted for your consideration.

This DPA contains (classified or sensitive) information as defined by the FAA Security Program, Order 1600.54B, paragraph 15. and is critical for accomplishment of the Federal Aviation Administration's mission.

Your unconditional or conditional approval of the security of the subject system, through signature of the Accreditation Statement included in the Report, is required for its continued operation.

The Accreditation Report includes documents to inform your decision. These documents:

1. profile the DPA's configuration, the sensitivity of its applications, its use and value;
2. describe risks to the system and its vulnerabilities;
3. assess the adequacy of safeguards that currently protect it;
4. describe contingency actions planned to maintain or replace its operations in the event of disasters and disruptions;
5. certify the security of its sensitive applications; and
6. recommend an accreditation action.

The findings presented in these documents have been reviewed by (names and titles of AISSO, AISSM, AISSC and other officials if appropriate). These officials have concurred with the following recommendation for your accreditation action and signature of the Accreditation Statement drafted on page (No.) of the attached report.

(Summary of Recommendation)

AISSC

Order 1600.54B establishes the position of AISSC for coordination of AIS security tasks in each Center and Region. The accreditation responsibilities of this position include assisting and coordinating the efforts of the AISSMs. The AISSC also reviews the documentation in the Accreditation Report, and

conveys the accreditation request to the DAA through the security manager. A draft transmittal memorandum is provided in Figure 1.

THE DAA

The DAA signs accreditation statements. These grant conditional or unconditional permission for DPAs to operate. By signing an accreditation statement, the DAA "either concurs, declaring that a satisfactory level of operational security is present or does not concur, indicating that the level of risk either has not been adequately defined or has not been reduced to an acceptable level for operational requirements." (FAA Order 1600.54B; 263).

The DAA's accreditation action is informed by the AISSO's recommendations, on the basis of the documentation presented in the Accreditation Report. While accreditation requires a complete report, the DAA may provisionally accredit a DPA pending action to obtain sensitive application certification statements.

The logical options for permission to operate a DPA are based on the adequacy of its protection. These options are summarized in Figure 2 on page iii. The first cell in this figure represents full, or Unconditional, Accreditation with no operational restrictions or requirements for additional safeguards. Cell 2 represents Conditional Accreditation. This involves granting permission for the DPA to operate and requiring actions to remedy deficiencies so it is sufficiently protected against threats to which it is exposed. Cell 3 represents denial of accreditation, with Unconditional Suspension. This extreme action might be taken if deficiencies cannot be remedied, and if operational restrictions are not practical. Conditional Suspension, represented by Cell 4, would involve temporary suspension of some or all operations, pending the implementation of additional safeguards.

If the DAA conditionally accredits the DPA's security, not granting its operations full approval, operational restrictions, additional safeguards or other remedial measures should be specified.

If the DAA disapproves of the security provided for the DPA, accreditation may be denied, with suspension of operations pending remedial action. Although, in cases of severe security deficiencies, accreditation could be denied to DPAs that process classified or sensitive data critical to accomplishment of the FAA's mission, permanent suspension of their operations would be a highly improbable action.

Appendix Figure 2
ACCREDITATION OPTIONS

REMEDY	APPROVAL TO OPERATE: GRANTED	APPROVAL TO OPERATE: DENIED
UNSPECIFIED	1 UNCONDITIONAL ACCREDITATION	3 UNCONDITIONAL SUSPENSION
SPECIFIED	2 CONDITIONAL ACCREDITATION	4 CONDITIONAL SUSPENSION

4. Specific remedial actions may involve:

1. Addition, replacement or deletion of security safeguards;
2. Operational restrictions;
3. Modification of the contingency plan;
4. Alterations in the facility; or
5. Other measures indicated as a result of the risk and vulnerability assessment of the DPA.

Decisions to invest in safeguards or other remedies should be based on comparison of their costs to anticipated losses. Protection should not cost more than the losses it would prevent.

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4378

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
AUGUST 1990

4. TITLE AND SUBTITLE
Automated Information System Security Accreditation Guidelines

5. AUTHOR(S)
Federal Aviation Administration

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)
Reprinted by permission of the Federal Aviation Administration, Office of Civil Aviation Security, 800 Independence Avenue, SW, Washington, DC 20591.

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Federal Aviation Administration's publication, Automated Information System Security Accreditation Guidelines, provides procedures for the preparation of documentation required for security accreditation of automated information systems. It has been designed to make the accreditation process as straightforward as possible for any system, whatever its purpose or level of complexity. The accreditation process requires the identification of the data processing activities in the data processing installation and the completion of the forms in this guideline to develop a security profile of the system, conduct a risk assessment and document contingency plans. A Designated Approving Authority then signs the accreditation statements that formally accept the risks to each data processing activity.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)
accreditation; ADP security; automated information system security; certification; computer security; contingency plan; risk assessment

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
48

15. PRICE
A03

ELECTRONIC FORM