NISTIR 4749

Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out

Dennis M. Gilbert
Project Leader

Nickilyn Lynch
Editor

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

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4749

Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out

Dennis M. Gilbert
Project Leader

Nickilyn Lynch
Editor

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

December 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

ABSTRACT

Each federal organization is fully responsible for its computer security program whether the security program is performed by in-house staff or contracted out. Time constraints, budget constraints, availability or expertise of staff, and the potential knowledge to be gained by the organization from an experienced contractor are among the reasons a federal organization may wish to get external assistance for some of these complex, labor intensive activities.

An interagency working group of federal and private sector security specialists developed this document. The document presents the ideas and experiences of those involved with computer security. It supports the operational field with a set of Statements of Works (SOWs) describing significant computer security activities. While not a substitute for good computer security management, organization staff and government contractors can use these SOWs as a basis for a common understanding of each described activity. The sample SOWs can foster easier access to more consistent, high-quality computer security services. The descriptions apply to contracting for services or obtaining them from within the organization.

NIST-SPONSORED WORKING GROUP

SAMPLE STATEMENTS OF WORK FOR FEDERAL COMPUTER SECURITY SERVICES: FOR USE IN-HOUSE OR CONTRACTING OUT

PROJECT PARTICIPANTS AND REPORT CONTRIBUTORS

Dennis Gilbert *	NIST Project Leader and Working Group Chair
Nickilyn Lynch *	NIST Editor
Douglas Arai *	General Service Administration
Jon Arneson * +	NIST
Michael Arant	Department of Veterans Affairs
Vernon Bostelman * +	National Institutes of Health
Nander Brown * +	Small Business Administration
Dick Costello	Department of Justice
Rita Crawford * +	United States Postal Service
Grace Culver *	General Service Administration
Dorothea de Zafra	Public Health Service
Barbara Estrada *	Department of the Treasury
Ellen Flahavin	NIST
Irene Gilbert *	NIST
Dara Gordon *	Nuclear Regulatory Commission
Dan Grulke	Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Barbara Guttman *	NIST
John Haines	Department of the Interior
Mildred Harrison	Federal Emergency Management Agency
John Ippolito *	COMSIS
Gerald Lang *+	Department of Veterans Affairs
Wayne Madsen	Department of State
Harris McGarrah	U.S. Coast Guard
Harold McKee	General Service Administration
Gary Oran * +	Federal Emergency Management Agency
Nick Pantiuk	Grumman Data Systems
John Przysucha * +	Department of Energy
Darryl Robbins *	Federal Aviation Administration
Emily Robinson *	Nuclear Regulatory Commission
Philip Sibert	Department of Energy
Merv Stuckey * +	Bureau of the Census
Jim Tippett	National Computer Security Center
Bob Umberger	Department of Labor

* denotes Report Contributor + denotes Subcommittee Chair
NIST - National Institute of Standards and Technology

SAMPLE STATEMENTS OF WORK FOR FEDERAL COMPUTER SECURITY SERVICES: FOR USE IN-HOUSE OR CONTRACTING OUT

TABLE OF CONTENTS

LIST OF TABLES

LIST OF APPENDICES

I. INTRODUCTION

A. Document Purpose, Scope and Audience

The Computer Security Act of 1987 and other federal regulations require federal organizations to develop programs and perform activities that protect federal systems that contain sensitive information. The organization is fully responsible for its computer security program whether the security program is performed by in-house staff or contracted out. There are many reasons why a federal organization may wish to get external assistance for some of these complex, labor intensive activities. Time constraints, budget constraints, availability or expertise of staff, and the potential knowledge to be gained by the organization from an experienced contractor are among factors to be considered and carefully balanced in deciding whether external assistance is warranted. Office of Management and Budget (OMB) Circular A-76, Performance of Commercial Activities, and its subsequent transmittal memos, provides additional encouragement and guidance.

The purpose of this document is to help federal information resources managers (IRMs), computer security officials (CSOs), and others exercise their computer security responsibilities. The document provides sample Statements of Work (SOWs) for often-performed computer security activities. Organization staff and government contractors may use these SOWs as a basis for understanding each described activity. The sample SOWs can foster easier access to more consistent, high-quality computer security services.

This document was developed by an interagency working group of federal and private sector security specialists. It was further reviewed by other specialists from both sectors. The document presents the ideas and experiences of those involved with computer security. It supports the operational field by describing significant computer security activities. It is felt federal organizations can more effectively carry out computer security responsibilities if clear descriptions of these activities are available.

This document addresses obtaining computer security services, not buying the actual hardware or software that provides security for a system. The document applies to systems subject to the Computer Security Act.

B. Not a Substitute for Good Computer Security Management

The SOWs are presented as samples and are not intended as "boiler plate." Each organization should analyze its specific needs and determine its functional, resource, and schedule requirements and constraints. The SOWs are designed to be modular and flexible, fitting a variety of situations. Computer systems, environments, and organization policies are different, making each computer security services buy unique. However, the computer security activities themselves are similar; this document focuses on those similarities.

The SOWs are not a substitute for good computer security management. They should help those requiring the described services by providing checklists of tasks to be performed. The document is a tool that can save the organization valuable time and provide important reminders of what needs to be done. The document can be of particular value to those trying to establish a security program; experienced computer security personnel can also benefit.

C. Security is not a One-time Activity

Security is not a one-time activity. It is an integral part of the installation/system lifecycle. The activities described by the SOWs in this document generally require either periodic updating or appropriate revision. These changes are made when configurations and other conditions and circumstances change significantly, or as required by federal regulations.

D. Obtaining Computer Security Services: In-house vs. Contracting Out

The SOWs describe activities that can be contracted out or obtained from within the organization (in-house). Which method an organization uses depends on time constraints, budget constraints, availability or expertise of staff, and the potential knowledge gained by the organization from an experienced contractor. Regardless, there is no substitute for managers who understand their environment and incorporate security as an integral part of their computer system activities. Each organization has primary responsibility for protecting its computer systems and the data contained in those systems. Acknowledgment and acceptance of this responsibility is of prime importance.

E. Overview of the Document

In this document, related SOWs are grouped together under computer security "areas." These areas address the elements of a well-rounded computer security program. OMB Circular A-130, Appendix III identifies application security, information technology installation security, security awareness and training, and personnel security as the minimum elements of an agency computer security program.

Three of the elements are addressed with SOWs in Section III, IV, and V of the document. The fourth element, personnel security, is not represented as a separate SOW in this document, but as a task in the Development of a Computer Security Program SOW in Section II, Computer Security Program Management. It is presented this way because typically the organization's personnel office and data security office, rather than the computer security office, have the lead roles in this area. These offices normally are responsible for establishing and maintaining policies and procedures on position sensitivity classification, personnel security screening, and information confidentiality.

OMB Circular A-130, Appendix III requires agencies to implement and maintain an automated information systems security program, including the preparation of

policies, standards, and procedures. This subject is addressed in this document in Section II, Computer Security Program Management.

Section VI covers the formation of a Computer Security Incident Response Team. Although not explicitly required by federal directives, forming such a team is one method agencies are using to deal with the threat of computer security incidents.

Section VII, Special Studies/Product Evaluation, presents a set of SOWs to perform evaluations of ADP and computer security products.

The computer security areas and related SOWs are in Table I-1.

TABLE I-1 - Computer Security Areas and SOWs

DOCUMENT SECTION		COMPUTER SECURITY AREAS AND SOWS
II	A	Computer Security Program Management
	B	SOW: Development of a Computer Security Program
	C	SOW: Program Assessment
III	A	Application Security
	B	SOW: Computer Security Plan Preparation
	C	SOW: Certification of a Sensitive System
	D	SOW: Contingency Planning
	E	SOW: Sensitive/Critical Application Review (SCAR)
IV	A	Installation Security
	B	SOW: Risk Analysis of a System
	C	SOW: Disaster Recovery and Continuity of Operations Planning
V	A	Computer Security Awareness and Training
	B	SOW: Computer Security Awareness and Training
VI	A	Computer Security Incident Response
	B	SOW: Incident Response Team
VII	A	Special Studies/Product Evaluation
	B	SOW: Security Evaluation of an ADP Product
	C	SOW: Evaluation of Hardware/Software Tool that Performs a Direct Computer Security Function
	D	SOW: Evaluation of a Computer Security Management Aid: A Risk Management Tool

The areas and SOWs derive, either directly or indirectly, from requirements contained in major federal directive addressing computer security. Table II-2 shows some major

computer security requirements, the relevant directive(s), and the related SOW(s). Appendix E has additional references.

TABLE I-2 - Major Federal Directives, Computer Security Requirements, and Document Sections

MAJOR FEDERAL DIRECTIVES AND COMPUTER SECURITY REQUIREMENTS	DOCUMENT SECTIONS
Computer Security Act	
Computer Security and Privacy Plan (CSPP) Preparation	III.B
Mandatory, periodic security awareness and training	V.B
OMB Circular A-130, Appendix III	
AIS program	II.B,C
Application Security	
Management control process	
Security specifications	
Design review & test	
Certification	III.C
Periodic review & recertification	III.C
Contingency plans	III.D
Personnel Security	
Information Technology Installation Security	
Assignment of responsibility	II.B
Periodic risk analysis	IV.B
Disaster & continuity plans	IV.C
Acquisition specifications	
Security Awareness & Training	V.B
Reports (OMB Cir A-123)	III.C,IV.B
OMB Circular A-123	
Annual control report	
Security & other control weaknesses	III.C
Assurance of adequate security of AIS	IV.B

Each computer security area is introduced with an overview which sets the framework for the sample SOWs that follow. The SOWs focus on the computer security technical content of the contract - Purpose, Scope and Tasks. Appendices B through I contain examples of contracting-related options. Local or organization contracting staff should be consulted for contracting-related options, as every organization handles these subjects differently. This document should not be used to obtain the described services without first consulting with the organization's Contracting Officer.

F. The Evolving Nature of This Document

The document complements other NIST computer security publications and will be modified as necessary to meet the needs of federal organizations. Experience gained

by organizations, vendors, and others in using this document will contribute to its improvement. To that end, your experience with the document is solicited. Agencies are also invited to submit relevant SOWs and comments about their use. Please address correspondence on this document to the NIST Computer Security Division, Computer Systems Laboratory, A216 Technology Building, Gaithersburg, MD 20899.

G. Conventions in This Document

The SOWs may be used, with appropriate tailoring, by different levels of a federal organization (e.g., department, agency, bureau, region, branch, field office, etc.). The term **organization** is used in this document to cover whichever applies.

The document uses the greater-than lesser-than symbols **<>** in the SOWs to indicate information the organization will complete. To help fill this area with the appropriate information, a generic term or explanation is used, e.g., organization name. The Deliverable Section of each SOW uses the symbol **<X>**. This represents the number of working days from the beginning of the contract or from the previous milestone, as determined by the organization. Elsewhere, when a number is to be filled in, **<N>** is used. All words in <> are in **bold typeface**. Instructions to those tailoring or refining the SOWs are presented as notes, indicated as *(NOTE: .....)*.

H. Additional Sources of Information

Those tailoring the SOWs in this document may find other NIST publications valuable. Those performing the tasks in the SOWs can also benefit from these publications. Call the Computer Systems Laboratory (CSL) at (301)975-2821 to receive NIST Publication List 91, Computer Security Publications, an annotated bibliography of NIST computer security documents. Documents can be purchased through the Government Printing Office (GPO) at (202) 783-3238 and the National Technical Information Service (NTIS) at (703) 487-4780.

CSL Bulletins are published by NIST. Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Among the bulletins available are those on Data Encryption Standard, Guidance to Federal Agencies on the Use of Trusted Systems Technology, Computer Virus Attacks, Review of Federal Agency Computer Security and Privacy Plans, The GOSIP Testing Program, Security Issues in the Use of Electronic Data Interchange, and File Transfer, Access, and Management. Bulletins are issued on an as-needed basis and are available from CSL Publications, NIST B151, Technology Building, Gaithersburg, MD 20899, telephone (301)975-2821 or FTS 879-2821.

The National Computer Security Center (NCSC) publishes Compusec Technical Publications, sometimes referred to as the "Rainbow Series." Although these documents have been developed to support the processing and protection of classified data, they contain information that may be of value to those with sensitive non-classified environments. Contact (301) 766-8729 for a list of publications.

NCSC has a glossary, NCSC-TG-004, Glossary of Computer Security Terms. CSL has NISTIR 4659, Glossary of Computer Security Terminology. There is also CSL Bulletin,

Bibliography of Computer Security Glossaries, Sept 1990, which describes a number of glossaries.

NIST sponsors the NIST Computer Security Bulletin Board System which emphasizes information systems security issues. The bulletin board contains various types of awareness and reference materials, including bibliographies, security-related seminar and conference lists, and information about actual computer security incidents and how to protect against or correct known system vulnerabilities. The bulletin board's number is (301) 948-5717 (300,1200 or 2400 baud), (301) 948-5140 (9600 baud), voice (301) 975-3359.

NSA sponsors the National Computer Security Center (NCSC) Bulletin Board on DOCKMASTER which has over 3000 subscribers and serves as a focal point for interacting and exchanging computer security-related ideas among its users. For information, please call, in Maryland, (301) 850-4446; outside Maryland, (800) 336-3625.

NIST, with the National Security Agency (NSA), operates a Risk Management Laboratory in Gaithersburg, Maryland which investigates tools and techniques for risk management.

NIST is also producing a related guidance document "Computer Security Requirements in Procurement: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials," on including security requirements in ADP acquisitions. The document addresses computer security in the procurement cycle, the use of risk analyses in specification development, gaining assurance, and a list of clauses and specifications for contracts.

Please address questions about this document and other NIST computer security activities to the NIST Computer Security Division at (301) 975-2934.

For convenience, a copy of this document is available in machine-readable form. Making the document available in this manner facilitates the tailoring and refinement that is such an important factor in appropriately using the SOWs presented here. For further information, please contact CSL Publications at (301) 975-2821.

II. COMPUTER SECURITY PROGRAM MANAGEMENT

A. OVERVIEW

OMB Circular A-130, Appendix III requires agencies to implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. An effective computer security program is an important managerial responsibility. Management establishes a positive climate by making computer security a part of the information resources management process and by providing support for a viable computer security program.

Overall computer security program goals are established by federal regulations and the agency mission. These goals become the basis for organization computer security policy. Specific security objectives result from computer security program policy and computer security principles. Consideration of technology, resources, security principles, and environmental factors as well as computer security objectives, are used in developing the computer security program details.

The computer security program ensures that compliance requirements are satisfied and day-to-day operating risks are cost-effectively minimized. It also ensures conformance with the information resources management program and that information resources are adequately protected. This protection means appropriate technical, personnel, administrative, environmental, and telecommunications safeguards are maintained, and effective operation of computers and applications supporting critical organization functions is continued.

Once the computer security program is in place, an organization should periodically reassess the computer security program goals, policies, and objectives. Reassessment is also done as significant changes occur in its technological, managerial, economic, or political environment, or in external federal requirements. If there has been significant change, the computer security program is modified accordingly.

A computer security program assessment is a high-level, qualitative review of the information security program. This includes evaluating the degree of compliance with the computer security program and effectiveness of in-place automated and manual controls. The assessment also focuses on the operating environment, general management practices, and the degree of managerial support for the computer security program.

The first sample SOW presented in this section develops a computer security program and the plan for implementing the program. The second SOW is for a computer security program assessment.

SAMPLE STATEMENT OF WORK

B. Development of a Computer Security Program

PURPOSE/OBJECTIVE

The purpose of this SOW is to develop a computer security program for **<organization name>** and the plan for implementing the program. The computer security program addresses the security of information and computing resources at all organizational levels.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor develops a computer security program framework for **<organization name>** which includes policy statement(s). The framework also addresses the major elements of the program, resources required (including staff, budget, and equipment), and milestone/schedules. The computer security program addresses compliance requirements, day-to-day operating risks, and protection of information resources.

The final product is a computer security program for **<organization name>** and a plan for implementing it.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Current Computer Security Status

The Contractor shall, with the assistance of the **<computer security officer or other designated person>**, determine the current computer security program status. The Contractor shall determine what computer security program elements and documents exist. For those that exist, the Contractor shall review them. The Contractor shall note what elements or documents do not exist. The review shall examine documentation from:

- o application systems certifications, reviews, and risk analyses;
- o information technology installation reviews;
- o technical software evaluation;
- o contingency and disaster recovery plans and tests;
- o personnel security;
- o computer security awareness and training; and
- o security management and coordination.

<The Contractor shall conduct an estimated <N> trips to field installations to assess their computer security program.>

The Contractor shall also review:

- o applicable federal regulations;
- o organization mission statements;
- o organization information management resources policy statements;
- o automated information security goals, policies, procedures, and standards;
- o computer security and privacy plans; and
- o other associated documents.

The Contractor shall prepare a report documenting the findings of this task, including elements or documents that do not exist. The Contractor shall deliver the Current Computer Security Status Report to the Contracting Officer's Technical Representative (COTR).

Task 3 - Develop Framework for the Computer Security Program

The Contractor shall develop the framework for the computer security program. This framework shall include a draft computer security policy statement. The framework shall identify the major program elements, to include at a minimum:

- o personnel security;
- o end user computing;
- o application systems security; and
- o information technology installation security.

The report shall identify the resources available and/or required, including staff, budget, and equipment.

The Contractor shall **<prepare/revise>** a draft **<organization name>** computer security goals and policies statement(s). The goals shall reflect federal regulations and the agency mission. The policies shall reflect the computer security goals.

The Contractor shall deliver a Computer Security Program Structure Report and Policy Statement to the COTR.

Task 4 - Develop Computer Security Program Details/Strategies

The Contractor shall develop a set of computer security program details or strategies to include the following at a minimum;

- o personnel security strategy;
- o end user computing strategy;
- o application systems security strategy; and
- o information technology installation security strategy.

These strategies are outlined in Subtasks 4A-4D below. Each strategy shall include the following at a minimum:

- o draft position descriptions including authorities and responsibilities;
- o staffing justifications;
- o resource requirements projections;
- o budget projections; and
- o milestones and schedules.

For each strategy, the Contractor shall develop draft policies, procedures, and standards or identify existing ones. The Contractor shall prepare documents for each strategy incorporating the above elements.

Subtask 4A - Develop a Personnel Security Strategy

The Contractor shall develop a personnel security strategy. The strategy shall address policies, procedures, and mechanisms for disseminating information on security awareness and training, automated information access control, and accountability of operations.

The Contractor shall coordinate with the **<organization name>** personnel office and the data security office. This is done to ensure the developed strategy is consistent with **<organization name>** policies and procedures on position sensitivity classification, personnel security screening, and information confidentiality. The Contractor shall ensure the strategy applies to all employees and Contractor personnel whose duties involve accessing the computer system, system design, development or maintenance, or handling of sensitive information in hardcopy or computerized form.

The Contractor shall deliver the Personnel Security Strategy to the COTR.

Subtask 4B - Develop an End User Computer Security Strategy

The Contractor shall develop a computer security strategy specifically addressing end users. This strategy shall include the necessary degree of protection according to the sensitivity of the information maintained and processed by the user.

As a minimum, the end user computer security strategy shall cover:

- o data and system integrity;
- o confidentiality of data;
- o access control and accountability;
- o separation of duties;
- o computer security awareness and training;
- o availability of service and continuity of operations; and
- o auditability of operations.

The Contractor shall deliver an End User Computer Security Strategy to the COTR.

Subtask 4C - Develop an Application Systems Security Strategy

The Contractor shall develop an application systems security strategy. The strategy shall address the safeguards required due to the nature of the data processed. A key consideration is the risk and size of loss or harm that could result from improper operation or deliberate manipulation of the application.

The following security and control features shall be included in the strategy at a minimum:

- o auditability;
- o isolation;
- o controllability;
- o recoverability;
- o sensitivity;
- o identification;
- o survivability;
- o availability;
- o integrity;
- o confidentiality; and
- o **<other control objectives>**

The Contractor shall also develop guidance for the preparation of computer security and privacy plans prepared in accordance with the Computer Security Act and OMB implementing instructions.

The Contractor shall deliver an Application Systems Security Strategy to the COTR.

Subtask 4D - Develop an Information Technology Installation Security Strategy

The Contractor shall develop an information technology installation security strategy. This strategy shall include conducting risk analyses and ensuring disaster recovery/continuity of operations planning for **<organization name>** ADP facilities and contingency planning for **<organization name>** application systems. This strategy shall address **<organization name>**'s unique distributed processing environment, network, and information sensitivity needs. Included in the strategy shall be an identification of critical systems and applications. It will also cover risk analysis

methodologies and techniques and alternative processing strategies.

The strategy shall address the following at a minimum:

- o individual accountability;
- o reliability of service;
- o separation of duties;
- o continuity of service;
- o recoverability;
- o confidentiality of data; and
- o resource protection.

The Contractor shall deliver an Information Technology Installation Security Strategy to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLE	DUE DATE
Work Plan Development	<X> *
Current Computer Security Status Report	<X> *
Computer Security Program Structure Report and Policy Statement	<X> *
Personnel Security Strategy	<X> *
End User Computer Security Strategy	<X> *
Application Systems Security Strategy	<X> *
Information Technology Installation Security Strategy	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and others are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

C. PROGRAM ASSESSMENT

PURPOSE/OBJECTIVE

The purpose of this SOW is to document the degree of compliance with the information security program and the effectiveness of security controls.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

Program assessment is a high-level review of the computer security program and its implementation to determine what is lacking and what needs to be looked at in depth, such as:

- o management procedures and controls;
- o physical, data, operating system, application software, personnel, and network security; and
- o disaster recovery.

Checklists shall be developed to assist in evaluating specific areas of interest. The Contractor shall identify problems that exist and make recommendations.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Management Procedures and Controls

The Contractor shall examine the management procedures that support security. This includes a study of the organization chart, the authorities and responsibilities, and the separation of functions. The Contractor shall also provide a list of management controls to be reviewed in each area (general, physical, data, and system and application software). This list shall, at a minimum, include:

- written policies and operating procedures of the data center;
- malfunction and hardware error reporting procedures;
- user job accounting procedures;
- efficiency control evaluations;
- organization and reporting hierarchy including proper separation of duties; and
- development and implementation of security awareness and training.

The Contractor shall deliver the Management Procedures and Controls Report to the Contracting Officer's Technical Representative (COTR).

Task 3 - Review Physical Security

The Contractor shall review the physical protection of personnel, facility, and computer assets. The Contractor shall develop a list of physical security procedures and controls in place. This list shall include authorizations for access to each area and, at a minimum include:

- physical access controls and their effectiveness;
- locks and entry procedures;
- air conditioning, uninterruptable power supply, and fire suppression and pumping equipment for adequacy and proper maintenance;
- reports distribution;
- protection against hardware and software theft and other human and machine-related threats;
- procedures for off-site storage of data and software;
- procedures for reacting to natural disasters and other nature-based threats to the facility, such as flood, fire, earthquake, hurricane, or twister; and
- personal computer use and software copyright license policy.

The Contractor shall deliver the Physical Security Procedures and Controls Report to the COTR.

Task 4 - Review Data Security

The Contractor shall examine sensitive and critical databases and files. The Contractor shall develop a list for review of data security techniques and methods, which, at a minimum, shall include:

- access control, integrity controls, and backup procedures;
- data element documentation;
- sensitive data procedures and implementation;
- existing privacy policies and protections;
- data access (both the authorization and implementation);
- application software and how applications are moved into production;
- written user responsibilities for management of data and applications; and
- direct access storage device (DASD) management techniques and the

impact on user file integrity.

The Contractor shall deliver the Data Security Techniques and Methods Report to the COTR.

Task 5 - Review Operating System Security

The Contractor shall examine the specific operating system. This examination shall, at a minimum, include:

- o review of the operating system and its installation;
- o backup and restore procedures;
- o review of system exits;
- o verification of audit trails;
- o review of handling and availability of system logs;
- o identification of change control procedures (installation of new software releases);
- o check for procedures which ensure that software patches are kept current;
- o review of installation for integrity;
- o review interfaces to access control package (if installed);
- o identification of primary access control software and files and procedures for ensuring that all software runs under its control;
- o review of access authorizations for appropriateness and completeness; and
- o review of interfaces with the access control package for integrity.

The Contractor shall deliver an Operating System Report to the COTR.

Task 6 - Review Application Software Security

The Contractor shall review the system development life cycle (SDLC) used to manage application development and maintenance. This review shall minimally include:

- o methods for developing and documenting application controls;
- o adherence to SDLC:
  - a review of quality assurance and testing procedures;
  - change control procedures for corrections and enhancements;
- o check for procedures which ensure that software patches are kept current;
- o system documentation and security standards and adherence to both; and
- o application operation and access to applications.

The Contractor shall deliver the Application Software Security Report to the COTR.

Task 7 - Review Personnel Security

The contractor shall develop a report which evaluates compliance with federal and **<organization name>** personnel security policies and procedures covering such elements as position sensitivity classification, personnel security screening, information confidentiality, and security training and awareness. The report shall address whether the policies and procedures cover personnel in all positions with access to sensitive data.

The contractor shall deliver the Personnel Security Report to the COTR.

Task 8 - Review Network Security

The Contractor shall review network security, evaluating its confidentiality, integrity, and availability. This review shall include, as applicable, access control, authentication, security administration, type and security of network media, security of file and print servers, encryption, interfaces between network and operating system/application software security modules, and conformance to networking standards.

The Contractor shall deliver the Network Security Review Report to the COTR.

Task 9 - Review Disaster Recovery Plans

(NOTE: This Task assumes there is an in-place disaster recovery plan. If there is no such plan or it is incomplete, a plan is done in a separate contract.)

The Contractor shall review the disaster recovery plan for user involvement, practical application, thoroughness, and correctness. The Contractor shall review the most recent test plans and test results, noting identified deficiencies and corrective actions incorporated into the plan.

The Contractor shall deliver a Disaster Recovery Review Report to the COTR.

Task 10 - Program Assessment Report

The Contractor shall develop a program assessment report which summarizes overall security compliance. The report shall detail major security weaknesses requiring correction and potential savings. It shall provide a summary of each area by: area reviewed, findings, impact of weaknesses in security (if any), and recommendations of actions that could be taken by management (if any). The report shall also identify those areas requiring more detailed study.

The Contractor shall deliver the Program Assessment Report to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Management Procedures and Controls Report	<X> *
Physical Security Procedures and Controls Report	<X> *
Data Security Techniques and Methods Report	<X> *
Operating System Report	<X> *
Application Software Security Report	<X> *
Personnel Security Report	<X> *
Network Security Review Report	<X> *
Disaster Recovery Review Report	<X> *
Program Assessment Report	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

III. APPLICATION SECURITY

A. OVERVIEW

Application security is identified by OMB Circular A-130, Appendix III as one of the four primary elements of an agency computer security program. Each of the SOWs presented in this section support application security. As indicated in Section I, application security activities should be performed in conjunction with the installation security activities described in Section IV as part of the organization's whole computer security program. Computer security plan preparation, certification, and contingency planning are discussed below. Also discussed is Sensitive/Critical Application Review (SCAR) of a specific application.

Computer Security and Privacy Plan Preparation (IAW OMB Cir 90-08)
The Computer Security Act of 1987 imposes three requirements on federal agencies. First, each organization must identify systems which contain sensitive information. Second, each organization must establish security plans for those systems. Finally, each organization must provide mandatory periodic training for all persons involved in the management, use, or operation of federal computer systems that contain sensitive information. This section addresses the second requirement, plan preparation.

Each organization identifies its own sensitive systems based on its unique environment within the scope of the Act. As defined in the Act, "sensitive information" is 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 the Privacy Act. Excluded from the definition is information that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

After identifying a sensitive system, a security plan is developed. The current suggested format is in Office of Management and Budget (OMB) Bulletin 90-08, "Guidance for the Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information."

A security plan prepared under OMB Bulletin 90-08 should be an abstract of the detailed security plan for the system. If a detailed security plan does not exist, the OMB Bulletin 90-08 plan can be a starting point. The detailed plan will contain significantly more information in such areas as risk analysis, contingency planning, backup procedures, personnel screening and selection, password management, user identification and authentication, and audit and variance detection.

This SOW addresses developing an OMB Bulletin 90-08 plan.

Certification
A major responsibility of management is to ensure that information resources are adequately protected. One method to meet this responsibility is periodic certification and accreditation of sensitive systems. OMB Circular A-130, Appendix III requires agencies to conduct periodic audits or reviews of sensitive applications and to

recertify the adequacy of safeguards. It specifies that this be done at least every 3 years and that audits and reviews be considered part of the agency vulnerability assessment and internal control reviews conducted in accordance with OMB Circular A-123.

Certification is a technical review made as part of and in support of the accreditation process. Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. It also produces a judgement and statement of opinion that the accrediting official can use to officially accredit the system.

Accreditation is the authorization and approval granted to a system or network to process sensitive data in an operational environment. Accreditation is based on a certification by designated technical personnel that a system's design and implementation meets security requirements and achieves adequate application security commensurate with the risks in the application's environment.

Based on the recommendations in the certification report, the accrediting official issues an accreditation decision. There are several accreditation alternatives depending upon results of the certification evaluation and report. Accreditation options are:

- o unconditional accreditation;
- o conditional accreditation granted with certain restrictions;
  - such as continued operation under specific conditions or pending the correction of minor security weaknesses;
- o accreditation withheld or delayed;
  - pending implementation of procedures or safeguards to address major security weaknesses;
- o accreditation denied;
  - design and development effort must implement required security measures;
  - system presents a major risk to the organization;
  - the complete system must be redesigned and redeveloped; and
  - a new certification evaluation is required.

Contingency Planning

OMB Circular A-130, Section III, requires agencies to establish policies and assign responsibilities to assure development of appropriate contingency plans and maintenance by end users of data processing. This policy is to ensure that essential business functions will continue if data processing support is interrupted. The Circular advises that contingency plans be consistent with the disaster recovery and continuity of operation plans for facilities that support sensitive applications. These plans are required for all such information technology installations. Each hardware system is included in the facility security plan. Each sensitive application needs a planned means of backup and recovery based on the cost-effectiveness of available alternatives. A risk analysis that identifies threats/vulnerabilities should be conducted prior to the planning process.

A sample SOW for reviewing contingency planning is presented in this section. A

sample SOW for reviewing disaster recovery/continuity of operations is presented in Section IV.C. Contingency planning and disaster recovery should be viewed as complementary activities performed taking into account the other. Together, they ensure that sensitive applications will have the necessary environment and resources to function, regardless of the circumstances.

Sensitive/Critical Application Review (SCAR)

One specific application may need an evaluation. In that event, an organization may contract for a sensitive/critical application review (SCAR). This review focuses on the security and criticality of that application. This section also contains a SOW addressing this activity.

SAMPLE STATEMENT OF WORK

B. COMPUTER SECURITY AND PRIVACY PLAN PREPARATION (IAW OMB CIR 90-08)

PURPOSE/OBJECTIVES

The purpose of this SOW is to produce a computer security plan for sensitive systems in the format suggested by Office of Management and Budget (OMB) Bulletin 90-08. This plan will satisfy a requirement of the Computer Security Act of 1987.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

Using OMB Bulletin 90-08 as a guideline and with specific direction from the Contracting Officer's Technical Representative (COTR), the Contractor shall prepare a security plan for the following system:

<list system name, size and function such as brand/model/function/networked>

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Prepare Plan According to OMB Bulletin 90-08

The Contractor shall interview all personnel on the list provided, read all provided documentation, and prepare an OMB Bulletin 90-08 plan. The interview list will consist of **<number of people>** in **<type of positions such as system managers, users, functional managers, programmers, operations personnel>.** The documentation shall consist of the following documents to be reviewed: **<Include the names and types, such as system documentation, policy, procedures, directives, user manuals, statutes, handbooks, security plans, contingency plans, risk analysis results, here or on a separate sheet.>** *(NOTE: If the Contractor is to use other means of obtaining information such as accessing the system or visiting sites, these activities must be described here.)* The names of interviewees and the documentation will be provided

by the COTR. OMB Bulletin 90-08 defines four sections of a Computer Security Plan.

For Section I, the Contractor shall **<analyze/review/verify>** and document the nature of the system and its environment.

For Section II, the Contractor shall **<analyze/review/verify>** and document the sensitivity of the system and the information contained in the system.

For Section III, the Contractor shall explain the degree to which controls have been implemented and current organization position as to when new controls will be implemented. The Contractor shall document the rationale for not implementing any of the controls listed in OMB Bulletin 90-08, Section III.

For Section IV, the Contractor shall document relevant comments or concerns raised during the interview process or plan preparation.

The Contractor shall prepare and deliver the Security Plan to the COTR. The plan shall incorporate all four sections identified in OMB Bulletin 90-08.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Security Plan	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

Possible intermediate deliverables for complex systems include:

- o interview reports
- o drafts in accordance with the three major sections of OMB Bulletin 90-08: System Identification, Sensitivity of Information, and System Security Measures.

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

Government-Furnished Equipment(GFE)/Government-Furnished Material(GFM)

No GFE will be provided. The contractor will be given an interview list and copies of the documentation referenced in Task 2. Any other existing documentation pertinent to this system and to this contract will also be provided.

C. CERTIFICATION OF A SENSITIVE SYSTEM

PURPOSE/OBJECTIVES

The purpose of this SOW is to conduct a security certification review of a sensitive system, **<under development/operational>** for **<certification/recertification>** of the adequacy of controls and security safeguards. The objective is to determine whether the control and security measures implemented on the system are sufficient to eliminate, contain or mitigate threats and identify vulnerabilities. The review follows OMB Circular A-130, Appendix III and **<organization name>** regulations on sensitive systems. The final report provides enough information to enable the designated official to make an accreditation decision.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The scope of the certification review is an assessment and evaluation of the controls implemented to ensure the security and integrity of the system and its software and data. Systems under development are evaluated to determine the presence of controls and security.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Determine Security Requirements

The Contractor shall study the system to gain an overall understanding of the system, its users, functional requirements, and security requirements.

Task 3 - Prepare/Review Statement of Systems Security Requirements

The Contractor shall prepare a statement of systems security requirements. For operational systems, the Contractor shall review and revise, as necessary, the existing statement of systems security requirements.

The Contractor shall deliver the Statement of Systems Security Requirements to the Contracting Officer's Technical Representative (COTR). After revisions are made and approved, the system shall be rated against the requirements in this document.

Task 4 - Perform Basic Evaluation of System

The Contractor shall review system documentation, pertinent regulations, and statutory provisions with which the system must comply. The Contractor shall also review and consider the results of any periodic information technology installation risk analysis. The Contractor shall evaluate whether:

- o security requirements are acceptable;
- o design or description of security functions satisfy the security requirements;
- o security functions are implemented; and
- o implementation method provides assurance that security functions have been acceptably implemented.

Among the items examined are:

- o internal controls;
  - adequacy of internal controls, audit trails, and technical security measures;
- o operational security;
  - operational and physical security measures;
- o data integrity;
  - techniques installed to ensure the integrity and reliability of data;
  - assessment of input, processing, output, and manual controls;
- o system functional requirements;
  - processing requirements and objectives to be minimally successful in meeting user needs;
- o software integrity;
  - techniques employed to ensure correctness, robustness, and trustworthiness of the software;
  - (a) construction of easily maintainable programs that reflect quality and structure; (b) compliance with programming standards; (c) use of comprehensive test procedures; and (d) inclusion of data error detection procedures; and
- o test plan and system test results;
  - test plan, results of system tests, and extent of user involvement;
  - compliance with FIPS (Federal Information Processing Standards) on application testing.

If additional evidence is necessary, as indicated by the basic evaluation, the Contractor shall perform a detailed evaluation addressing:

- o whether the controls function properly;
- o whether controls satisfy performance criteria;
- o how readily controls can be broken or circumvented; and
- o if components needing detailed analysis.

The Contractor shall deliver the System Evaluation Report to the COTR.

Task 5 - Prepare Control Matrix

Based on evaluations in above tasks, the Contractor shall prepare a control matrix identifying the basic strategy and the control techniques implemented to contain threats, address vulnerabilities, and achieve security objectives. The Contractor shall review the control matrix and security requirements to determine where additional safeguards are needed.

The Contractor shall deliver the Control Matrix and Report to the COTR.

Task 6 - Prepare Security Certification Report

The Contractor shall prepare a security certification report summarizing the performance results and recommendations of each above task for the designated accrediting official. The statement shall address the adequacy of the security and integrity measures implemented or under development.

The Contractor shall deliver the Security Certification Report and Statement to the COTR.

Task 7 - Prepare Draft Accreditation Decision Statement (Optional)

(NOTE: Some organizations choose to cleanly separate the certification and accreditation activities. Although an accreditation decision statement is necessary, its inclusion as part of this SOW is optional.)

Based on the recommendations included in the certification report and the security certification statement, the Contractor shall prepare a draft accreditation decision statement for the designated accrediting official. The Contractor shall coordinate the statement with the **<organization name>** Computer Security Officer and the designated accrediting official. The draft accreditation decision statement will address:

- o whether the accreditation is conditional or unconditional;
- o if conditional, what restrictions apply to accreditation; and
- o whether the accreditation is withheld, delayed, or denied, and what needs to be done to change the conditions.

The Contractor shall deliver the Draft Accreditation Decision Statement to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Statement of Systems Security Requirements	<X> *
System Evaluation Report	<X> *
Control Matrix and Report	<X> *
Security Certification Report and Statement	<X> *
Draft Accreditation Decision Statement (Optional)	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

D. CONTINGENCY PLANNING

(NOTE: Based on the long-stated OMB requirements for agencies to have contingency plans for their information technology applications, this SOW assumes there is an in-place contingency plan. If there is no such plan, or it is incomplete, a plan may be developed in a separate contract. This SOW can be modified for developing the contingency plan, reflecting the elements described in the review tasks below. The references in Appendix E under Risk Analysis and Program Assessment and the corresponding SOWs in this document can be useful if either a risk analysis needs to be done and/or an organization security plan needs to be developed. The references in Appendix E under Contingency Planning contain information regarding emergency response, damage assessment, backup, and disaster recovery.)

PURPOSE/OBJECTIVES

The purpose of this SOW is to review existing contingency plans for sensitive applications. The Contractor assesses the validity and viability of existing contingency plans. Based on this assessment, the Contractor recommends changes, if any, to the contingency plans.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor shall evaluate each selected sensitive application and its contingency plan. This SOW encompasses applications which are processed on various computer platforms (e.g., Pcs, mainframes, and mini-computers). This SOW covers the following systems: **<list of sensitive systems>.**

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Installation Risk Analysis and Organization Security Plan

The Contractor shall review the appropriate **<organization name>** installation risk analysis and **<organization name>** security plan for the sensitive applications targeted by this SOW. The Contractor shall prepare a report documenting this review. The report shall address the controls and procedures outlined in the plan and the requirements of the referenced regulations and directives.

The Contractor shall deliver the **<organization name>** Installation Risk Analysis and Security Plan Report to the Contracting Officer's Technical Representative (COTR).

Task 3 - Review Contingency Plans

The Contractor shall review existing contingency plans developed for sensitive applications. Each review shall evaluate the current strategy for addressing emergencies and how that strategy is integrated into the overall security plan. The Contractor will also review the results of the most recent contingency plans test results, including the scenarios used. The Contractor shall document the findings of this review in a report.

The Contractor shall deliver the Contingency Plan Review Report to the COTR.

Task 4 - Review Current Emergency Response Procedures

The Contractor shall review current emergency response procedures and evaluate their effect on the continuous operation of the systems processing sensitive applications. The review shall be a step-by-step look at the planned responses and whether they are adequate to protect lives, limit damage, and minimize the impact on data processing operations. The Contractor will also review the results of the most recent emergency response procedures test results, including the scenarios used. The Contractor shall document the findings of this review in a report.

The Contractor shall deliver the Emergency Response Procedures Review Report to the COTR.

Task 5 - Evaluate Damage Assessment Methods

The Contractor shall evaluate the methods used to perform damage assessment, including their impact on security, and document the findings in a report. This report shall cover the methodologies used for damage assessment. The Contractor shall specify for each damage assessment methodology type of use, application, data integrity violation, and system damage.

The Contractor shall deliver the Damage Assessment Methods Evaluation Report to the COTR.

Task 6 - Review Backup Procedures

The Contractor shall review the backup procedures, including documentation of the most recent disaster recovery test, to assess adequacy of procedures and security of the system throughout the process. The Contractor will also review the results of the most recent backup procedures test results, including the scenarios used. It shall also include backup transportation, storage, and specific procedures supporting each sensitive application.

The Contractor shall deliver the Backup Procedures Review Report to the COTR.

Task 7 - Evaluate Disaster Recovery Plan

The Contractor shall evaluate the disaster recovery plan to determine its adequacy in providing a temporary or longer operating environment. The review shall cover required levels of security to see that they continue in force throughout the process of recovery, temporary operations, and the move back to the original processing site or to the new processing site. The Contractor will also review the results of the most recent disaster recovery test results, including the scenarios used. The Contractor shall document the review in a report.

The Contractor shall deliver the Disaster Recovery Evaluation Report to the COTR.

Task 8 - Prepare a Summary Report

The Contractor shall provide a summary report of all findings. The report shall take into account the risk analysis and disaster recovery planning procedures. The report shall address the plan for each sensitive application and data facility.

The Contractor shall deliver the Summary Report to the COTR in draft form. After revision, the final version shall be delivered to the COTR.

Task 9 - Prepare a Detailed Recommendations Report

The Contractor shall prepare a detailed report recommending changes to the contingency plan. It will include:

- a list of all documents reviewed or evaluated in the above tasks, recommendations made, personnel involved in the review, and recommendations impact;
- an estimate of the effort and cost associated with the recommendations;
- the scenarios for testing the plan;
- determination of how dependencies, any assistance needed from outside organizations, as well as difficulties in obtaining essential resources, impact on the plan;
- a list of priorities observed in recovery operations and the rationale in establishing those priorities; and
- a discussion of how these recommendations can be incorporated to

support the organization security plan.

The Contractor shall submit the Detailed Recommendations Report, first in draft form and then as a finished deliverable, to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
<organization name> Installation Risk Analysis Security Plan and Report	<X> *
Contingency Plan Review Report	<X> *
Emergency Response Procedures Review Report	<X> *
Damage Assessment Methods Evaluation Report	<X> *
Backup Procedures Review Report	<X> *
Disaster Recovery Evaluation Report	<X> *
Draft Summary Report	<X> *
Detailed Recommendations Report	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

E. Sensitive/Critical Application Review (SCAR)

PURPOSE/OBJECTIVE

The purpose of this SOW is to perform a security review of a sensitive/critical application of the **<Application Name>.**

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor shall evaluate the security and criticality of a computer application, **<application name>.** This shall form the basis of a technical certification and judgments about acceptance of the level of risk, i.e., accreditation by an authorized organization official.

TASK DESCRIPTIONS

Task 1 - Prepare a SCAR Work Plan

The Contractor shall conduct an initial site survey. Upon completion of the site survey, the Contractor shall develop a work plan and present it to the Contracting Officer's Technical Representative (COTR).

This work plan shall include the following:

- a statement of the Contractor's approach to the project including a description of specific procedures, methodology, and techniques to be employed in conducting the SCAR;
- a schedule for site visits, the identification of specific organizations and organization staff to be interviewed, the specific elements of information to be gathered during the visits, and an outline of the entrance and exit briefings at each site; and
- areas of potential weakness identified, and testing (if any) to be performed.

The **<organization name>** will review and approve the plan or return it for revision.

Task 2 will not begin before plan approval.

Task 2 - Perform Data Collection

The Contractor shall perform data collection according to the SCAR Work plan. This data will include at a minimum for the **<Application Name>**:

- o OMB Bulletin 90-08 Computer Security and Privacy Plan;
- o assignments of responsibility;
- o security specifications;
- o design reviews and test results;
- o audits results and certification and accreditation statements; and
- o contingency plans.

Task 3 - Prepare SCAR Report

The Contractor shall analyze the information collected during Task 2 and prepare a SCAR report. The SCAR report shall contain the following:

- o an executive summary of not more than two pages;
- o a discussion of the objectives and authority for the review;
- o a description of the application and its criticality and sensitivity status at the time the review was conducted;
- o the identified strengths and weaknesses in the application's security/internal control procedures (automated and manual);
- o the recommendations for improvements (if any), rated as to their potential effect on the security environment (low, moderate, high) and an implementation priority proposal; and
- o a draft certification statement which includes the Contractor's recommendation whether the application should be certified acceptable, not acceptable, or acceptable with qualification. If the Contractor makes a recommendation of certification with qualification, the draft certification statement shall also include those recommendations that must be implemented to obtain an unqualified acceptable certification.

The Contractor shall deliver the SCAR Report to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
SCAR Report	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

IV. INSTALLATION SECURITY

A. OVERVIEW

OMB Circular A-130, Appendix III identifies installation security as an element of an agency computer security program. Each of the SOWs presented in this section support installation security. As indicated in Section I, installation security activities should be performed in conjunction with the application security activities described in Section III as part of the organization's whole computer security program. Risk analysis and disaster recovery/continuity of operations are discussed below.

It should be noted that an installation or network, especially one that supports more than one application, may require its own Computer Security and Privacy Plan. If that is the case, refer to Section III.B.

Risk Analysis

Risk management is an iterative process that ensures reasonable steps are taken to protect automated information resources. Risk management seeks cost-effective safeguards against deliberate and accidental threats to computer system availability, data integrity and confidentiality. Managing risks involves identifying information assets and threats, assessing their potential impact and severity, and selecting appropriate safeguards. Computer security program assessment and risk analysis are part of risk management. One cannot have a full risk management process without the results of a program assessment and risk analysis. The results are presented to the organizations' management for a decision about the acceptable risks versus the cost of safeguards that can be implemented.

OMB Circular A-130, Appendix III requires agencies to establish and maintain a program to conduct periodic risk analysis at each installation to ensure that appropriate, cost-effective safeguards are incorporated into new and existing applications. The results of the risk analysis are taken into account by the official (re)certifying/accrediting the sensitive applications being processed at the installation. The risk analysis is also used in the evaluation of general controls over the management of information technology installations conducted in accordance with OMB Circular A-123. A risk analysis is required to be conducted at intervals consistent with the data processed, but at least every 5 years.

Risk analysis is the cornerstone of a risk management program, forming the basis for selecting cost-effective security controls. A risk analysis should, at a minimum, perform the following functions:

- identify and value assets;
- identify threats and vulnerabilities;
- consider the environment and review the effectiveness of current system safeguards;
- provide a risk calculation;
- optionally, perform a cost-benefit analysis; and
- recommend safeguards and develop a safeguards implementation plan.

The risk analysis SOW can be used to conduct a risk analysis of a computer facility, installation, or a communications network. The system may be in-place or under development.

Although there are common elements and concerns in both program assessment and risk analysis, program assessment is a broader look at the computer security environment.

Disaster Recovery and Continuity of Operations Planning

OMB Circular A-130, Section III, requires agencies to maintain continuity of operations plans for all information technology installations. This is to provide continued data processing support in the event that normal operations are prevented. These plans should be consistent with the contingency plans for the applications running on the installation and based on the cost-effectiveness of available alternatives. A risk analysis that identifies threats/vulnerabilities should be conducted prior to the planning process.

Reasonable continuity of operations is achieved by careful planning for an appropriate response to any interruption in data processing service. The elements to be considered include incident response, off-site storage, backup and recovery, and disaster/move planning. Disaster recovery and continuity of operations plans must be fully documented and tested periodically. For large facilities or those that support mission-essential/critical functions, these plans should be tested annually. Recovery plans must ensure that there is sufficient computer capacity to absorb the added workload from the damaged site in a timely manner for all sensitive applications and that backups are current. Staff must be trained to carry out procedures. These procedures need to include the management of communications among support systems.

Newer environments, such as distributed mini-computers linked by wide-area networks, local area networks of personal computers, and standalone multi-user and single user processors, present new concerns that must be addressed.

A SOW for disaster recovery and continuity of operations planning is presented in this section. A SOW for contingency planning is presented in Section III.D. Contingency planning and disaster recovery should be viewed as complementary activities, one taking into account the other. Together, they ensure that sensitive applications will have the necessary environment and resources, regardless of the circumstances.

B. RISK ANALYSIS OF A SYSTEM

PURPOSE/OBJECTIVE

The purpose of this SOW is to conduct a risk analysis. The risk analysis will include at a minimum:

- o identification and evaluation of computer/communications network assets;
- o identification of potential threats to those assets;
- o assessment of adequacy of existing management, operational, and technical controls in safeguarding assets against waste, loss, unauthorized access and use, and misappropriation; and
- o analysis of the consequences/impact of the potential threats resulting in safeguard recommendations.

An optional task will be to recommend cost-effective safeguards to reduce risks to an acceptable level.

ENVIRONMENT

(Note: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

A risk analysis on the **<computer facility/installation or communications system name>** will be conducted.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Select Methodology for Risk Analysis (Optional)

(NOTE: The organization may specify a specific risk analysis methodology or tool is to be used. If the organization does not designate a methodology or tool, then this task should be performed.)

The **<Contractor or organization name>** shall select the technique for estimating the probability and results of the occurrence of harmful events. The risk analysis methodology selected should include the following basic parts:

- o data collection necessary for the analysis;
- o asset valuation;
- o threat analysis;
- o safeguards effectiveness analysis;
- o risk calculation;
- o safeguards recommendations; and
- o optionally, cost-benefit analysis.

The Contractor shall deliver a Methodology Selection Report to the COTR, explaining the rationale for selecting the methodology.

Task 3 - Data Collection

The Contractor shall collect the data required to support the risk analysis methodology selected in Task 2 or specified by the organization. The validity of the results of the risk analysis is a direct reflection of the accuracy of the input. The requirements for the data collection task are:

- o establish system boundaries;
- o value assets;
- o identify threats; and
- o identify weakness in current safeguards systems.

Subtask 3A - Establish System Boundaries

The Contractor shall establish the boundaries of the system under analysis. Establishing parameters in which the system operates guarantees consideration of all security issues. Particularly, distributed systems and networks associated with the system should be considered.

Interviews shall be conducted with senior installation and project managers, user managers, and their staff. A review of system documentation shall be conducted.

Subtask 3B - Value Assets

The Contractor shall collect from the organization a complete list of assets, their value, sensitivity, and importance to the business of the organization.

Assets are defined as valuable objects that require protection from harm or compromise. Assets include information, data, hardware, environmental equipment (heating, ventilation and air conditioning (HVAC)), inventories, documents, personnel, real property, reputation, and services.

Subtask 3C - Identify Threats

The Contractor shall identify the threats to the system(s). This shall include both deliberate and accidental causes. Deliberate threats are those caused by people, and include willful damage, misuse of system resources, theft, and others. Accidents that threaten assets include acts of nature, errors by people, and malfunction of hardware and equipment.

Subtask 3D - Identify Weaknesses in Current Safeguards Systems

The Contractor shall analyze the effectiveness of security measures as an integral part of risk analysis. This shall include weaknesses in the organization's protection strategy that would illustrate not only ineffectiveness, but nonexistence of appropriate controls. The safeguards to evaluate fall into these categories:

- o administrative security;
- o physical security;
- o software security;
- o hardware security;
- o personnel security;
- o environmental security; and
- o communications security.

Task 4 - Risk Calculation

The Contractor shall determine the effect that a successful threat could have upon the organization. The risk calculations result from analyzing the values in Task 2 (asset values, relative weakness of current safeguards, and relative strength of the dynamic threat).

The calculation results shall be expressed in quantitative or qualitative terms. A quantitative approach produces results expressed in monetary terms, while a qualitative method makes use of phraseology and linguistic values.

The Contractor shall design the Risk Analysis Report in a manner that contributes to its use by the organization. The Contractor shall deliver the Risk Analysis Report to the COTR.

Task 5 - Cost-Benefit Analysis Report (Optional)

(NOTE: While the cost-benefit analysis is a necessary step in risk management, its inclusion in a risk analysis is optional. Therefore this task is optional in the SOW.)

The Contractor shall develop a cost-benefit analysis to provide a basis for selecting safeguards. The analysis shall describe safeguards that are both mutually supportive and cost-effective. The cost-benefit analysis report shall outline how much each proposed safeguard will cost and how much the it will reduce exposure. The Contractor will examine mutually supportive combinations of safeguards and prioritize

them based on cost-benefit.

The Contractor shall deliver a Cost-Benefit Analysis Report to the COTR.

Task 6 - Safeguards Recommendations (Optional)

The Contractor shall prepare a Safeguards Recommendations Report. The report shall recommend safeguards to minimize the impact of threats to the system. The report shall prioritize mutually supportive combinations of safeguards so as to minimize the organization's losses.

The Contractor shall deliver the Safeguards Recommendations Report to the COTR.

Task 7 - Develop a Safeguards Implementation Plan (Optional)

Contractor shall develop a plan for implementing the safeguards selected by the organization. The plan shall include:

- o where and how to obtain the safeguards;
- o staff and skills to operate or maintain the safeguards;
- o budget projections; and
- o milestones and schedules.

The Contractor shall deliver the Safeguards Implementation Report to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Methodology Selection Report (Optional)	<X> *
Risk Analysis Report	<X> *
Cost-Benefit Analysis Report (Optional)	<X> *
Safeguards Recommendations Report (Optional)	<X> *
Safeguards Implementation Report (Optional)	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts and other are found in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

C. DISASTER RECOVERY AND CONTINUITY OF OPERATIONS PLANNING

(NOTE: Based on the long-stated OMB requirements for agencies to maintain disaster recovery and continuity of operations plans for all information technology installations, this SOW assumes a disaster recovery and continuity of operations plan is in-place. If there is no such plan or it is incomplete, a plan can be done in a separate contract. This SOW can be modified for developing the disaster recovery and continuity of operations plan reflecting the elements described in the review tasks below. The references in Appendix E under Risk Analysis and Program Assessment and the corresponding SOWs in this document can be useful if either a risk analysis needs to be done and/or an organization security plan needs to be developed. The references in Appendix E under Disaster Recovery and Continuity of Operations Planning contain information regarding emergency response, damage assessment, backup, and disaster recovery.)

PURPOSE/OBJECTIVES

The purpose of this SOW is to review and improve the effectiveness of the disaster recovery and continuity of operations plan for a **<type of facility(ies)>** facility. The effort will ensure reasonable continuity of data processing support should normal operations be interrupted. The disaster recovery and continuity of operations plan is integrated into the contingency plans for the sensitive applications operating at the facility. The plan should be documented and tested periodically at a frequency consistent with the loss that could result from a disruption in service.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor reviews the disaster recovery and continuity of operations plan and recommends ways to increase the effectiveness of the plan. This plan must cover the following systems: **<List of sensitive systems>.**

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Installation Risk Analysis and <Organization Name> Installation Security Plan

The Contractor shall review the appropriate **<organization name>** installation risk analysis and the **<organization name>** security plan. The Contractor shall prepare a report documenting this review. The report shall cover how the controls and procedures outlined in the plan address the requirement of the referenced regulations and directives.

The Contractor shall deliver the **<organization name>** Installation Risk Analysis and Security Plan Report to the COTR.

Task 3 - Review Contingency Plans

The Contractor shall review existing **<organization name>** contingency plans for the sensitive applications, identifying the general nature of emergencies that are likely to occur, and determine a comprehensive continuity of operating strategy. Each plan review shall evaluate current strategy for addressing emergencies and their integration into the overall security plan. The Contractor will also review the results of the most recent contingency plans test results, including the scenarios used. The Contractor shall document the findings of this review in a report.

The Contractor shall deliver the Contingency Plan Review Report to the COTR.

Task 4 - Review Backup Procedures

The Contractor shall review all system backup procedures. The Contractor will also review the results of the most recent backup procedures test results, including the scenarios used. The review ensures that during the recovery of a failed system and/or the move of a system during a disaster, all controls normally in place remain intact.

The Contractor shall deliver the Backup Procedures Review Report to the COTR.

Task 5 - Review Continuity of Operations/Disaster Recovery Move Plan

The Contractor shall review the continuity of operations/disaster recovery move plan to ensure that it provides continuous support for systems during or following a major disaster at the computer facility or when difficulties disable a computer system. This plan includes restoring the computer system in its original environment. The Contractor will also review the results of the most recent continuity of operations/disaster recovery move plan test results, including the scenarios used. Any

discrepancy in the plan for restoration shall be documented.

The Contractor shall deliver the Continuity of Operations/Disaster Recovery Move Plan Review Report to the COTR.

Task 6 - Examine Procedures and Practices for Off-Site Storage

The Contractor shall examine procedures and practices for off-site storage. This includes:

- o inventory all data files required by each system;
- o check timing of backup and retention of data files;
- o walk through the off-site storage procedures for system backup;
- o examine the off-site storage facility for adequacy of protective controls;
- o review procedures for delivery of the backup systems to the recovery facility/site;
- o check for backup copies, adequacy, and location of backup documentation; and
- o check on security maintenance for off-site storage.

The Contractor shall deliver the Procedures and Practices for Off-Site Storage Evaluation Report to the COTR.

Task 7 - Disaster Recovery Test Procedures Review

The Contractor shall evaluate and report the effectiveness of disaster recovery test procedures. The report should include an evaluation of the procedures for documenting weaknesses and a discussion of how security is tested in the recovery/backup system.

The Contractor shall deliver the Disaster Recovery Test Procedures Review Report to the COTR.

Task 8 - Evaluate ADP Backup Processing Alternatives

The Contractor shall identify and compare ADP processing alternatives against those currently employed.

The Contractor shall deliver a ADP Backup Processing Alternatives Report in draft form to the COTR.

Task 9 - Prepare a Summary and Recommendations Report

The Contractor shall develop a summary of all findings. This summary shall become input to the risk analysis and contingency planning procedures. The Contractor shall also prepare a detailed recommendations report. The Contractor shall describe how the recommendations can be incorporated to support the organization security plan.

The report shall include:

- o list all documents reviewed or evaluated in above tasks, recommendation made, personnel involved in the review, and recommendations impact;
- o estimate the effort and cost associated with the recommendations;
- o specify the scenarios designed for the plan;
- o determine how dependencies, any assistance needed from outside organizations, as well as difficulties in obtaining essential resources, impact on the plan; and
- o list the priorities observed in recovery operations and the rationale behind those priorities.

The Contractor shall submit a Recommendations Report, first in draft form and then, following comments by the COTR, as a finished deliverable.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
<organization name> Installation Risk Analysis Report and Security Plan	<X> *
Contingency Plan Review Report	<X> *
Backup Procedures Review Report	<X> *
Continuity of Operations/Disaster Recovery Move Plan Review Report	<X> *
Procedures and Practices of Off-Site Storage Evaluation Report	<X> *
Disaster Recovery Test Procedures Review Report	<X> *
ADP Backup Processing Alternatives Report	<X> *
Recommendations Report	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these

sections and the Contracting Officer should be consulted.)

V. COMPUTER SECURITY AWARENESS AND TRAINING

A. OVERVIEW

Federal organizations have a mandatory requirement to provide computer security awareness and training for employees responsible for management and use of federal computer systems that process sensitive information. To satisfy the requirement, organizations should ensure that employees receive training which covers the basics of computer security as well as courses specific to the needs of the employee.

The computer security awareness and training requirement is based on federal regulations which emphasize this as an element of resources management. These requirements are derived from Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems, and Public Law 100-235, the Computer Security Act of 1987.

SAMPLE STATEMENT OF WORK

B. COMPUTER SECURITY AWARENESS AND TRAINING

PURPOSE/OBJECTIVE

The purpose of this SOW is to develop a computer security awareness and training course specific to **<organization name>**. This course may be conducted by organization staff or by Contractor staff under a separate contract. The course encompasses lesson plans, training aids, hand-out material, and periodic visual reminders for heightening awareness.

The Contractor develops a computer security awareness and training course tailored to the organization's needs. This contract requires the development of computer security awareness training materials tailored to the organization's needs which may be used by a contractor or by the organization, in subsequent training sessions.

At a minimum, the Contractor shall include one or more of the five basic subject areas into a computer security awareness and training plan for the specific audience categories within the organization. The five basic subject areas are:

- computer security basics;
- security planning and management;
- computer security policies and procedures;
- contingency plan/disaster recovery planning; and
- systems life cycle management.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor shall design and develop an Instructor's Guide and a participant material packet for a classroom-based course. The Instructor's Guide will provide the instructor with guidance for presentation of the course. The participant material packet will provide the participant with the materials discussed in the course for future reference. The Instructor's Guide and the participants material shall be designed for distribution in a three-ring binder. This will facilitate updating.

These items shall be included in the Instructor's Guide:

- o a table of contents;
- o a list of materials required to present the course;
- o a list of frequently used acronyms;
- o approximate time estimates to present each section;
- o references to other manuals and guides on security awareness and training; and
- o hardcopies of the transparencies.

These items shall be included in the participant material packet:

- o a table of contents;
- o an agenda;
- o a list of organization-specific and federal regulations and policies;
- o a reference list of manuals and guides for more security awareness information;
- o an acronym listing; and
- o hardcopies of the transparencies.

The Contractor shall design two versions of a text-only cover for the Instructor's Guide and the participant materials. The **<organization name>** will review the covers and make a selection with possible changes to be incorporated in the final reproducible covers.

The Contractor shall submit to the organization all course materials for review. The Contractor shall meet with the organization to discuss revisions. Any revisions shall be incorporated in a revised draft and submitted to the organization. The Contractor shall meet with the organization to present the final draft before presenting the course to the training participants.

The Contractor shall submit to the organization:

- o two copies each of the draft, revised draft, reproducible master of the Instructor's Guide, participant materials, and transparencies;
- o final machine-readable copy of all course materials **<specify machine, software and version>**; and
- o reproducible covers for the Instructor's Guide and participant materials.

The purpose and course objectives are to be stated for each course. If videos are used, they shall be submitted to the organization IRM Systems Security Officer for review.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Develop Course Outline and Master Lesson Plan

The Contractor shall develop a master lesson plan and supporting course material for each audience category within the organization. The guidelines for this task are in the task description section.

The Contractor shall present the Course Outline and Master Lesson Plan to the computer security staff.

Task 3 - Develop Lesson Plan for Each Audience Category

The Contractor shall develop a lesson plan and supporting course material for each audience category within the organization. The guidelines for this task are in NIST SP 500-172, Computer Security Training Guidelines.

The Contractor shall present each Lesson Plan and Supporting Course Material for each audience category to the computer security staff.

Task 4 - Conduct Pilot Class

The Contractor shall conduct a pilot class for each course developed and use an evaluation methodology approved by the organization to measure course results.

Task 5 - Final Course Materials

The Contractor shall submit the final Instructor Guide and Participant Material Packet to the Contracting Officer's Technical Representative (COTR). This shall include all supporting material developed in the above tasks.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Course Outline and Master Lesson Plan	<X> *
Lesson Plan and Supporting Course Material for each Audience Category	<X> *
Conduct Pilot Class	<X> *
Instructor Guide and Participant Course Material	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

Government-Furnished Equipment (GFE)/Government-Furnished Materials (GFM)

The organization shall furnish the space in which the training will be conducted, the required reproduced copies of the Instructor's Guide and participants materials, and the necessary audio/visual equipment.

VI. COMPUTER SECURITY INCIDENT RESPONSE

A. OVERVIEW

Government organizations increasingly need the ability to handle computer security incidents. A computer security incident is any event in which a computer system is attacked, intruded into, or threatened with an attack or intrusion. Thus, examples of computer security incidents include viruses, worms, Trojan horses, hacker events, hoaxes, and extortion.

The primary activity of an incident response team is to provide assistance to sites when such aid is requested. This help includes assessing the nature and extent of damage to computer systems, coordinating technical efforts to develop and collect software 'patches' for problem resolution, advising site personnel on damage control and recovery procedures, and providing direct support on computer security-related problems.

It should be noted that other organizations provide incident response support. The activities of these organizations should be considered in developing the organization's computer security incident response capability. Based on this consideration, some of the tasks described in this SOW may be optional. This may be especially true for a small organization with limited resources. See NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC) for further information.

This SOW presumes the organization has made a determination that a centralized approach to computer security incident response will be used. The above NIST Special Publication can be useful in determining the appropriate placement of this capability within the organization.

See Appendix E (Computer Security Incident Response) for further information prior to doing the SOW described below.

SAMPLE STATEMENT OF WORK

B. INCIDENT RESPONSE TEAM

PURPOSE/OBJECTIVE

The purpose of this SOW is to form a Contractor Incident Response Team to provide virus and incident response capability to support **<organization name>**. This will include incidents such as viruses, worms, or other malicious code, intrusions, hoaxes and insider attacks. This team, when requested by an **<organization name>** site, will also assist in analyzing any unusual or unexplained event that may involve computer or network security.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor will form an Incident Response Team (the team) to increase the **<organization name>**'s ability to respond to computer security incidents. The team will provide **<N>** hours a day on-call technical assistance to **<organization name>** sites and respond to incidents at those sites within **<N>** hours. The team will also communicate important information about threats and vulnerabilities to the organization in a timely manner.

The team charter will involve proactive efforts. These include developing incident handling guidelines, identifying software tools for responding to incidents/events, and conducting training and awareness activities.

The team may also perform research on viruses, conduct system attack studies, and develop computer security tools. These efforts will provide knowledge that the team can use and information to issue before and during incidents. In addition, the team will maintain a clearinghouse of relevant information and help sites learn about and use the computer security tools which they have developed.

This project is responsible for specific deliverables (e.g., incident-handling guidelines, software tools, etc.). The project is an on-going, multi-year effort. The team will identify, isolate, neutralize and be responsible for handling malicious programs (viruses, worms, Trojan Horses) infecting **<organization name>** systems and/or networks.

TASK DESCRIPTIONS

(NOTE: Some of the following tasks are independent of the others. All of them may not be necessary in a particular environment. Each task should stand on its own merits, considering organization requirements, resources and the sensitivity of the activity.)

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Establish Incident Response Team

The Contractor shall form an Incident Response team (the team) to provide direct technical assistance. This aid shall include on-site presence at the **<organization name>**'s sites request. The objective is for the team to provide to every site requesting aid, sufficient support to solve the technical problems created by the incident.

The team shall establish and maintain an office at **<organization name>** headquarters that will be the center for conducting team activities. The center shall also house the computers and other hardware needed to handle communications with other sites.

Task 3 - Establish a Clearinghouse

The team shall develop a clearinghouse for **<organization name>** to locate pertinent information about previous incidents, known viruses and worms, known vulnerabilities of systems, and key people to contact. This clearinghouse shall include information about security clearances needed by key computer security and technical personnel at each site. The team shall develop an automated tracking system to track incidents.

The Contracting Officer's Technical Representative (COTR) will review the Automated Tracking System and Clearinghouse.

Task 4 - Develop Cooperative Procedures

At the organizations's discretion, the team shall form cooperative procedures between **<organization name>** and other federal organizations. Part of the team's task shall be to develop procedures for incident reporting. These procedures define who is contacted during an incident, what kind of information is shared, who performs a particular task, and how subtasks are divided under different types of incidents and conditions. The team shall develop cooperative relationships with vendors to learn of security holes and fixes. The team shall also work with vendors to ensure problems are fixed. The Contractor shall document these cooperative procedures which will be included in the Incident Handling Guidelines, described in Task 5 below.

The Contractor shall deliver the Cooperative Procedures Report to the COTR.

Task 5 - Develop Guidelines for Incident Handling

The team shall develop guidelines for incident handling that both the team and technical personnel at the **<organization name>** sites can follow. These guidelines shall include managerial as well as technical guidance for event handling and the Cooperative Procedures Report developed in Task 4. The team shall define what an incident is and conditions under which the team becomes involved. These guidelines shall be consistent with the **<organization name>** policy. These guidelines shall also contain the necessary details to solve technical problems, conduct coordinated efforts, and preserve evidence important to follow-up prosecution. Finally, these guidelines shall help those involved in incident handling to categorize events and prioritize responses to those incidents/events.

The Contractor shall deliver the Incident Handling Guidelines to the COTR.

Task 6 - Develop Electronic Communications Capabilities

The team shall establish electronic communications capabilities with **<organization name>** sites, so the team can send and receive electronic mail from numerous sites, send and receive patches and technical data, etc. This implies that the team shall have to establish controls on dissemination of sensitive and privileged information. There shall be no open access to any information the team encounters.

Task 7 - Identify Software Tools for Incident Handling

The team members shall determine the types of software tools which can ease the incident handling process. Tools include anti-viral programs, intrusion monitoring, detection and recording capabilities, incident analysis and reverse engineering tools, and real-time notification. The Contractor shall write a report on the tools' capabilities. This report shall include recommendations on which tool, if any, would be the most cost-effective to aid incident handling by **<organization name>.**

The Contractor shall deliver the report on Software Tools to Handle Incidents to the COTR.

Task 8 - Conduct a Training and Awareness Function

The team shall cooperate with the **<organization name>** to conduct workshops/training seminars. These activities shall require the team to develop demonstrations of viruses and eradication methods. The team shall also circulate information about useful software tools to aid in incident handling.

The COTR will receive the Workshop/Training Seminars Outline and Schedule. The Contractor shall coordinate the dates and places of the Workshops/Training Seminars with the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Automated Tracking System and Clearinghouse	<X> *
Cooperative Procedures Report	<X> *
Incident Handling Guidelines	<X> *
Software Tools to Handle Incidents Report	<X> *
Outline of Proposed Workshop/Training Seminars	<X> *
Workshop/Training Seminars Outline and Schedule	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

VII. SPECIAL STUDIES/PRODUCT EVALUATION

A. OVERVIEW

Federal security managers find need to evaluate products from a computer security perspective. These products may be ADP products or computer security-related products. They may be hardware, software, or firmware. The products may be ones that they are currently using or ones that they are considering.

Organizations are experiencing logistical and technical changes in their ADP environment. These changes include the proliferation of distributed processing, networks, and microcomputers. Continuity of organization security controls throughout the implementation of new products and services must be assured. Complete reviews and approval by the organizational security manager in advance of procurement or development is a control for ensuring continuity of an organization's security program.

Federal security managers need to determine how the products they are using or considering relate to organizational requirements for computer security.

There are three specific areas of concern reflected in the SOWs in this section. The first area is the impact on computer security when implementing ADP products on existing organization systems. This SOW looks at gauging the impact when introducing technology such as an OSI-compatible local area network or wide area network, a new type of mass storage media, a database management system, or an office automation or electronic mail package.

The second area measures the impact of a hardware or software product designed to perform a direct computer security function. Examples of this include a virus scanning package, a PC-based access control package, a mainframe access control system, an accounting add-on to an operating system, an encryption device, or a smart card-based identification and authentication system.

The third area examines a product to be used as a computer security management aid. A SOW for evaluating a risk management product serves as illustration.

(NOTE: The term "evaluation" in the SOWs below is not being used in the same sense as in a formal evaluation performed by the National Computer Security Center as part of its Trusted Product Evaluation Program. NCSC maintains an Evaluated Products List (EPL) for those products that have been determined to satisfy specific security criteria (i.e., evaluated against NCSC's Trusted Computer Systems Evaluations Criteria - the Orange Book). Each new piece of software or hardware needs to be tested and evaluated in the environment in which it will be operating before being placed in production. Products on the EPL are usually only evaluated in a stand-alone environment. While inclusion of a product on the EPL is not a substitute for environmentally testing new hardware and software, understanding the evaluation process may provide useful information in performing the SOWs below. Contact NCSC for further information on the Trusted Product Evaluation Program.)

SAMPLE STATEMENT OF WORK

B. SECURITY EVALUATION OF AN ADP PRODUCT

PURPOSE/OBJECTIVES

The purpose of this SOW is to evaluate the impact of implementing and using **<product name>** by this organization on existing security controls.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor reviews the organization security plan and requirements for the product. The Contractor evaluates **<product name>**'s ability to meet the stated application function(s) and security requirements as well as the computer security impacts of the package on the computer system.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Organization Security Plan and Requirements for an ADP Product

The Contractor shall review the **<organization name>** security plan, emphasizing existing controls, and the stated requirements for the **<product name>**. Based on this, the Contractor shall develop a report on the potential security implications of installing the needed capability. The report shall identify those areas of concern which require more in-depth examination.

The Contractor shall deliver a Security Plan/Requirements Review Report to the Contracting Officer's Technical Representative (COTR).

Task 3 - Evaluate the Product to Determine Security Features

The Contractor shall determine the security features of the **<product name>** and/or its interfaces with other security products on the system. When appropriate, this may require direct contact with **<product name>** vendor's representative. Although purchase of the product may be necessary, obtaining an evaluation copy on a trial basis may be preferable. The Contractor shall also ensure that the product conforms to relevant existing federal standards. The Contractor shall draft a report on the security features of the product.

The Contractor shall deliver a Product Measurement Report to the COTR.

Task 4 - Recommendations and Implementation Plan

The Contractor shall prepare a recommendations report on whether or not **<product name>** will meet the organization requirement. Recommendations shall be based on cost, response time, ease of use, ease of implementation and operation, customer support, and quality of documentation. If the recommendation is positive, the Contractor shall prepare a plan for implementing **<product name>** supporting the organization security objectives. The plan should describe how the objectives are met throughout the implementation process.

The Contractor shall deliver the Recommendations and Implementation Plan Report to the COTR.

(NOTE: Updating the organization security plan is a necessary activity, however its inclusion in this SOW is optional.)

Task 5 - Security Plan Update (if necessary)

The Contractor shall draft the update to the **<organization name>** computer security plan incorporating the use of **<product name>.**

The Contractor shall deliver an updated **<organization name>** Computer Security Plan to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLES	DUE DATE
Work Plan Development	<X> *
Requirements/Security Plan Review Report	<X> *
Product Evaluation Report	<X> *
Recommendations and Implementation Plan Report	<X> *
Updated Computer Security Plan	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

C. EVALUATION OF HARDWARE/SOFTWARE PRODUCTS THAT PERFORMS A DIRECT COMPUTER SECURITY FUNCTION

PURPOSE/OBJECTIVE

The purpose of this SOW is to evaluate computer security products. The products provide assistance in **<computer security function>** for the organization.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor evaluates one or more automated products for **<organization name>**, based on organization needs. The Contractor then demonstrates the product(s) and recommends the product(s) for organization use or rejects it as not suitable.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Organization Requirements and Available Products

The Contractor shall review the organization's computer security plan and the requirement for a **<type of computer security product>** computer security product. The review shall document the capabilities that would be most appropriate to meet organization needs. The Contractor shall also assemble a list of the type of products designed for these needs. This list shall include a short general description of each product.

The Contractor shall deliver a Product Requirements Report and Possible Products List to the COTR.

(NOTE: If the organization does not have a specific type of computer security product in mind, the following should be included:

When the report is approved, the Contractor shall submit for approval a list of products to be evaluated in Task 3. The **<organization name>** will select **<N>** products for further evaluation.)

Task 3 - Evaluate Available Products

For each product identified in Task 2 as requiring further evaluation, the Contractor shall obtain a working or demonstration copy of the product to test its capabilities. When appropriate, this may require direct contact with **<computer security product name>** vendor's representative. Although purchase of the product may be necessary, obtaining an evaluation copy on a trial basis may be preferable. The Contractor shall also ensure that the product conforms to relevant existing federal standards.

The report shall address the computer security functions performed by the **<computer security product>**. It shall also address data collection capabilities, utility (e.g., ease of use, error messages, documentation quality), security controls, reporting capabilities, product support, and compatibility with the organization's other computer security products and procedures. The Contractor shall prepare a report documenting advantages and disadvantages of each product.

The Contractor shall deliver a Product Evaluation Report to the COTR.

Task 4 - Demonstration and Recommendations

The Contractor shall conduct a demonstration of each identified computer security product and emphasize the advantages and disadvantages in the evaluation report. The Contractor shall recommend a product or product(s) and a plan for implementation. Recommendations shall be based on the product's ability to meet specific organization security requirements, as well as cost, response time, ease of use, ease of implementation and operation, customer support, quality of documentation, and output reports.

The Contractor shall deliver a Recommendations Report to the COTR.

(NOTE: While identification of the advantages and disadvantages of each identified computer security product, is required, demonstration of each product is optional.)

Task 5 - Security Plan Update (if necessary)

The Contractor shall draft an update to the **<organization name>** computer security plan. It will include references to the product's use and the implementation plan.

The Contractor shall deliver a Security Plan Update to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLE	DUE DATE
Work Plan Development	<X> *
Product Requirements Report and Possible Products List	<X> *
Product Evaluation Report	<X> *
Recommendations Report	<X> *
Security Plan Update	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

D. EVALUATION OF A COMPUTER SECURITY MANAGEMENT AID: A RISK MANAGEMENT TOOL

PURPOSE/OBJECTIVE

The purpose of this SOW is to evaluate one or more automated risk management products. These products provide aid in the risk management and security planning required for the organization.

ENVIRONMENT

(NOTE: See Appendix H for sample text for environment considerations.)

REFERENCES

The Contractor shall perform the tasks described below according to the following references: *(NOTE: See Appendix E for the applicable references and include specific* **<organization name>** *directives.)*

SCOPE OF WORK

The Contractor evaluates one or more automated products for **<organization name>**, based on organization needs. The Contractor then demonstrates the product and recommends the product for organization use or rejects it as not suitable.

TASK DESCRIPTIONS

Task 1 - Work Plan Development

(NOTE: Appendix F contains a sample work plan development task statement.)

Task 2 - Review Organization Requirement and Available Products

The Contractor shall review the organization's computer security plan and the requirement for an automated risk management product. The review shall document the capabilities that would meet organization needs. The Contractor shall also assemble a list of products designed for these needs. This list shall include a short general description of each product. *(NOTE: If the organization has a specific product in mind, then no list is required for Task 2. The product in mind is named at this point.)*

The Contractor shall deliver an Organization Requirements Report to the COTR.

(NOTE: If the organization does not have a specific product in mind, the following should be included:

When the report is approved, **<organization name>** will select **<X>** products for further evaluation.)

Task 3 - Evaluate Available Automated Products

For each product identified in Task 2, the Contractor shall obtain a working or demonstration copy of the product and evaluate its capabilities. When appropriate, this may require direct contact with **<risk management product>** vendor's representative. Although purchase of the product may be necessary, obtaining an evaluation copy on a trial basis may be preferable. The Contractor shall prepare a report documenting advantages and disadvantages of each product. The report shall address whether the risk analysis is quantitative, qualitative, or both. It shall cover the soundness of the underlying methodology used by the product. It shall also address data collection capabilities, utility (e.g., ease of use, clarity of error messages, and documentation quality), security controls, reporting capabilities, product support, and compatibility with the organization's computer security products and procedures.

The Contractor shall deliver a Product Evaluation Report to the COTR.

Task 4 - Demonstration and Recommendations

The Contractor shall conduct demonstrations of each identified product and emphasize the advantages and disadvantages in the evaluation report. The Contractor shall recommend a product(s) and a plan for implementing the recommended product(s). Recommendations shall be based on the product's ability to meet organization security requirements, as well as soundness of the underlying methodology, cost, response time, ease of use, ease of implementation and operation, customer support, quality of documentation, and output reports.

The Contractor shall deliver a Recommendations Report to the COTR.

(NOTE: Updating the organization security plan is a necessary activity, however its inclusion in this SOW is optional.)

Task 5 - Security Plan Update (if necessary)

The Contractor shall draft an update to the **<organization name>** computer security plan. It shall include references to the product's use and the implementation plan.

The Contractor shall deliver a Security Plan Update to the COTR.

DELIVERABLES

(NOTE: See Appendix G for a sample text on SOW deliverables. In all cases, consult the Contracting Officer.)

DELIVERABLE	DUE DATE
Work Plan Development	<X> *
Organization Requirements Report	<X> *
Product Evaluation Report	<X> *
Recommendations Report	<X> *
Security Plan Update	<X> *

* (working days from the beginning of the contract or from the previous milestone, as determined by the organization)

REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER

(NOTE: Suggested statements for reporting requirements, technical contacts, and other are in Appendix B. Some organizations have their own guidelines for these sections and the Contracting Officer should be consulted.)

APPENDICES

APPENDIX	CONTENT
A	ANNOTATED REFERENCES
B	SAMPLE TEXT FOR REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER IN A SOW
C	ALTERNATE TEXT FOR REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER IN A SOW
D	SAMPLE JOB DESCRIPTIONS
E	COMPUTER SECURITY AREA AND SOW-SPECIFIC REFERENCES
F	SAMPLE WORK PLAN DEVELOPMENT TASK STATEMENTS
G	SAMPLE TEXT ON SOW TASK DELIVERABLES
H	SAMPLE TEXT ON ENVIRONMENT CONSIDERATIONS FOR SOWs
I	SUMMARY TASK LIST OF SOWs

APPENDIX A:
ANNOTATED REFERENCES

FEDERAL LAWS

BROOKS ACT (Pub. L. 89-306)

This law directed the Administrator of the General Services Administration (GSA) coordinate and provide for the economic and efficient purchase, lease, and maintenance of automated data processing equipment by Federal agencies. The Brooks Act authorized the Department of Commerce (DOC) to establish standards, to conduct research, and to provide scientific and technological advisory services. The Act also charged the Office of Management and Budget (OMB) with fiscal control and the development of administrative and management policy. OMB Circular A-130, Management of Federal Information Resources, implements provisions of the Brooks Act. This Act is the primary law controlling the acquisition of automated data processing (ADP) and telecommunications resources.

Significant amendments to the Brooks Act were made in the Paperwork Reauthorization Act and the Computer Security Act of 1987.

PAPERWORK REDUCTION ACT (Pub. L. 96-511)

This law was enacted to reduce the paperwork burden on the public and to enhance the economy and efficiency of the government and the private sector by improving federal information policymaking. This law requires each agency designate a senior information resources management official who is responsible for Brooks Act acquisitions. OMB's Office of Information and Regulatory Affairs (OIRA) was established and made responsible for implementing the Act. GSA was designated to advise and assist OMB in triennial reviews of information management activities of each agency. This law defined automated data processing equipment (ADPE) to exclude some types of data and telecommunications equipment (later referred to as the "Warner Amendments").

WARNER (ASPA) AMENDMENT (Pub. L. 97-86)

This amendment to the Armed Services Procurement Act exempted the Department of Defense (DoD) from the Brooks Act for certain applications. These involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment integral to a weapon or weapons systems, or critical to fulfillment of military or intelligence missions. (See secs. 111(a)(2) and (3) for the Federal Property and Administrative Services Act for complete definition and exceptions.)

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT OF 1982 (Pub. L. 97-225)

This law enacted the main provisions of OMB Circular A-123. Its purpose is to ensure that agencies maintain effective systems of accounting and administrative controls against fraud, waste and abuse.

PAPERWORK REAUTHORIZATION ACT OF 1986 (Pub. L. 99-500)

This law clarified the Brooks Act definition of "ADPE" to include telecommunications, ADP services and support services. This law gave permanent protest jurisdiction to the GSA Board of Contract Appeals (GSBCA). Implementation of this law in the Federal Information Resources Management Regulation (FIRMR) resulted in the adoption of the term "Federal Information Processing (FIP) Resources" to encompass all resources defined by the Brooks Act amendment.

COMPETITION IN CONTRACTING ACT (Pub. L. 98-369)

This law emphasized competition in acquisitions, established exceptions to full and open competition, provided legislative authority for Government Accounting office (GAO) protest functions, and authorized GSBCA to resolve ADP protests on a pilot basis.

COMPUTER SECURITY ACT OF 1987 (Pub. L. 100-235)

This law amends the NBS Organic Act of 1901, Federal Property and Administrative Services Act of 1949 and Brooks Act of 1965 to add provisions on the protection of computer-related assets (e.g., hardware, software, and data). This Act:

- assigns responsibility of development of computer security guidelines and standards to the NIST;
- requires federal agencies identify existing and under development systems that contain sensitive information;
- requires development of a security plan for each identified sensitive computer system; and
- requires mandatory periodic training in computer security awareness and accepted computer security practice of all employees involved with the management, use, or operation of federal computer systems within or under the supervision of a federal agency.

Current instructions for implementing the Computer Security Act are provided in OMB Bulletin 90-08, Guidance for the Preparation of the Security Plans for Federal Computer Systems that Contain Sensitive Information.

PRIVACY ACT OF 1974 (Pub. L. 93-579)

This law was enacted to provide for the protection of information related to individuals maintained in federal information systems, and to grant access to such information by the individual. The law establishes criteria for maintaining the confidentiality of sensitive data and guidelines for determining which data are covered.

OMB Circular A-130 implements provisions of this act. FIPS PUB 41 provides computer security guidelines for implementing the act.

COPYRIGHT ACT OF 1980 (17 USC)

This law amends the copyright laws to recognize the realities of modern data processing systems. Section 117 permits copying of copyrighted software for backup or archival

purposes if a copy is required to install the software.

TRADE SECRETS ACT (18 USC 1905)

This law establishes specific penalties for the improper disclosure of trade secrets entrusted to government agencies.

PATENT AND TRADEMARK LAWS (31 USC)

This law applies when an application contains or uses patented software, users have a responsibility to protect the rights of the patent holder. Specifically, the user must ensure that the patented software is not improperly disclosed, used, or copied.

ELECTRONIC COMMUNICATIONS PRIVACY ACT (Pub. L. 99-508)

This law provides for the protection of transmissions of various communications technologies.

COUNTERFEIT ACCESS DEVICE AND COMPUTER FRAUD AND ABUSE ACTS (Pub. L. 98-473, Pub. L. 99-474)

These laws established computer related crime as an offense with specific penalties.

PUBLIC PRINTING AND DOCUMENTS ACT (44 USC 33)

This law established procedures for the proper disposal of records.

COMPUTER MATCHING AND PRIVACY PROTECTION ACT (Pub. L. 100-503)

This law established procedures to ensure the accuracy of computer matching programs.

FREEDOM OF INFORMATION ACT (Pub. L. 90-23)

This law makes federal information readily available to the public. It also establishes the conditions under which information may be withheld form the public to ensure that certain information such as trade secrets be protected.

FEDERAL REGULATIONS

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR 1-51)

The Federal Acquisition Regulation is the primary regulation used by federal agencies for acquisition of supplies and services with appropriated funds.

FEDERAL INFORMATION RESOURCES MANAGEMENT REGULATION (FIRMR) (41 CFR 101)

The FIRMR governs the acquisition, management, and use of federal information processing (FIP) resources (commonly referred to as ADPE or telecommunication resources). The FIRMR relies on the FAR's general policies and procedures and contains policies and procedures

that are in addition to, or take precedence over, the FAR. If the FAR and FIRMR conflict, the FIRMR normally prevails.

OPM REGULATIONS

The Office of Personnel Management's (OPM) regulation (5 CFR 930) requires training for all employees involved in the management and use of federal computer systems that process sensitive information.

OPM's Federal Personnel Manual (Ch. 731, 732, and 736) establishes policy on position sensitivity, personnel screening procedures, adjudication, and security investigations.

OMB CIRCULARS

OMB CIRCULAR A-123
INTERNAL CONTROL SYSTEMS

OMB Circular-123 has specific policies and standards for federal agencies for establishing and maintaining internal controls in their programs and administration activities. This includes requirements for vulnerability assessments and internal control reviews. The main provisions of A-123 became law through the enactment of the Federal Manager's Financial Integrity Act of 1982.

OMB CIRCULAR A-127
FINANCIAL MANAGEMENT SYSTEMS

OMB Circular A-127 has specific policies and standards for federal agencies for establishing and maintaining internal controls in financial management systems. This includes requirements for annual reviews of agency financial systems which build on reviews required by OMB Circular A-123.

OMB CIRCULAR A-130
MANAGEMENT OF FEDERAL INFORMATION RESOURCES

OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, has specific requirements for establishing the agency computer security program. The program should include application security, personnel security, information technology installation security, and security awareness and training programs. It also assigns responsibilities to: Department of Commerce, Department of Defense, General Services Administration, and Office of Personnel Management. Federal agencies are required to address security in their annual internal control report required under OMB Circular A-123.

CENTRAL AGENCIES

The following organizations have primary authority for overseeing various aspects of federal information processing resources acquisition.

GENERAL SERVICES ADMINISTRATION (GSA)

The Brooks Act placed in GSA the authority and responsibility to acquire ADPE resources. GSA exercises its authorities by delegating procurement authority to other agencies through a formal delegations process. GSA exercises oversight in various ways, including periodic review of agencies' acquisition activities. These reviews can result in raising or lowing the procurement authority delegated to an agency. GSA issues the FIRMR, which contains regulations unique to FIP acquisitions. and related bulletins that provide additional guidance. GSA also publishes a Federal ADP and Telecommunications Standards Index, available through the Government Printing Office.

OFFICE OF MANAGEMENT AND BUDGET (OMB)

The Brooks Act charged OMB with fiscal and policy control for ADP resources. OMB has assigned management functions to GSA.

The Paperwork Reduction Act (and reauthorization) granted OMB broad authority on planning, budgeting, organizing, directing, training, promoting, controlling, and other managerial activities involving the collection, use, and dissemination of information.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST, formerly the National Bureau of Standards (NBS), is an agency of DOC. The Brooks Act makes NIST responsible for providing scientific and technological services to agencies for ADP and for developing and maintaining standards to increase agencies' ability to share computer programs and data. The FIPS PUBS are published by NIST for this purpose. The Computer Security Act of 1987 amends several laws to add an acquisition provision, relating to the protection of computer-related assets (e.g., hardware, software, and data). The Act also assigned responsibility for the development of computer security guidelines and standards to the NIST.

NATIONAL COMPUTER SECURITY CENTER (NCSC)

The National Security Agency's NCSC: develops and publishes criteria and guidelines for the development, evaluation, and use of trusted information processing systems; works with industry to assist in the development of trusted commercial information processing products and evaluates the resulting products; works with NIST in developing a coherent U.S. approach to computer and information security standards; provides computer security assistance in cooperative efforts with NIST under the Computer Security Act, to other government departments and agencies; and promotes information security and awareness education through cooperative efforts, public seminars and other forums.

APPENDIX B:
SAMPLE TEXT FOR REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER IN A SOW

The sample text in this appendix should be included in each SOW in the Reporting Requirements, Technical Contact, and Other sections. The contents of each section will need to reflect the requirements of the specific task as well as the standardized requirements provided by organization contract personnel. The sample text provided below is applicable to most SOWs. Alternative text and considerations for revising the contents of these sections are in Appendix C. In all cases, consult the Contracting Officer.

REPORTING REQUIREMENTS

Progress Reports

The Contractor shall prepare and submit monthly progress reports. Progress reports shall be submitted to the **<Contracting Officer's Technical Representative (COTR)>** within 5 days after the end of the month reporting period. Progress reports shall discuss the status of all on-going work about specific tasks listed in the SOW. At a minimum, each progress report shall contain:

- o a description of:
  - work performed during the reporting period just ended;
  - work to be performed during the next reporting period;
  - any planned travel including travel objectives;
  - any problems encountered with corrective action proposed or taken and a statement about the potential impact of the problem; and
  - any government action requested;
- o an estimate of the percent complete for each task; and
- o cost reimbursable or time and materials tasks only, the hours and funds expended to-date and for the reporting period just ended.

Meeting Minutes

The Contractor shall maintain minutes of meetings during which the progress of the work is discussed. The Contractor shall submit the meeting minutes to the COTR within **<N>** working days after the subject meeting. The meeting minutes shall highlight any decisions reached, agreements made, or actions to be taken.

Exception Reports

The Contractor shall prepare and submit an exception report describing any problems encountered that may impact the government adversely, require clarification or action by the government, require documentation, or result in a deviation from the approved work plan.

TECHNICAL CONTACT

The COTR for this effort is **<Name, Address, and Phone Number>.**

OTHER

Contractor Personnel Requirements

Contractor personnel assigned to this effort shall have appropriate **<background screening/security clearance>** up to **<screening level/-security clearance level (Secret, Top Secret)>.**

The Contractor shall propose staff for assignment to this effort using the skill categories contained in Appendix D.

(NOTE: A security clearance level specification should be consistent with the information sensitivity designation and required type of background investigation.)

Travel

The Contractor **<shall/shall not>** be required to travel to sites beyond a 50 mile radius of the location identified by the COTR.

Government-Furnished Equipment (GFE)/Government-Furnished Materials (GFM)

No GFE shall be provided. Documentation relevant to the specified tasks will be provided or made available as appropriate.

APPENDIX C:
ALTERNATE TEXT FOR REPORTING REQUIREMENTS, TECHNICAL CONTACTS, AND OTHER IN A SOW

REPORTING REQUIREMENTS

Reporting requirements imposed on a Contractor should be sufficient to provide adequate information for monitoring task progress without being burdensome. Preparing reports is a project cost and should be realistic to the overall project cost and complexity.

Regular monthly progress reports augmented by exception reports and meeting minutes are usually enough for most projects. Where more frequent reporting is desired, one of the following may be appropriate:

- The Contractor shall prepare and submit brief (not more than two pages) weekly progress reports. The progress report shall describe the status of each task identified in the SOW and any problems and corrective action proposed or taken. The progress report shall be submitted to the COTR on the first work day following the end of the week.
- The Contractor shall provide **<weekly/biweekly>** oral progress reports to the COTR. Oral progress reports may be made in person or by telephone. Oral progress reports shall include a discussion of the status of each task identified in the SOW, any problems encountered, and corrective actions proposed or taken.

Travel

Many computer systems and applications support or are used by staff in remote locations. Site visits are generally required to remote sites to review security arrangements and evaluate the impact on overall system/application security of the remote location. Since travel to sites can be a significant cost, the following techniques should be considered instead of visits to each site:

- data collection by questionnaire;
- site visits to a sample of sites; and
- questionnaires and selected site visits.

If site visits are required, one of the following should be included in the SOW:

- For each site, the Contractor shall conduct an entrance and an exit briefing. Each briefing shall be no more than 1 hour in duration. The entrance briefing shall provide site personnel with information describing the objective of the site visit and the work to be performed. The exit briefing shall provide site personnel with information about the work completed at the site.
- The Contractor shall coordinate all site visits with the Point of Contact (POC) for each site provided by COTR to ensure compliance with site-specific security requirements.

Government-Furnished Equipment (GFE)/Government-Furnished Materials (GFM)

In some instances, it is appropriate to provide the Contractor with government space and equipment. Instances where such action may be appropriate include:

- o long-term efforts where on-site Contractor support will result in lower costs; and
- o classified or other highly sensitive environments where it may not be practical or efficient to permit duplication or removal of material from the government location.

In some instances, documents may be included in the GFM section. This is a partial list of documents the government may provide:

- o organizational charts;
- o legislation, regulations, orders, directives, and other publications that affect the organization's operations;
- o long and short-range plans;
- o minutes of meetings of the data processing steering committee;
- o schematic of hardware and network environment;
- o inventory of hardware and system and application software;
- o systems development life cycle methodology;
- o program change procedures;
- o data and computer security procedures;
- o backup and contingency plan documents;
- o system flowcharts showing the jobs, programs, input, major processing modules, and outputs;
- o narratives describing the application;
- o design specifications;
- o user guides;
- o operation run instructions including input, processing, and output requirements; error messages and required operator actions; and, restart and recovery instructions;
- o descriptions or critical files and their data elements;
- o prior audit reports (if any); and
- o previously issued management reports about this application.

APPENDIX D:
SAMPLE JOB DESCRIPTIONS

This section presents suggested skill categories for contractor staff assigned to support a task(s) defined in a SOW.

Automated Information Systems (AIS) Security Project Manager

The AIS Security Project Manager (AISSPM) independently performs or leads one or more project teams in performing risk analysis and security audit services. The AISSPM independently develops or supervises the development of analytical reports and other products specified in a SOW.

AIS Senior Security Analyst

The AIS Senior Security Analyst (AISSSA) leads a team in performing risk analysis and security audit services. The AISSSA independently develops or supervises the development of analytical reports and other products specified in a SOW.

AIS Security Analyst

The AIS Security Analyst (AISSA) independently performs risk analysis and security audit services. The AISSA develops analytical reports and other products specified in a SOW.

AIS Technical Assistant

The AIS Technical Assistant (AISTA) provides help to AIS security team members in data collection, data analysis, and report preparation.

Technical Subject Matter Specialist

The Technical Subject Matter Specialist (TSMS) applies principles, methods, and knowledge of a particular area of expertise to specific project task requirements. The TSMS augments project teams, in support of the project leader, by providing technical knowledge and analysis of highly specialized applications and operational environments. Technical support may include technical advice on security requirements for highly specialized AIS applications, technical report preparation, or other services specified in a SOW.

AIS Specialist

The AIS Specialist (AISS) provides specialized aid on problems requiring in-depth knowledge of a specialized AIS discipline (e.g., AIS systems software, database management, office automation, AIS hardware specialist, and AIS data communications). The AISS augments project teams, in support of the project leader, by providing technical knowledge and analysis of highly specialized and complex security problems. Technical support may include designing controls, implementing secure data communication networks, preparing technical reports, or other services specified in a SOW.

Analyst/Programmer

The Analyst/Programmer (A/P) performs assigned portions of studies. The A/P participates in all phases of study development and production, with emphasis on performing the less complex aspects of information gathering, analysis, and programming. The A/P collects data via manuals, publications, personal interviews, etc. applying to the activities of data, software, hardware, communications, and personnel. The A/P compiles data collected in various compositions such as checklists, survey formats, various worksheets and reports, and will then analyze the data. The A/P applies standard business and data manipulation principles and methods to technical problems to arrive at automated solutions. The A/P is skilled in programming and canned software packages. The A/P designs and prepares technical reports and related documents, and draws charts and graphs to record results. The A/P prepares and edits AIS documentation incorporating information provided by **<organization name>**, specialist, analyst, programmer, and operations personnel. The A/P also writes, edits, and graphically presents technical information for technical and non-technical personnel.

Technical Editor

The Technical Editor (TE) helps to prepare, review, and edit formal reports to ensure that they are well-written, grammatically correct, and follow a format specified in a SOW.

Graphics Specialist

The Graphics Specialist (GS) prepares formal technical security drawings, graphics, and illustrations (e.g., graphics for facility security profiles, AIS training aids and materials, presentation viewgraphs and slides, flow charts, floor plans, and other related material) specified in a SOW.

Technical Typist

The Technical Typist (TT) provides clerical and typing support to the AIS security team members. The TT types, copies, and binds formal reports.

AIS Training Specialist

The AIS Training Specialist (AISTS) works with AIS security content specialists and managers to design, implement, and evaluate platform training programs, computer-based training packages, and interactive video training systems in AIS security awareness and techniques.

APPENDIX E:
COMPUTER SECURITY AREA AND SOW-SPECIFIC REFERENCES

The following are federal requirements or guidance used as references for each SOW. These are the basic references used to ensure that the tasks conducted, recommendations made, and products delivered are consistent with government requirements. These references are not intended to be all inclusive. Individual organization computer security directives should be identified, added to a SOW, and complied with, where applicable. For a description of many of the references listed below, please see Appendix A. See note at the end of this section regarding definition and usage of computer security terms.

The following abbreviations are used:

- FIPS PUB - Federal Information Processing Standards Publication
- NBS - National Bureau of Standards
- NBSIR - National Bureau of Standards Information Report
- NCSC - National Computer Security Center
- (N)CSL - (National) Computer Systems Laboratory
- NIST - National Institute of Standards and Technology
- NISTIR - National Institute of Standards and Technology Information/Internal Report
- NIST SP - NIST Special Publication
- OMB - Office of Management and Budget
- OPM - Office of Personnel Management
- PCMI - Presidents Council on Management Improvement

SECTION II
COMPUTER SECURITY PROGRAM MANAGEMENT

DEVELOPMENT OF A COMPUTER SECURITY PROGRAM

- Computer Security Act of 1987, (Pub. L. 100-235)
- Privacy Act of 1974, (Pub. L. 93-579)
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- OPM Federal Personnel Manual Chapter 731 (Personnel Suitability) and Chapter 732 (Personnel Security)
- Executive Order 10450, Security Requirements for Government Employment
- NIST SP 500-120, Security of Personal Computers Systems: A Management Guide
- NIST SP 500-133, Technical Assessment: Methods for Measuring the Level of Computer Security
- NBSIR 86-3386, Work Priority Scheme for EDP Audit and Computer Security Review

PROGRAM ASSESSMENT

- FIPS PUB 31, Guidelines for ADP Physical Security and Risk Management
- FIPS PUB 87, Guidelines for ADP Contingency Planning Risk Management

- o FIPS PUB 94, Guideline on Electrical Power for ADP Installations
- o FIPS PUB 112, Standard on Password Usage
- o FIPS PUB 113, Standard on Computer Data Authentication
- o OPM Federal Personnel Manual Chapter 731 (Personnel Suitability) and Chapter 732 (Personnel Security)
- o Executive Order 10450, Security Requirements for Government Employment

SECTION III
APPLICATION SECURITY

COMPUTER SECURITY AND PRIVACY PLAN PREPARATION
(IAW OMB CIR 90-08)

- o Computer Security Act of 1987, (Pub. L. 100-235)
- o OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- o OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
- o OPM Federal Personnel Manual Chapter 731 (Personnel Suitability) and Chapter 732 (Personnel Security)
- o NISTIR 4409, 1989 Computer Security and Privacy Plans (CSPP) Review Project: A First-year Federal Response to the Computer Security Act of 1987 (Final Report), September 1990

CERTIFICATION OF A SENSITIVE SYSTEM

- o OMB Circular A-130, Appendix III, Paragraph 3.a.(1)(2), Security of Federal Automated Information Systems
- o FIPS PUB 73, Guidelines for Security of Computer Applications
- o FIPS PUB 88, Guideline on Integrity Assurance and Control in Database Administration
- o FIPS Pup 102, Guidelines for Computer Security Certification and Accreditation
- o NIST SP 500-109, Overview of Computer Security Certification and Accreditation
- o NIST SP 500-133, Technical Assessment: Methods for Measuring the Level of Computer Security
- o Model Framework for Management Control Over Automated Information Systems, January 1988 PCMI
- o NISTIR 4451, U.S. Department of Commerce: Methodology for Certifying Sensitive Computer Applications

CONTINGENCY PLANNING

- o OMB Circular A-130, Appendix III, Paragraph 3.a.(3), Security of Federal Automated Information Systems
- o FIPS PUB 31, Guidelines for ADP Physical Security and Risk Management
- o FIPS PUB 87, Guidelines for ADP Contingency Planning
- o FIPS PUB 102, Guideline for Computer Security Certification and Accreditation,
- o NBS SP 500-85, Executive Guide to ADP Contingency Planning and Disaster

SENSITIVE/CRITICAL APPLICATION REVIEW (SCAR)

- o OMB Circular A-123, Internal Control Systems
- o OMB Circular A-127, Financial Management Systems
- o OMB Circular A-130, Management of Federal Information Resources
- o FIPS PUB 73, Guidelines for Security of Computer Applications
- o FIPS PUB 101, Guideline for Lifecycle Validation, Verification, and Testing of Computer Software
- o FIPS PUB 102, Guideline for Computer Security Certification and Accreditation
- o FIPS PUB 105, Guideline for Software Documentation Management
- o General Accounting Office (GAO) publications, including:
  - Evaluating Internal Controls in Computer-based Systems (GAO Audit Guide)
  - Review Guide for Federal Agency Accounting Systems
  - Audit Guide for Assessing Reliability of Computer Output
  - Evaluating the Acquisition and Operation of Information Systems

SECTION IV
INSTALLATION SECURITY

RISK ANALYSIS OF A SYSTEM

- o Computer Security Act of 1987, (Pub. L. 100-235)
- o Federal Managers' Financial Integrity Act of 1982, (Pub. L. 97-255)
- o OMB Circular A-130, Appendix III, Paragraph 3.c.(2), Security of Federal Automated Information Systems
- o FIPS PUB 65, Guidelines for Automated Data Processing Risk Analysis
- o NISTIR 4325, U.S. Department of Energy Risk Assessment Methodology, Volumes 1 and 2, May 1990
- o NIST SP 500-174, Guide for Selecting Automated Risk Analysis Tools
- o Automated Risk Management Software Tools, Irene E. Gilbert and Nickilyn Lynch, Computer Systems Laboratory, NIST, 1991

DISASTER RECOVERY AND CONTINUITY OF OPERATIONS PLANNING

- o OMB Circular A-130, Appendix III, Paragraph 3.c.(3), Security of Federal Automated Information Systems
- o FIPS PUB 87, Guidelines for ADP Contingency Planning
- o FIPS PUB 102, Guideline for Computer Security Certification and Accreditation
- o NBS SP 500-85, Executive Guide to ADP Contingency Planning
- o NBS SP 500-134, Guide for Selecting ADP Backup Processing Alternatives

SECTION V
COMPUTER SECURITY AWARENESS AND TRAINING

COMPUTER SECURITY AWARENESS AND TRAINING

- o Computer Security Act of 1987, (Pub. L. 100-235)
- o OMB Circular A-130, Appendix III, Section 3.d Automated Information Systems Security Programs
- o NIST SP 500-169, Executive Guide to the Protection of Information Resources
- o NIST SP 500-170, Management Guide to the Protection of Information Resources
- o NIST SP 500-171, Computer User's Guide to the Protection of Information Resources

- o NIST SP 500-172, Computer Security Training Guidelines
- o OPM Regulation (5 CFR 930)

SECTION VI
COMPUTER SECURITY INCIDENT RESPONSE

INCIDENT RESPONSE TEAM

- o Computer Security Act of 1987, (Pub. L. 100-235)
- o OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- o NIST SP 500-166, Computer Viruses and Related Threats: A Management Guide
- o NIST SP 500-170, Management Guide to the Protection of Information Resources
- o NIST SP, Establishing a Computer Security Incident Handling Capability, 1991
- o Organizing a Corporate Anti-Virus Effort, Alan Fedeli, 1991
- o Security Policy Handbook, P. Holbrook and J. Reynolds, 1991
- o Responding to Computer Security Incidents: Guidelines for Incident Handling, E.E. Schultz, D.S. Brown, and T.A. Longstaff, 1990

SECTION VII
SPECIAL STUDIES/PRODUCT EVALUATION

SECURITY EVALUATION OF AN ADP PRODUCT

- o OMB Circular A-130, Appendix III, Paragraph 3, Security of Federal Automated Information Systems
- o OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
- o Model Framework for Management Control Over, Automated Information Systems, January 1988 PCMI

EVALUATION OF HARDWARE/SOFTWARE PRODUCT THAT PERFORMS A DIRECT COMPUTER SECURITY FUNCTION

- o OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- o OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
- o Model Framework for Management Control Over Automated Information Systems, January 1988, PCMI

EVALUATION OF A COMPUTER SECURITY MANAGEMENT AID: A RISK MANAGEMENT TOOL

- o OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- o OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
- o Model Framework for Management Control Over Automated Information Systems, January 1988, PCMI
- o NIST SP 500-174, Guide for Selecting Automated Risk Analysis Tools

- Automated Risk Management Software Tools, Irene E. Gilbert and Nickilyn Lynch, Computer Systems Laboratory, NIST, 1991

NOTE: For definition and usage of computer security terms, there are several reference sources. These include NISTIR 4659, Glossary of Computer Security Terminology, NCSC-TG-004, Glossary of Computer Security Terms and CSL Bulletin, Bibliography of Computer Security Glossaries, Sept 1990.

Appendix E in Tabular Form

	COMPUTER SECRTY		APPLICATION				INSTALLATION		SEC AWAR	INCIDENT	SPEC ICAL STUDIES/		
	PROGRAM MGT		SECURITY				SECURITY		& TRNG	RESPONSE	PRODUCT EVALUATION		
	Section II		Section III				Section IV		Section V	Section VI	Section VII		
			CSA	Sensitive					Security		Sec Eval	Sec Eval	Sec Eval
	Developmnt	Program	Plan	System	Contingncy		Risk	Disaster/	Awareness	Incident	New ADP	Comp Sec	Managemt
REFERENCE	C/S Pgm	Assessmnt	Preparatn	Certificat	Planning	SCAR	Analysis	Recovery	& Training	Response	Product	Product	Aid
Audit Guide													
Auto RM Tools							X						X
Eval Int Ctls													
EO 10450	X	X											
Fedeli-91										X			
FIPS Pub 31		X			X								
FIPS Pub 41													
FIPS Pub 65							X						
FIPS Pub 73				X		X							
FIPS Pub 87		X			X			X					
FIPS Pub 88				X									
FIPS Pub 94		X											
FIPS Pub 101						X							
FIPS Pub 102				X	X	X		X					
FIPS Pub 105						X							
FIPS Pub 112		X											
FIPS Pub 113		X											
GAO-Aud Gd						X							
GAO-Revu Gd						X							
GAO-Eval A/O						X							
Holbrook										X			
Model Framewk				X							X	X	X
NBSIR 86-3386	X												
Schultz-91										X			
SP 500-85					X			X					
SP 500-109				X									
SP 500-120	X												
SP 500-133	X			X									
SP 500-134					X			X					
SP 500-153				X									
SP 500-166										X			
SP-500-169									X				
SP 500-170									X	X			
SP 500-171									X				
SP 500-172									X				
SP 500-174							X						X
SP CSIRP-drft										X			
NISTIR 4325							X						
NISTIR 4409			X										
NISTIR 4451				X									
OMB Bul 90-08			X								X	X	X
OMB Cir A-123						X							
OMB Cir A-127						X							
OMB Cir A-130	X		X	X	X	X	X	X	X	X	X	X	X
OPM Ch 731	X	X	X										
OPM Ch 732	X	X	X										
PL93-579 PA	X												
PL97-255FMIA							X						
PL100-235CSA	X		X				X		X	X			

APPENDIX F:
SAMPLE WORK PLAN DEVELOPMENT TASK STATEMENTS

The following are examples of work plan development task statements. This would normally be the first task of the SOW. Each organization should tailor it and the SOW to which it applies.

SAMPLE 1

Task 1 - Work Plan Development

The Contractor shall conduct an initial survey to verify system information provided by **<organization name>** and to collect other data necessary to perform the work. Upon completion of the survey, the Contractor shall develop a work plan and present it to the Contracting Officer's Technical Representative (COTR). The work plan shall include the following:

- a statement of the Contractor's approach to the project, including a description of specific procedures, methodology, and techniques employed in performing the **<SOW activity>**;
- a schedule for site visits, the identification of specific organizations and organization staff to be interviewed and the specific elements of information to be gathered during the visits, and an outline to be used for entrance and exit briefings at each site.

The **<organization name>** shall review and approve the plan or return it once for revision. Task 2 shall not begin before plan approval.

SAMPLE 2

Task 1 - Work Plan Development

The Contractor shall provide the Contracting Officer's Technical Representative (COTR) with a detailed work plan. The work plan will detail the methodology employed and the processes (tasks, subtasks, etc.) undertaken by the Contractor, the critical path for each process, the level of effort for each process, and the timelines, project milestones and delivery dates for performance of each task identified in the work plan. In addition, the Contractor shall prepare and deliver to the COTR a presentation of their understanding of the work and the approach and processes provided in the detailed work plan. The Contractor shall provide slides, overheads, handouts, and/or other presentation aids. A copy of the presentation materials shall be provided to the COTR at the presentation.

APPENDIX G:
SAMPLE TEXT ON SOW TASK DELIVERABLES

The following is a sample text on SOW deliverables. In all cases, consult the Contracting Officer.

DELIVERABLES

Most work called for in this SOW involves the submission of documents, papers, reports, slides, etc. to the COTR. To avoid redundancy in the task-specific deliverables that follow, the COTR stipulates that all deliverables required under this contract be prepared and presented according to the following discussion. Deliverables contracted for typically require two iterations: 1) a draft and 2) a final version. The Contractor will submit drafts to the COTR for review and comment by the date agreed upon in the detailed project plan. The Contractor will submit final versions to the COTR within **<X>** days from receipt of written comments. The Contractor shall provide the COTR with one hard copy original of the drafts and one hard copy original and one diskette containing **<organization word processing format>** data file for final versions.

All deliverables submitted under this contract shall be accompanied by a transmittal letter that will identify the contract and the products presented. A copy of each transmittal letter will be forwarded to the Contracting Officer for inclusion in the contract file.

APPENDIX H:
SAMPLE TEXT ON ENVIRONMENT CONSIDERATIONS FOR SOWs

The purpose of the environment section of the SOW is to provide the Contractor sufficient understanding of the context in which the specified tasks are accomplished. This appendix contains sample text which might apply. It may not be necessary to include all the items covered in this appendix in a particular SOW. Some organizations have their own wording or format for this section and the Contracting Officer should be consulted in all cases.

Description of the system to include:

- an organization and mission statement;
- the type and sensitivity of data processed (e.g., financial, personnel, etc.) and how it relates to the daily and overall functioning of the organization;
- a statement on the significance of the system and the impact to the organization if the data is either unavailable, accidentally or without authorization accessed, or modified;
- the geographical location of principal offices, headquarters, and offices where the study will be conducted or where data or systems to be studied reside;
- any pertinent hostile environment (such as, heat, cold, water, etc.) at the geographic locations described above;
- major system components, including hardware (mainframe computer(s), minicomputer(s), microcomputer(s), and local area and wide area network(s)), application and system software, and any supporting network and communications arrangements, whether dedicated or shared, and security packages used;
- the number and types of users (local and remote);
- the number and complexity of computer programs (including language used), databases, and/or files;
- a list of appropriate technical, personnel, administrative, physical, environmental, and telecommunications safeguards;
- statement on the continuity of operation of all information systems that support mission-essential/critical organization functions.

This section should also cover the location, source, and contact for any other information that the Contractor may need to know in order to perform the tasks in the SOW. This includes the results of any previous audits, reviews, studies, certifications, analyses, etc. that address the computer security of the system(s) for which the SOW applies.

APPENDIX I:
SUMMARY TASK LIST OF SOWs

SECTION II
COMPUTER SECURITY PROGRAM MANAGEMENT

Development of a Computer Security Program

Task 1 - Work Plan Development
Task 2 - Review Current Computer Security Status
Task 3 - Develop Framework for the Computer Security Program
Task 4 - Develop Details for Computer Security Program Details/Strategies
Subtask 4A - Develop a Personnel Security Strategy
Subtask 4B - Develop an End User Computer Security Strategy
Subtask 4C - Develop an Application Systems Security Strategy
Subtask 4D - Develop an Information Technology Installation Security Strategy

Program Assessment

Task 1 - Work Plan Development
Task 2 - Review Management Procedures and Controls
Task 3 - Review Physical Security
Task 4 - Review Data Security
Task 5 - Review Operating System Security
Task 6 - Review Application Software Security
Task 7 - Review Personnel Security
Task 8 - Review Network Security
Task 9 - Review Disaster Recovery Plans
Task 10 - Program Assessment Report

SECTION III
APPLICATION SECURITY

Computer Security and Privacy Plan Preparation
(IAW OMB CIR 90-08)

Task 1 - Work Plan Development
Task 2 - Prepare Plan According to OMB Bulletin 90-08

Certification of a Sensitive System

Task 1 - Work Plan Development
Task 2 - Determine Security Requirements
Task 3 - Prepare/Review Statement of Systems Security Requirements
Task 4 - Perform Basic Evaluation of System
Task 5 - Prepare Control Matrix
Task 6 - Prepare Security Certification Report

Task 7 - Prepare Draft Accreditation Decision Statement (Optional)

Contingency Planning

Task 1 - Work Plan Development
Task 2 - Review Installation Risk Analysis and Organization Security Plan
Task 3 - Review Contingency Plans and Critical Processing Scheme
Task 4 - Review Current Emergency Response Procedures
Task 5 - Evaluate Damage Assessment Methods
Task 6 - Review Backup Procedures
Task 7 - Evaluate Disaster Recovery Plan
Task 8 - Prepare a Summary Report
Task 9 - Prepare a Detailed Recommendations Report

Sensitive/Critical Application Review (SCAR)

Task 1 - Prepare a SCAR Work Plan
Task 2 - Perform Data Collection
Task 3 - Prepare SCAR Report

SECTION IV
INSTALLATION SECURITY

Risk Analysis of a System

Task 1 - Work Plan Development
Task 2 - Select Methodology for Risk Analysis (Optional)
Task 3 - Data Collection
Subtask 3A - Establish System Boundaries
Subtask 3B - Value Assets
Subtask 3C - Identify Threats
Subtask 3D - Identify Weaknesses in Current Safeguards Systems
Task 4 - Risk Calculation
Task 5 - Cost-Benefit Analysis Report (Optional)
Task 6 - Safeguards Recommendations (Optional)
Task 7 - Develop a Safeguards Implementation Plan (Optional)

Disaster Recovery and Continuity of Operations Planning

Task 1 - Work Plan Development
Task 2 - Review Installation Risk Analysis and **<Organization Name>** Security Plan
Task 3 - Review Contingency Plans and Critical Processing Scheme
Task 4 - Review Backup Procedures
Task 5 - Review Continuity of Operations/Disaster Recovery Move Plan
Task 6 - Examine Procedures and Practices for Off-site Storage
Task 7 - Disaster Recovery Test Procedures Review
Task 8 - Evaluate ADP Backup Processing Alternatives

Task 9 - Prepare a Summary and Recommendations Report

SECTION V
COMPUTER SECURITY AWARENESS AND TRAINING

Computer Security Awareness and Training

Task 1 - Work Plan Development
Task 2 - Develop Course Outline and Master Lesson Plan
Task 3 - Develop Lesson Plan for Each Audience Category
Task 4 - Conduct Pilot Class
Task 5 - Final Course Materials

SECTION VI
COMPUTER SECURITY INCIDENT RESPONSE

Incident Response Team

Task 1 - Work Plan Development
Task 2 - Establish Incident Response Team
Task 3 - Establish a Clearinghouse
Task 4 - Develop Cooperative Procedures
Task 5 - Develop Guidelines for Incident Handling
Task 6 - Develop Electronic Communications Capabilities
Task 7 - Identify Software Tools for Incident Handling
Task 8 - Conduct a Training and Awareness Function

SECTION VII
SPECIAL STUDIES/PRODUCT EVALUATION

Security Evaluation of an ADP Product

Task 1 - Work Plan Development
Task 2 - Review Organization Security Plan and Requirement for an ADP Product
Task 3 - Evaluate the Product to Determine Security Features
Task 4 - Recommendations and Implementation Plan
Task 5 - Security Plan Update (if necessary)

Evaluation of Hardware/Software Products that Performs
a Direct Computer Security Function

Task 1 - Work Plan Development
Task 2 - Review Organization Requirements and Available Products
Task 3 - Evaluate Available Products
Task 4 - Demonstration and Recommendations
Task 5 - Security Plan Update (if necessary)

Evaluation of a Computer Security Management Aid:
A Risk Management Tool

Task 1 - Work Plan Development
Task 2 - Review Organization Requirement and Available Products
Task 3 - Evaluate Available Automated Products
Task 4 - Demonstration and Recommendations
Task 5 - Security Plan Update (if necessary)

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 4749

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
December 1991

4. TITLE AND SUBTITLE

Sample Statements of Work For Federal Computer Security Services: For Use In-House or Contracting Out.

5. AUTHOR(S)

Dennis Gilbert, Nickilyn Lynch

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
N/A

8. TYPE OF REPORT AND PERIOD COVERED
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

Same as item #6

10. SUPPLEMENTARY NOTES

N/A

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.)

Each federal organization is fully responsible for its computer security program whether the security program is performed by in-house staff or contracted out. Time constraints, budget constraints, availability or expertise of staff, and the potential knowledge to be gained by the organization from an experienced contractor are among the reasons a federal organization may wish to get external assistance for some of these complex, labor intensive activities.

An interagency working group of federal and private sector security specialists developed this document. The document presents the ideas and experiences of those involved with computer security. It supports the operational field with a set of Statements of Works (SOWs) describing significant computer security activities. While not a substitute for good computer security management, organization staff and government contractors can use these SOWs as a basis for a common understanding of each described activity. The sample SOWs can foster easier access to more consistent, high-quality computer security services. The descriptions apply to contracting for services or obtaining them from within the organization.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Computer Security; Computer Security Management; Computer Security Services; Computer Security Services Procurement; Statement of Work

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
97

15. PRICE
A05

ELECTRONIC FORM