c. Department of Energy

(1) DOE Order 1360.2, ''Computer Security Program for Unclassified Computer Systems.''
(2) DOE Order 5636.2, ''Security Requirements for Classified Automatic Data Processing Systems.''
(3) DOE Manual 5636.2, ''Computer Security Guidelines for Classified Automatic Data Processing Systems.''

d. Department of Health and Human Services

(1) Part 6, ''ADP Systems Security,'' Chapter 6-00, HHS ADP Systems Manual.

e. Department of Housing and Urban Development

(1) ''HUD ADP Security Policy Handbook.''

f. Department of the Interior

(1) 306 DM 7, Departmental Management Part 306 (Automatic Data Processing), Chapter 7 (ADP Security Program).
(2) ''ADP Standards Handbook'' (306 DM), Chapter 2 (ADP Security Program).

g. Department of Justice

(1) DOJ Order 2640.2, ''Automatic Data Processing (ADP) Security.''

h. Department of Transportation

(1) DOT Order 1640.7, ''Department of Transportation Automatic Data Processing Security Policy.''
(2) DOT Order 1640.8, ''Department of Transportation Automatic Data Processing Security'' (DOT ADP Security Handbook).

i. Department of the Treasury

(1) DOT Order 102-3, ''Personnel, Physical and Automatic Data Processing (ADP) Systems Security—Organization and Delegation of Authority.''
(2) Treasury Directive 10-08, Part VII, ''ADP Resource Protection.''
(3) Treasury Directive 10-08, Part VII, ''ADP Privacy Act Guidelines.''
(4) Treasury Directive 10-08, Part VII, (DRAFT) ''ADP Resource Protection Guidelines.''

j. Federal Aviation Administration

(1) ''Security Certification Guidelines for the Federal Aviation Administration's Uniform Payroll System.''

k. National Aeronautics and Space Administration

(1) NASA Management Instruction 2410.7, ''Assuring Security and Integrity of NASA Data Processing.''

1. Nuclear Regulatory Commission

(1) Part XII, ''Security of Automatic Data Processing Systems,'' Appendix to NRC Manual Chapter 2101, ''NRC Security Program.''
(2) Part XVII, ''Automated Information Systems Security Program for Sensitive Data,'' Appendix to NRC Manual Chapter 2101.

APPENDIX C

ILLUSTRATIVE SENSITIVITY CATEGORIES FOR APPLICATIONS

There are many different points of view on whether and how to categorize applications by sensitivity. Some prefer to avoid categorization, noting that all applications have some degree of sensitivity and that sensitivity is a complex, multifaceted attribute that does not lend itself to representation by simple categories. Others stress that an imperfect categorization is better than none at all. In using this Guideline, the important point is that there be agreement within the agency on which applications require certification and accreditation.

For those who prefer to establish sensitivity categories, two sample categorizations are presented here. Note that these are sensitivity categorizations for applications, not for information or personnel clearances. There is typically a correlation between these, but it cannot be assumed that a highly sensitive application contains highly sensitive information or requires highly cleared people. For example, applications might be sensitive due to loss or harm that could result from operational failure (denial of service), rather than from unauthorized disclosure or manipulation of sensitive data. A sensitive application might not require cleared people if effective separation of duties removes the need for highly trusted positions.

Both categorizations are from DoD, although they might be adapted for use by non-DoD agencies. Note, for example, the GAO statement that "each executive agency head's responsibility for ensuring security of all agency information also includes information classified for purposes of national security" [GA082-1, p. 11].

The first categorization (Figure C-1) is from Army Regulation 380-380 [USA380] and has official status. The second (Figure C-2) is an unofficial categorization adapted with minor changes from [EPP80, pp. J-14, J-15]. This Guideline recommends neither approach over the other, but simply presents them for use.

A. CRITICALLY SENSITIVE (CS). A DPA which processes classified defense information or applications involving large dollar volumes of asset/resource accounting or authorization data ($10 million per annum or higher). There are four levels of critically sensitive DPA (in descending order of sensitivity):

1. Level 1 (CS1)—A DPA that processes any amount of compartmented national intelligence information or SIOP-ESI.
2. Level 2 (CS2)—A DPA that processes Top Secret information.
3. Level 3 (CS3)—A DPA that processes Secret information.
4. Level 4 (CS4)—A DPA that processes Confidential information or large dollar volumes of asset/resource accounting or authorization data.

B. HIGHLY SENSITIVE (HS). A DPA, not specifically included in A. above, which processes information requiring protection under the provisions of the Privacy Act of 1974 and/or asset/resource accounting or authorization data of moderate dollar value ($1,000,000—$10,000,000).

C. SENSITIVE. A DPA, not specifically inlcuded in A. or B. above, which processes information relating to asset/resource, proprietary or contractual information.

D. NONSENSITIVE. A DPA, not specifically included in A., B., or C. above.

Figure C-1. *Sensitivity categories for Army data processing activities (DPA)*[1]

[1] Taken from [USA380].

CRITICAL SENSITIVE. Applications shall be categorized as critical sensitive when one or more of the following criteria are met.

1. *Top Secret National Security Information.* Protection is required in the interest of national security, and the highest involved information classification designation is Top Secret.

2. *Mission Critical for Agency.* Denial of use or disablement of the application or loss, compromise, or unauthorized alteration of the data contained therein could reasonably be expected to directly and gravely degrade or jeopardize the capabilities of an agency as a whole to timely and effectively discharge its primary functions.

3. *Life Critical.* Denial of use or disablement of the application or loss, compromise, or unauthorized alteration of the data contained therein could reasonably be expected to directly and gravely jeopardize human life.

4. *Automated Decision-making Systems.* Applications, not otherwise included in the foregoing, that issue checks, requisition supplies, or perform similar asset control functions, based on programmed criteria with little human intervention, wherein the potential loss or exploitable monetary value of the assets handled could exceed $10,000,000 per year.

NONCRITICAL SENSITIVE. Applications that do not meet any of the foregoing criteria for critical sensitive shall be categorized as noncritical sensitive when one or more of the following criteria are met.

1. *Secret or Confidential National Security Information.* Protection is required in the interest of national security, and the highest involved information classification designation is either Secret or Confidential.

2. *Mission Critical for Staff Element.* Denial of use or disablement of the application or loss, compromise, or unauthorized alteration of the data contained therein could reasonably be expected to degrade or jeopardize component or major staff element capabilities to support timely and effective discharge of agency missions and functions.

3. *Privacy.* The application includes personal information requiring protection pursuant to the Privacy Act of 1974.

4. *FOIA Exemptions.* The application has been determined to be exempt from public disclosure, consistent with the requirements of the Freedom of Information Act (FOIA).

5. *Automated Decision-making Systems.* Applications, not otherwise included in the foregoing, that issue checks, requisition supplies, or perform similar asset control functions, based on programmed criteria with little human intervention, wherein the potential loss or exploitable monetary value of the assets handled could range between $1,000,000 and $10,000,000 per year.

NONSENSITIVE. All other applications that do not meet the criteria for the critical sensitive or noncritical sensitive categories as set forth above.

Figure C-2. *Illustrative sensitivity categories for applications*[1]

The two categorizations differ primarily in (1) the number of levels and sub-levels involved, (2) the treatment of classified information, and (3) the lack of explicit treatment of mission criticality in [USA380]. An area of similarity between the two is the use of the term "nonsensitive" for the lowest level. This has been criticized as implying "not sensitive" and thus susceptible to interpretation as "not needed." The Department of Commerce has defined labels for levels of record protection that avoid this problem [DoCRP1]:

1. Vital Sensitive

2. Important Sensitive

3. Useful Nonsensitive

[1] Adapted from [EPP80].

APPENDIX D

DOCUMENT REVIEW GUIDE

Purpose Code	Area/Title
	ADMINISTRATIVE
R	Organization Charts
R	Phone Book
R, C	Position Descriptions
	OPERATIONAL
R, C	Application Run Book
R, C	Application Flow Chart
R	Violation Reports
R, C	Audit Journals
R, C	Audit or Evaluation Findings
R	Problem Reports
R	Operational Statistics
R	Billing Data
R, C	Application-Specific Documents (e.g., inputs and outputs)
	REQUIREMENTS
C	Project Request
R	Feasibility Study
R	Risk Analysis
R	Cost-Benefit Analysis
C	Functional Requirements Document
R	Data Requirements Document
R	Requirements Traceability Matrix (used in DoD to correlate requirements with implementation features and tests)
	PLANS
R	Project Management Plan
C	Contingency Plan
C	Software Development/Conversion Plan
C	Security Development Plan
C	Configuration Management Plan
C	General Test Plan
R	System Integration Plan
R	Maintenance Plan
R	Data Base Management Plan
R	Integrated Logistic Support Plan
R	System Engineering Facilities Plan
	SPECIFICATIONS
C, R	System/Subsystem Specifications
C, R	Program Specifications
C, R	Data Base Specifications
C, R	Interface Specifications
C, R	Formal Specifications
R	Engineering Drawings
R, C	Human Engineering Design Approach Document
R	Engineering Change Proposals and Requests for Deviations/Waivers; Specification Change Notices
C, R	Source Listings
R	Equipment Lists
R	Floor Plan

Purpose Code	Area/Title
	MANUALS
C, R	Users Manual
C, R	System Security Manual
C, R	Computer Operators Manual
R, C	Program Maintenance Manual
R	System Manuals
	TECHNICAL ANALYSIS DOCUMENTS
R	Security Evaluation Reports (from prior certifications)
R	Risk Analysis
C	Test Procedures
C	Test Analysis Reports
R, C	Security Analysis Reports
C	Formal Verification Reports
R	Design Analysis Reports
R	Failure Mode and Effect Analysis Report
R	Reliability and Maintainability Analysis Report

KEY: C= Critical Review. Analyze for security deficiencies, whether technical, procedural, or organizational.

R= Research and Reference Review. Review to understand application functionality and characteristics or reported shortcomings in order to better perform critical reviews; use for reference purposes.

The role listed first is the highest priority role.

APPENDIX E

USDA PROCEDURE: INTERNAL CONTROL & SECURITY EVALUATION INTERVIEWS[1]

E.1 Introduction

The objective of an evaluation is for reviewers to examine an entity for the purpose of rendering an informed opinion of its state. Evaluating internal controls and computer systems security requires the talents of a number of different disciplines. Because evaluations are rare occurrences, it is not usually practical to retain a permanent staff of highly specialized technicians who only perform these reviews. A compromise is sought whereby a small number of full-time reviewers is retained (possessing the specialties most commonly used) while at the same time infrequently used technicians are matrixed into the review group as necessary. Using this approach has definite advantages: it reduces costs, exposes personnel to a wide variety of projects, and adds credibility to the reviews. On the other hand, there are also some disadvantages, the most important of which is the fact that the use of part-time reviewers requires a continuing education effort. It is certainly reasonable to expect part-time reviewers to know their specialty thoroughly, but not at all reasonable to expect them to fully understand review techniques and procedures. The purpose of this procedure, therefore, is to provide guidance to part-time reviewers in conducting interviews. Because the individual talents and skills of reviewers may vary, portions of the following material may seem obvious to some. However, to be as comprehensive as possible, such material was included.

To understand the interview process requires an understanding of the overall review process. For simplicity, it can be divided into discrete phases, each with its own duties and responsibilities. Reviewers become involved in the review during the preliminary arrangement phase and participate through the preparation of the final report.The reviewer's objective is to render an informed opinion in the final report; the objective of the information gathering phase is a means to achieve this end. Obviously, then, the information gathering phase, especially the interview portion of it, is crucial to a successful evaluation.

E.2 General Background Information

Reviewers must recognize several facts that tend to make their interviewing somewhat difficult. First, the review team is an official body, an extension of upper management. As such, it is viewed by project personnel (both agency technical area specialists and data processing personnel) with some degree of apprehension. Their current positions, past accomplishments, and perhaps even future careers may depend directly upon the project. They may not perceive the review as being in their own best interest or good for the project itself. In rare cases, project personnel may expect only negative results from an evaluation, with no positive benefit possible. Second, a variety of project personnel will be interviewed, representing a mixture of job types. As a result, reviewers will interview persons of differing levels of skills, job understanding, and intelligence. Finally, the interview itself is a form of interpersonal communication subject to the usual problems of misunderstanding between both parties.

The above factors combine in unexpected ways to complicate the job of the reviewer. It is not uncommon, for example, to interview persons who feel threatened by the evaluation, and therefore do not wish to communicate any information to ''outsiders.'' Also, it is possible to interview persons who do not yet fully understand the project or their relation to it. On the other hand, it is entirely possible that the person being interviewed possesses the information desired, is willing and able to communicate it, but is misunderstood by the reviewer himself.

Thus, the seemingly simple interview process is, in reality, highly complex and subject to erroneous information gathering. Reviewers must always keep this in mind, and constantly strive

[1] This Appendix is taken from the certification program of the U.S. Department of Agriculture.

to obtain accurate, truthful, and relevant information about the project. To aid the process, a number of aspects relevant to interviewing are noted below.

1. **Formality**—The degree of formality varies with the position of the individual being interviewed. Generally with the higher levels of project management a more formal approach is used then with the lower levels of technical or clerical personnel. At the higher levels, formality is almost expected, but at the lower levels it may only introduce artificial barriers, hampering the free flow of information.

2. **Appointments**—In many situations project management is under time constraints that may cause conflicts with interviews. In these cases, it is advisable to arrange appointments to allow ample time to complete the entire interview without interruption. At lower levels of the project, this is usually unnecessary; it is not unreasonable for a reviewer to interview some project personnel in an impromptu manner.

3. **Personnel Selection**—There are two ways to determine who to interview: project management can choose those persons it feels can best portray an appropriate image of the project, or the review team can make its own choices. To rely solely on either method may skew the information collected, a combination of the two is far superior and produces a more balanced result.

4. **Interview Location**—The location of the interview has a direct impact upon the information gathered. It is preferable to have an assigned office borrowed from the project to conduct most of the interviews. This has several advantages—the person interviewed is more likely to be candid in a private office, reviewers do not waste time searching for the offices of others, and it is easier to control review material if it is kept in one place. However, not all interviews can take place in a fixed location; interviews of project management usually take place in their own offices.

5. **Number of Interviewers**—There is no ''proper'' number of reviewers to be present during an interview; individual conditions should dictate the actual number. For interviews of project management, any number seems permissible because management can be expected to be able to address a crowd, if necessary. Other members of the project team, however, may feel intimidated by the presence of too many reviewers. In these cases, at least two reviewers are recommended to help prevent communications misunderstandings between reviewers and project personnel.

6. **Project Liaison**—If the size of the project warrants, the review team should request that the project manager assign a person to act as a liaison to the review team. This greatly aids reviewers by eliminating the necessity of locating persons to interview and explaining the review process to them. Furthermore, when security walk throughs are used, it is advisable to have a project member along to assure project personnel that the review team has the authority to investigate all aspects of the project.

7. **Interview Termination**—Interviews should be terminated when all information desired is obtained (the questionnaire completed) or when it becomes obvious that the information being gathered does not justify the time being spent to acquire it (that is, the person being interviewed is either unwilling or unable to provide information.)

8. **Number of Interviews**—The number of interviews necessary to gather enough information to write the evaluation report varies from one project to another. Usually, all major operations should be investigated,—with several interviews in each functional area. However, if repeated responses to questions fail to uncover any deficiencies, the number of interviews can be reduced in that area and the time spent investigating other areas.

9. **Project Objective**—The objective of the review is to investigate and report on the project being evaluated. This is not the objective of the project itself. At times these two objectives may conflict. In such cases the daily operations of the project must take precedence over the review. Ideally, the review team should perform its function with as little disruption as possible to the project's operation and personnel.

E.3 Specific Aspects of the Interview

After all preparations have been made (background material studied, management briefing attended, appointments made, and familiarity with the questionnaire achieved) interviews can begin. From prior information gathering, a general impression of the project should already be forming. An opinion of the adequacy of the project may also be forming, but reviewers must guard against premature judgments that are unsupported by facts. Thorough study of all information may indicate several areas of concern that could be investigated more fully during interviews or by direct observation. Preparation is the key to successful evaluating; reviewers should strive to conduct interviews where they already know the answers to some of the questions asked. In this manner they can verify the information previously gathered, whether in other interviews, observations, or project documentation. The following points may expedite the interview.

Always remember that the person being interviewed may be nervous. After making initial contact try to put him at ease—introduce yourself and be sure to correctly note his name, use it often during the interview. Do not engage in trivial conversation, but do not jump immediately into minute details, either. Take the time to explain why both parties are meeting: 1) outside reviewers add objectivity and expertise to the review, 2) the agency can provide firsthand information about the status of the project. Use the first few moments to get them to talk about their job and their place in the overall project. Maintain good eye contact. If appropriate, encourage them to speak candidly by telling them that the information given will remain anonymous, not revealed to their supervisors. Try to allay any fears that the review is on a "fishing expedition," looking for only negative aspects. Explain that you will be taking notes only to ensure that the report is accurate, but do not use any type of recording device. Pay close attention to what is said, mentally sort the information to verify previously collected information and to use it to verify subsequent information. Take copious notes; all material may be needed to help compile the final report, which could be written a considerable length of time after the interview is held.

Begin filling out the questionnaire by first obtaining identification information such as the full name, title, office number and telephone number. Also, determine the length of time the individual has been in the present position in addition to previous assignments. These two seemingly unimportant facts can greatly aid the reviewer in deciding how much credence to place upon the responses. For example, if the individual has been in this present position for several years, a firm understanding of the job can be expected, with a reasonable basis for personal opinions. However, if the individual is relatively new to the position, the information given could be of little value because it may be incorrect. In such cases, it is useful to inquire about previous positions, but only if they were also with the project currently being evaluated. If so, it may be better to discuss the previous position; if not, the interview should be terminated because it serves little purpose to interview a person who has not yet settled into a new job.

Be sure to ascertain exactly where in the project the individual fits—use an organization chart, if necessary. It may be useful to obtain position descriptions prior to holding interviews so that the person's actual duties can be compared to those for which they are officially held responsible. Ask for a short explanation of duties, and note each major functional area that can be explored more fully later in the interview, but try not to interrupt this portion of the response. Determine from the duties mentioned where in the questionnaire to start asking questions—it is not unusual to skip entire sections because the individual has no working knowledge of certain areas. Do not try to rush; if additional time is needed to arrange papers to find the proper section, take it. Always retain control of the interview, and above all do not allow the individual to lead the conversation into areas of little or no interest to the evaluation.

Each time a question is asked the reviewer should follow a set procedure. Read or paraphrase the question. Explain it if the person questions some part or if the individual appears puzzled. Then stop talking and listen to the answer. Listening is the most important part of the interview; it is the reason for the interview. Oddly enough, many reviewers tend to be better talkers than listeners. Make a concerted effort to listen. If possible, do not interrupt the answer until it is complete; then if some point is unclear try to clarify it. Record the answer, either on the questionnaire, or on a note pad. Mentally verify it against previous information and remember it to verify subsequent information against it.

If any answer is unusual, unexpected, or differs from previous information, special action may be necessary. First, the importance of the discrepancy must be evaluated. If minor it can be ignored and the interview resumed without discontinuity. If a substantive disparity exists, it is a sign that problems may exist. Deviate from the questionnaire to probe into the subject as necessary—do not proceed to another topic until you are satisfied that you thoroughly understand the subject or at least the reason for the discrepancy. If unable to obtain enough information, make a note to investigate the subject in detail elsewhere. If the seriousness of the incident dictates, inform other members of the review team to be alert for further information to confirm your findings.

During interviews observe the individuals closely. If they become uncomfortable, fidget, or show signs of being excessively nervous, suspect that you are talking about a subject that, for some reason, they would rather avoid. Be extremely careful in situations such as these. There may be valid reasons for some individuals not wanting to discuss certain subjects. Decide if the subject is germane to the review—if not drop it and proceed to more important issues. If it is germane to the review, probe tactfully, with discretion. Remember that your function is not to unduly pressure project personnel. If this particular individual is reluctant to discuss an issue, it may be sufficient to simply note the topic that caused the anxiousness and investigate it further elsewhere.

A reviewer's responsibility in the interview is to obtain information about the status of the project, not to give information. Do not supply information because it might influence the responses of the individual. While speaking or listening, do not show emotion or offer judgments about the projects. Furthermore, do not indicate whether information confirms or contradicts previous sources.

After all questions are asked, it is usually a good practice to open the interview to anything the project member wishes to discuss. This could be done by saying: "We have talked about a lot of subjects. Is there anything we have not discussed that you would like to tell me at this time?" If no response is elicited, say "Is there anything this project does especially well that you would like to point out?" Reviewers should be especially attentive during this time because quite often the individual will then offer additional information, sometimes providing more useful responses than during the more structured portion of the interview.

When finished, thank the individual for contributing to the review. Also, indicate that future contact may be necessary to clarify information. Terminate the interview. As a final step, take a short time to study the questionnaire and notes. Highlight the points to be verified elsewhere, fill in any gaps that are obvious, and retain the information to be used during the writing of the evaluation report.