Food and Nutrition Service

Electronic Benefits Transfer System Security Guidelines Handbook

Version 6.0

February 2004

Booz | Allen | Hamilton

TABLE OF CONTENTS

1.0 INTRODUCTION 1-1
- 1.1 PURPOSE OF THE GUIDELINE 1-1
- 1.2 SCOPE OF THE GUIDELINE 1-2
- 1.3 ELECTRONIC BENEFITS TRANSFER SYSTEM 1-2
- 1.4 EBT SYSTEM SECURITY ISSUES 1-4
- 1.5 EBT SYSTEM SECURITY REVIEWS 1-4
- 1.6 GUIDELINE ORGANIZATION 1-5

2.0 IT SECURITY CONTROLS 2-1
- 2.1 MANAGEMENT CONTROLS 2-2
  - 2.1.1 EBT SECURITY PROGRAM AND SYSTEM-SPECIFIC POLICY 2-2
  - 2.1.2 EBT SECURITY MANAGEMENT ROLES AND RESPONSIBILITIES 2-3
  - 2.1.3 RISK MANAGEMENT 2-5
- 2.2 OPERATIONAL CONTROLS 2-8
  - 2.2.1 MEDIA PROTECTION 2-8
  - 2.2.2 PERSONNEL SECURITY 2-9
  - 2.2.3 PHYSICAL SECURITY 2-10
  - 2.2.4 CONTINGENCY PLANNING 2-11
  - 2.2.5 INCIDENT RESPONSE 2-12
  - 2.2.6 CONFIGURATION MANAGEMENT 2-13
  - 2.2.7 SECURITY AWARENESS, TRAINING AND EDUCATION 2-14
- 2.3 TECHNICAL CONTROL 2-15
  - 2.3.1 IDENTIFICATION AND AUTHENTICATION 2-15
  - 2.3.2 LOGICAL ACCESS CONTROL 2-16
  - 2.3.3 AUDITING 2-17
  - 2.3.4 INTERNET/WEB SECURITY 2-18
  - 2.3.5 NETWORK SECURITY 2-22
  - 2.3.6 DATABASE SECURITY 2-23
  - 2.3.7 VIRUS PROTECTION CONTROLS 2-24
  - 2.3.8 PENETRATION TESTING 2-25
- 2.4 EBT SPECIFIC CONTROLS 2-26
  - 2.4.1 EBT ACCESS CARD SECURITY 2-26
  - 2.4.2 POS TERMINAL AND ATM SECURITY 2-27

3.0 DEVELOPING A SECURITY PLAN 3-1
- 3.1 SYSTEM IDENTIFICATION 3-1
- 3.2 SENSITIVITY OF INFORMATION HANDLED 3-2
- 3.3 SYSTEM SECURITY MEASURES 3-2
  - 3.3.1 MANAGEMENT CONTROLS 3-2
  - 3.3.2 OPERATIONAL CONTROLS 3-3
  - 3.3.3 TECHNICAL CONTROLS 3-4
  - 3.3.4 EBT SYSTEM-SPECIFIC CONTROLS 3-7

APPENDICES

A1 CHECKLISTS FOR ASSESSING SECURITY CONTROLS A-1

A2 SAMPLE RISK ASSESSMENT A-2

A3 SAMPLE CONTINGENCY PLAN A-3

A4 GLOSSARY A-4

A5 ACRONYMS A-5

A6 REFERENCES A-6

1.0 Introduction

The Electronic Benefits Transfer (EBT) system allows recipients to use their State and Federal benefits at retailers using cards similar to debit cards. The primary function of the EBT System is to deliver government benefits to appropriate recipients in a secure and efficient manner. In response to this nationwide effort, the U.S. Department of Agriculture, Food and Nutrition Service (FNS), has established partnerships with States and is providing funds to assist States in distributing benefits via the EBT System. This assistance also extends to the food store merchants that participate in the food stamp program.

1.1 Purpose of the Guidelines

According to 7 Code of Federal Regulation Seven (7 CFR), Sections 277.18 (p)(2), ADP Security Program***, "State agencies shall implement and maintain a comprehensive ADP Security Program for ADP systems and installations involved in the administration of the Food Stamp Program."*** FNS developed this guideline to assist States in developing security programs that protect EBT Systems. FNS regulations require that certain security controls be incorporated into the EBT System.

The purpose of this guideline is to—

- Provide security policies and procedures for protecting State EBT Systems from potential risks resulting from vulnerabilities and threats
- Assist the senior management of an agency implementing the EBT System to understand the system's overall security posture
- Provide security guidelines for system program managers and security managers involved in developing, implementing, operating, and managing EBT Systems
- Provide the security and system administrators with security controls that should be implemented into EBT Systems and serve as a guideline for conducting system security reviews
- Provide guidelines to security managers for accomplishing security activities that are necessary for obtaining agency management's authorization to approve system operation.
- Provide guidelines for EBT service providers involved in procurement processes to ensure that their products comply with Federal and agency regulations.

This guideline is designed to be modular so individuals involved in the EBT System's life cycle activities can refer to only those sections that apply.

1.2 Scope of the Guidelines

The *EBT Security Guidelines Handbook* outlines the steps that States should take when developing a comprehensive security program. This guideline provides information on security controls that can be incorporated to address the following areas of ADP security required by paragraph (ii) of 7 CFR, as stated above:

- Physical security;
- Equipment security;
- Software and data security;
- Personnel security;
- Contingency planning;
- Designation of and Agency ADP Security Manager; and
- Performing periodic risk assessments.

These security measures are based on Federal security regulations and standards, EBT System documentation, and industry best practices.

1.3 Electronic Benefits Transfer System

An EBT System is a special application of electronic funds transfer (EFT) technology, which transfers funds directly from one account and to another. The system uses the same type of debit services as those used by EFT systems through retail point-of-sale (POS) terminals and Automated Teller Machines (ATM). An EBT System consists of a complex communications network linking together a series of terminals, computer systems, and financial institutions. Figure 1.1, illustrates a generic EBT system.

The EBT System processor, which is the core component of the EBT System stores, processes, and transmits information related to benefit recipients, retailers, and all the benefit transactions between them. The processor also receives transaction data from other EBT System components, including Federal, State, and local agencies, financial institutions, retailers, and third party processors. These components are connected to each other through various communication methods (e.g., direct dial-up lines, Integrated Services Digital Network [ISDN], Frame Relay Network, and transmission control protocol/internet protocol [TCP/IP]).

Recipients access their benefits through POS terminals and ATMs using EBT access cards requiring personal identification numbers (PIN) for authorization. The recipients can obtain their benefit account status, change their PINs, or report lost or stolen cards through Audio Response Units (ARU).

FIGURE 1-1. GENERIC EBT PROCESS

1.4 EBT System Security Issues

The EBT System processes, stores, and transmits sensitive and privacy act information. All State agencies are mandated by FNS to protect sensitive information and to minimize financial losses and fraud. This information includes, but is not limited to, recipient names, Social Security Numbers, benefit amounts, user identifications (ID), passwords, PINs and Personal Account Numbers (PAN).

Because of the complexity of system configuration and the nature of information processed on the system, an EBT System is subject to a wide array of vulnerabilities and threats. A vulnerability is defined as a weakness in the system's design or procedures that could be exploited to gain unauthorized access to the system. A threat can be a person or an event with the potential to cause harm to the system. When a threat successfully exploits a vulnerability, risks may be associated with the vulnerability. These risks could seriously impact EBT System operation. Security controls contained in this guideline must therefore be included in the design and functionality of the EBT System to reduce identified risks to an acceptable level.

According to 7 Code of Federal Regulation Seven (7 CFR), Sections 274 and 277, each EBT System should maximize system security by using the most recent technology available to protect the system and its resources against fraud and abuse. These new technologies include smart cards, fingerprint biometrics, firewalls, client/server computing, and wireless communications, and data warehousing technologies that allow on-line analytical processing and database replication. This security guideline will address the current technology used within EBT systems and also address future implementations of new technology and functionality.

1.5 EBT System Security Reviews

The purpose of a system security review is to evaluate the security effectiveness of the EBT System and review any changes that occurred within the system's operating environment. Depending on the scope of the changes, security reviews may involve all the security areas or may be limited to one area.

According to 7 Code of Federal Regulation Seven (7 CFR), Sections 277.18 (p)(3), ADP system security reviews, ***"State agencies shall review the ADP system security of installations involved in the administration of the Food Stamp Program on a biennial basis. At a minimum, the reviews shall include an evaluation of physical and data security, operating procedures, and personnel practices. State agencies shall maintain reports of their biennial ADP system security reviews, together with pertinent supporting documentation, for Federal on-site review."*** Security controls in EBT Systems should also be reviewed whenever significant modifications are made to the system and/or to its processing environment.

A periodic security review is necessary to identify changes in the risk profile of the EBT System. The security review provides an interim review between risk assessments, ensuring that a minimum level of security is being provided to the EBT System and that the system's certification is still valid. If the periodic review indicates there may be a change in the risk profile of the system, a new risk assessment may need to be conducted.

The security controls outlined in section 2.0 (*IT Security Controls)* should be used as the basis for measuring the effectiveness of the EBT Security Program. Within each of the four major control areas: *Management Controls, Operational Controls, Technical Controls, and EBT Specific Controls,* there are a number of subtopics that should be used to form the foundation for the security review. The IT security controls captured in Section 2.0, Table 2.1. (*IT Security Controls),* outline the subtopics that should be used to create the security control objectives to adequately test the EBT system.

To assist management, developers, and security personnel in performing system security reviews, a checklist is provided in Appendix A1. This checklist outlines the security control objectives derived from section 2.0 (*IT Security Controls)* to include the subtopics that need to be addressed for the security review.

The results of the system security review should be documented in a System Security Review Report. This report should be forwarded to the appropriate officials for their review and acceptance and a copy must be maintained for Federal on-site review.

1.6 Guidelines Organization

The *EBT System Security Guidelines Handbook* is comprised of an introduction, two main sections and six appendices. Individuals involved in developing the EBT System (e.g., system program manager, system security manager, and EBT service provider) should make extensive use of section 2.0 when incorporating security measures into the system. Each section provides the following information:

- Section 1.0 – outlines the purpose, scope and organization of this document and provides an overview of EBT system security,

- Section 2.0 – provides the major security controls that apply to EBT System security and the associated information security features that should typically be incorporated into an EBT System.

- Section 3.0 – provides detailed procedures for developing an EBT System security plan.

- Appendix A-1 – provides a checklist for conducting a security review

- Appendix A-2 – provides a sample risk assessment template

- Appendix A-3 – provides a sample contingency plan for EBT systems
- Appendix A-4 – provides a glossary to define specific technical terms
- Appendix A-5 – provides and acronym list for easy reference
- Appendix A-6 – lists references used in creating this document

2.0 IT Security Controls

In accordance with the NIST Handbook (*Introduction to Computer Security*) the four major subsections of this section deal with information technology security controls: Management Controls, Operational Controls, Technical Controls and EBT Specific Controls. The term *management controls* is used to address those controls that are deemed to be managerial in nature. The *technical controls* are security controls that should be implemented on systems that transmit, process, and store EBT information. The *operational controls* address security controls that are implemented by people and directly support the technical controls and EBT processing environment. The *EBT specific controls* are security controls that are unique to the EBT system.

Each of the four control sections along with their associated subsections (see table 2.1, below) will provide a basic understanding of the security controls and provide guidance on developing and maintaining a secure computing environment.

Table 2.1. IT Security Controls

IT Security Controls	
Control Section	**Control Subsection**
Management Controls	IT Security Program and System-Specific Policy
	IT Security Management Roles and Responsibilities
	Risk Management
Operational Controls	Media Protection
	Personnel Security
	Physical Security
	Contingency Planning
	Incident Response
	Configuration Management
	Security Awareness, Training and Education
Technical Controls	Identification and Authentication
	Logical Access Control
	Auditing
	Internet/Web Security
	Network Security
	Database Security
	Virus Protection
	Penetration Testing
EBT Specific Controls	EBT Access Card Security
	POS Terminal and ATM Security

2.1 Management Controls

Management Controls are necessary to manage the security program and its associated risks. They are techniques that are non-technical and are policy and process driven. This section will highlight the management controls that are put in place to meet the protection requirements of information systems. Management controls are normally addressed by the organization's management and provide controls in the following areas:

Management Controls	❑ **IT Security Program and System-Specific Policy** ❑ **IT Security Management Roles & Responsibilities** ❑ **Risk Management**

2.1.1 IT Security Program and System-Specific Policy

Program security policies and system-specific policies are developed to protect sensitive information transmitted, stored, and processed within EBT system components. Program security policies are broad and are developed to establish the security program and enforce security at the program management level (i.e. An Information System Security Officer (ISSO) shall be appointed for every EBT system). System-specific security policies are detailed and are developed to enforce security at the system level (passwords controls, audit trial configurations, etc.).

2.1.1.1 IT Security Program Policy

All EBT information, applications, systems, networks and resources must be protected from loss, misuse, and unauthorized modification, access or compromise. All organizations that process, store or transmit EBT information must develop, implement, and maintain an IT Security Program to ensure the protection of EBT information. The IT Security Program must include appropriate protection for the EBT resources within their organization to include hardware, software, physical, and environmental facilities.

The EBT program security policy establishes the security program, assigns the appropriate security personnel and outlines the security duties and responsibilities for all individuals within the program. The head of each EBT operating unit is responsible for the protection of EBT resources and its staff. System owners are responsible for providing protection for EBT resources under their control. System owners are also responsible for preventing unauthorized disclosure, ensuring accurate processing of EBT information, and ensuring continuity of operations to accomplish the organization's mission. Every employee who has access to EBT resources is responsible for protecting those resources within their control or possession. EBT policies shall be mandatory for all employees, contractors, and others who have access to EBT information and resources.

The EBT program security policy will encompass all the appropriate security controls contained in this guidelines handbook under *Management Controls, Operational*

Controls, *Technical Controls* and *EBT Specific Controls*. Security controls shall be cost effective and based on a risk assessment, as outlined in Section 2.1.3, *Risk Management*.

2.1.1.2 System-Specific Policy

System-specific controls are used to implement the technical aspects of the EBT program security policy. System-specific security policies for EBT systems will be enforced through logical access controls as well other technical security configuration controls. The system-specific policies that are used to ensure the overall protection of EBT resources and information include but are not limited to the following:

- Access to EBT information and resources is limited to authorized users who have a legitimate "need-to-know" for all the information that they have access to.
- User access to EBT information will be based on the "least privilege" (see section 2.3.2) principle.
- EBT systems will enforce individual accountability (username and password) and record the actions of each user on the system.
- The EBT audit system will record actions taken by system users, applications and processes.
- The EBT audit system will be protected from unauthorized use, modification or deletion.
- All EBT systems must allow for the availability of EBT information for mission critical applications.
- EBT systems will ensure the confidentiality and integrity of EBT information when stored, processed, or transmitted.
- Only those services and applications required for EBT processing will be allowed on EBT systems and resources.
- EBT systems will authenticate all remote access connections to include system users, processes, and applications.
- EBT systems will provide for the continuity of operations in cases of security incidents or system disruptions.
- EBT systems must be developed, designed and configured to support the EBT system security policy.

2.1.2 IT Security Management Roles and Responsibilities

This section is intended to provide a basic familiarity with the primary roles and responsibilities within an IT security program in accordance with *NIST* policies and guidance. It does not describe all the responsibilities of each role and will not uniformly apply to all organizations. This section will not be able to capture the uniqueness of all organizations, but will provide a basic template and outline the responsibilities that should be performed under each role. Due to budgetary and other fiscal concerns, some of the duties described below may be combined and performed by the same person.

2.1.2.1 Senior Management

Senior Management provides the high-level direction for carrying out the organization's mission. They are ultimately responsible for the overall security of the organization, including the security of IT systems and the assurance of mission-critical operations. The authority for implementing the day-to-day management of the security program is delegated to the Information Systems Security Officer.

2.1.2.2 Information System Security Officer

An Information System Security Officer (ISSO) should be appointed for any system or group of EBT systems that are owned or operated by the organization. The ISSO is appointed to develop, administer, and maintain an adequate information system security program. The ISSO directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among the organizational elements involved in the computer security program as well as those external to the organization. The ISSO performs the following functions.

- Ensures compliance with Federal and State regulations regarding information security policies and procedures
- Maintains system access based on approved personnel security investigations, a need-to-know, or other organizational authorizations
- Develops, maintains, and distributes security procedures and guidance for systems administrators and users of their system(s).
- Prepares and provides systems-specific security awareness training for their system(s).
- Reports any suspected or known security incidents/violations.
- Reviews audit records routinely and reports any deviation of security practices.

2.1.2.3 Technology Providers

Technology Providers assist the ISSO in implementing and administering system-specific security controls. Systems and/or network administrators under the oversight of the ISSO securely configure EBT systems. Security guidance passed down by the ISSO to Technology Providers is distributed through the EBT Security Plan and other security documentation (security configuration guides, etc.).

- *System/Network Administrators*. System/Network Administrators are responsible for implementing the technical security controls based on security guidance from the ISSO. Depending on the size of the network, these duties could be separate or combined under the same individual or distributed among a group of individuals. The system/network administrators will work closely with the ISSO to ensure that all the required security measures are implemented in accordance with the organization's security plan. The system/network administrator will notify the ISSO immediately of any unauthorized activity within the network. Some of the security responsibilities of the system/network administrators include:

    - Securely configuring the system/network (authentication, access control)
    - Updating the system with the latest system/security patches
    - Monitoring user activity on the network/system
    - Periodically reviewing the system audit logs
    - Performing data back-up procedures.

- *Help Desk*. The Help Desk staff should be incorporated into the incident handling process. The Help Desk staff should receive the proper training to be able to recognize security incidents. The Help Desk staff should be the first point of contact for users who suspect or are aware of a security breach. The Help Desk staff should know when to escalate a security incident by notifying the appropriate person (usually the ISSO). The help desk staff are responsible for:

    - Receiving all security incidents (or suspected) from EBT users
    - Documenting all security incidents (or suspected) received from users
    - Informing users of the proper actions to mitigate the situation (when possible)
    - Escalating the incident to the appropriate staff.

2.1.3 Risk Management

According to *NIST*, risk management is the total process of identifying and assessing risks and taking steps to reduce them to an acceptable level. The goal of risk management is to protect the organization's assets to preserve their ability to perform. Risk management, when applied to EBT systems is a continuous process of identifying threats, determining risks, determining security controls and selecting the most cost effective controls. It includes the following four phases:

- *Risk Assessment* – identify threats and vulnerabilities
- *Risk Analysis* – determine the severity of the risks
- *Risk Mitigation* – identify security controls to mitigate risks
- *Cost Considerations* – select cost effective security controls to implement

2.1.3.1 Risk Assessment

The risk assessment is used to identify the vulnerabilities, threats, and likelihood of loss or impact to the system. The risk assessment is used within EBT systems to determine if the current security controls are adequate to reduce the probability of loss due to a vulnerability or potential threat to the EBT system. The risk assessment should be based on a methodical and structure approach when identifying threats for a specific EBT system. Depending on the physical location of the system, such threats may include:

- *Natural disasters*
- *Sabotage*
- *Vandalism*
- *Theft*
- *Fraud*
- *Human error*
- *Hardware failure*
- *Public utility failure.*

The estimate of the threat probabilities can be based on the analysis of historical data (number of earthquakes, floods, etc.), incident reports maintained by the security office, local crime statistics and other known threats that have been identified by local and Federal government organizations. System log files and Intrusion Detection System (IDS) logs are also an excellent source to gather potential threat information.

The results of the risk assessment will be analyzed during the risk analysis phase to determine the severity of the threat or vulnerability. The results of the risk assessment can also be used to create security requirements for EBT systems.

2.1.3.2 Risk Analysis

Once the risks have been identified during the risk assessment, a risk analysis is performed in order to determine the severity of each risk to the EBT system. The severity levels of risks are usually measured in degrees of high, medium or low. *NIST* defines the severity levels as:

- High – a major (highly costly) loss of assets and resources (including data) that may significantly impact the organizations mission
- Medium – a (costly) loss of assets and resources (including data) that may adversely impact the organizations mission
- Low – a loss of assets or resources that may noticeably impact the organizations mission

The degree to which you assign a severity level depends on the likelihood of the threat and/or the effectiveness or absence of the current security controls to counter the threat. Appendix A2 provides a sample risk assessment for EBT systems.

2.1.3.3 Risk Mitigation

During the risk mitigation process the risks that are identified during the risk assessment and analyzed and prioritized during the risk analysis phase are evaluated to determine the most appropriate security controls to counter the threats and vulnerabilities. The most appropriate security controls are identified to reduce the "high" and "medium" level risks to an acceptable level (usually low).

The non-technical controls identified in the *management control* and *operational control* sections of this document under: security policies, media protection, personnel and physical security, incident response, contingency planning and security awareness training can be used to counter specific threats and vulnerabilities. The technical controls identified in the *technical controls* section under: identification and authentication, access control, auditing, virus protection, Internet, network and database security can be used to counter specific technical and system related threats to EBT systems.

2.1.3.4 Cost Considerations

Management's decision to implement the selected security controls identified during the risk mitigation process should be based on the cost of the security controls versus the cost of the information or resource requiring protection. A cost benefit analysis should be completed to justify the cost for implementing the control versus the cost of the information or resource requiring protection. According to *NIST*, the cost benefit analysis should include the following:

- Determining the impact of implementing the security control
- Determining the impact of not implementing the security control
- Estimating the cost of implementing the security control.

There is a cost to an organization when implementing a security control and a cost to the organization by not implementing a security control (accepting the risk). EBT system owners should be aware of both costs when making their decision to implement a specific security control to counter a threat or vulnerability.

EBT business areas and "owners" of information systems should conduct a risk assessment for each system. Since a major change to the system could adversely affect the protection profile from the last risk assessment performed, a new risk assessment should be performed whenever there is a major change to the information system.

2.2 Operational Controls

Operational Controls focus on controls that are, implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and often rely upon management activities as well as technical controls. The following operational controls will be covered in this section:

Operational Controls	❑ **Media Protection** ❑ **Personnel Security** ❑ **Physical Security** ❑ **Contingency Planning** ❑ **Incident Response** ❑ **Configuration Management** ❑ **Security Awareness and Training**

2.2.1 Media Protection

Media controls address the storage, retrieval, and disposal of sensitive materials that should be protected from unauthorized disclosure, modification, or destruction. All storage media for EBT systems requires protection to ensure the integrity and confidentiality of EBT information. It is composed of two security requirements: Computer Output Controls and Electronic Media Controls.

2.2.1.1 Computer Output Controls

All printout copies of sensitive EBT information should be clearly marked as such. If required, sensitivity levels with the associated labels may be required to identify different sensitivity levels of EBT information. In addition, procedures for storage, mailing, marking, and disposal for the different levels of sensitive EBT information may also need to be defined.

2.2.1.2 Electronic Media Controls

All the requirements (labeling, storage, mailing, etc.) for computer outputs should be applied to electronic media that contain sensitive EBT information. However, the disposal and reuse of electronic media that contains sensitive EBT information will differ vastly from that of paper printouts. Procedures need to be established to ensure that data cannot be recovered from electronic media that contains EBT information before transfer,

reuse (non-EBT related) or disposal. Electronic media containing EBT information can be sanitized (cleared or destroyed) using some of the methods described below:

- Overwriting all addressable locations with a single or random character
- Degaussing the media using an approved degausser
- Physically destroying the media so it cannot be reused.

The sanitization methods described above will depend on the type of electronic media requiring clearing or destroying.

2.2.2 Personnel Security

All personnel with responsibilities for the management, operation, maintenance, or use of EBT system resources and access to sensitive EBT information should have the appropriate management approval. An employee's access to EBT systems should be restricted to the required resources that the employee needs to fulfill his or her duties. The following personnel security controls should be enforced on all EBT systems:

- The ISSO or the system owners who directly support business operations should authorize, in writing, any non-EBT personnel who use their system.
- Technical support personnel from outside EBT, who perform maintenance on EBT systems within EBT-controlled facilities, should be escorted at all times, unless they have been approved for unescorted access.
- All employees must be removed from the system on or before their employment termination date.
- An employee's access to the system should be removed prior to notifying the employee of termination procedures.

2.2.2.1 Contractor Personnel Requirements

All contractors accessing EBT systems should sign a non-disclosure form as a condition of receiving EBT accounts. The ISSO shall provide non-disclosure forms and maintain completed forms. Contractors should be required to follow the same personnel security requirements as State employees.

2.2.2.2 Separation of Duties

Separation of duties ensures that no single individual has total control of the system's security mechanisms; and, therefore, no one individual can compromise the EBT system completely.

- Assign portions of security-related tasks to several individuals.
- Implement separation of duties using the security principle of least privilege.
- Ensure that users and processes in a system have the least number of privileges for the least amount of time to perform assigned tasks.

- Require different individuals to be assigned the roles of systems/network administrator and the ISSO.

2.2.3 Physical Security

Physical security is concerned with the measures to prevent unauthorized physical access to EBT equipment, facilities, material, information, and documents. Physical security also safeguards EBT's assets against espionage, sabotage, damage, tampering, theft and other covert acts. All hardware, software, telecommunications, documentation, and sensitive information handled by a system should be adequately protected to prevent unauthorized access, use, modification, disclosure, or destruction.

Physical security policies and requirements for EBT computer facilities must include physical construction, fire protection, access controls and environmental controls. Facility security measures are developed and implemented based on the level of risk to the computer and information resources as identified during the risk assessment. Rooms containing system hardware and software, such as local area network rooms or telephone closets, are secured, where possible, to ensure that they are accessible to authorized personnel only.

2.2.3.1 Non-centralized systems

Servers and mid-tier systems not housed in a central facility must be afforded protection from unauthorized access and both intentional and accidental damage. The following physical security procedures shall apply:

- Access to these systems shall be physically controlled
- The rooms or cabinets that house this equipment should be secured
- Environmental controls (separate air conditioning, fire protection, etc.) may be warranted.

2.2.3.2 Centralized Computer Facilities

The physical security protection employed in the centralized computer facility should be commensurate with the maximum sensitivity of the EBT information handled. Computer rooms processing EBT information and those approved for open storage of EBT information should provide a separate level of access control (separate from main building) for protection of the restricted area. Unescorted access to administration areas is limited to personnel who have official business in the area or have approval of the ISSO. The following physical security procedures should apply:

- Establish internal access control procedures (zoning)
- Use identification badges for physical recognition
- Require contractor or vendor badges to be clearly identified as such
- An intrusion detection system (alarm) should be used to monitor the perimeter and interior of the computer room

- Use a closed circuit television (CCTV) to monitor access to the computer room and its critical assets.

2.2.4 Contingency Planning

Preparing a well-planned contingency operations and disaster recovery plan will make the difference between continued business processes and significant reduction in operations by having to replace lost data or systems along with the associated inability to continue to work. Contingency Planning develops procedures that provides continued essential business processes if systems or information technology support are interrupted.

Each major EBT application and general support system must have a viable and logical Contingency Plan. This Plan will be routinely reviewed, tested, and updated to:

- Minimize damage and disruption caused by undesirable events;
- Provide for continued performance of essential system and computer processing operations, services, and mission-critical function.

The ISSO and appropriate systems personnel (system owner) should coordinate to develop and maintain a current, viable Contingency Plan. The plan will provide reasonable assurance that critical data processing support can be continued, or quickly resumed, if normal operations are interrupted.

Contingency Plans include the following:

- Backup operations plans, procedures and responsibilities to ensure that essential (mission-critical) EBT operations will continue if normal activities are stopped for a period of time.
- Emergency response procedures that include civil disorder; fire; flood; natural disaster; bomb threat; or other incidents or activities where lives, property or the capability to perform essential functions are threatened or seriously impacted.
- The lowest acceptable level of essential system or functional operations, so that plan priorities may be made. This must include provisions for storage, maintenance and retrieval of essential backup and operational support data.
- Post-incident recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at a primary site or, if necessary, at an alternate facility, following destruction, major damage or other significant interruptions of the primary site.

Contingency plans should be tested periodically (biannually) to ensure accuracy and completeness. A sample Contingency Plan can be found in Appendix A3.

2.2.5 Incident Response

A security incident is any event or condition that has the potential to impact the security of an EBT system. These incidents may result from intentional or unintentional actions and may include loss or theft of computer media, introduction of malicious code, unauthorized attempts to gain access to EBT information or failure of the system security function to perform as expected.

Examples of reportable incidents are:

- Discovered viral infection
- Discovered malicious code (i.e., viruses, trap doors, logic bombs, worms, Trojan Horses, etc.)
- Uncovered hacker activity
- Discovered system vulnerabilities
- Unauthorized attempt, successful or not, to access an EBT system
- Deviation from security policy
- Other unusual activities.

2.2.5.1 Reporting Incidents

If malicious code is detected, whether prior to system entry or after system infection, or you detect a security violation that may result in:

- Disclosure of sensitive information to unauthorized individuals,
- Unauthorized modification or destruction of system data, or loss of computer system processing capability, or
- Loss or theft of computer system resources-report it to your supervisor or other appropriate supervisory channels, as a security incident.

The incident must be promptly reported to the immediate supervisor. The supervisor will in turn report the incident to the ISSO for technical resolution. The ISSO documents and reports the incident, as appropriate, and address the impact of the security incidents. When reporting an incident, the following information must be provided:

Table 2-2, Incident Reporting

Incident Reporting	
1.	Type of incident.
2.	Date and time of the incident.
3.	Name of the victimized system.
4.	Description of the incident.
5.	Impact of the incident.

2.2.6 Configuration Management

The primary goal of configuration management (CM) is to keep track and document changes to the system's configuration (versions of hardware, software, documentation, etc.) under the control of change management. The primary security goal of configuration management is to ensure that the changes to the system do not adversely affect the security posture of the system and/or environment.

Configuration management provides the discipline for managing and controlling all components that are used in the EBT operational environment and covers both the application environment and the EBT infrastructure. To be effective, CM must be applied to the full life cycle of activity involved in building and implementing business applications and the EBT infrastructure. The discipline consists of a set of processes that produce and validate components such as the configuration items (CIs) for the EBT systems environment. All components that are to become part of the EBT systems environment (including EBT inventory information) need to be deposited and maintained within a configuration management database (CMDB) where the information can be referenced by other management functions.

2.2.6.1 Configuration Management Plan

The first steps in developing the configuration management plan (CMP) are to define the scope and objectives of the configuration management process and to identify specific business goals to be achieved. Both short and long-term objectives should be defined. A clear understanding of the scope and objectives helps guide the configuration management staff in the performance of their assigned activities. Configuration management applies to all EBT infrastructure systems and equipment. CM helps for identify, control, and track all components of the EBT environment. To accomplish these tasks, configuration management must be shared with numerous groups within the organization. To ensure the usefulness of the configuration management process, EBT organizations should:

- Identify and label all CIs in the EBT environment
- Control and track all changes to CIs throughout the system life cycle
- Coordinate the documentation of all changes to the EBT environment with change management
- Establish and maintain baseline configurations
- Control assets by knowing what assets are held by the organization
- Manage software licenses and ensure that only authorized copies of software are used in the EBT environment
- Conduct audits to ensure that the actual state of the EBT environment matches what is documented in the CMDB
- Train organizational groups about the CMP process and the importance of using only authorized CIs in the EBT environment
- Provide reports to management.

2.2.6.2 Change Management

Change management is responsible for changes in technology, systems, applications, hardware, tools, documentation, processes, and roles and responsibilities. The security goal for change management is to identify all proposed changes to affected systems and processes before the change is implemented in order to mitigate or eliminate any adverse effects on the security posture of the system.

Change management is most closely tied to release management and configuration management. Change management involves assessing the impact of proposed changes to the EBT environment, prioritizing and categorizing changes, determining the course of action, and monitoring the planning, development, testing, and implementation of changes. Utilizing a change management process will increase service availability and EBT efficiency by reducing the number of unnecessary changes. Change management should manage changes that:

- Will affect multiple users/customers
- Could potentially disrupt mission-critical functionality
- Involve hardware (such as servers) or software modifications
- Involve operational and process modifications that affect multiple users/customers.

2.2.7 Security Awareness, Training and Education

Personnel who manage, operate, program, maintain, or use the EBT System should be aware of their security responsibilities. Security awareness training should be provided in addition to functional training before system users are allowed access to the EBT System. This training should be conducted periodically (e.g., once a year).

The primary purpose of security training is to help system users become familiar with using the system's security features. Security training also ensures that users understand their responsibilities and security procedures for protecting the sensitive EBT information they manage. ISSO's have a very important function within their organization and therefore, require a comprehensive and continuing security training program.

Security awareness training should be mandatory and should be completed prior to granting access to the system. Periodic refresher (annual) security training should be required for continued access. Therefore, each user (including contractors) must be versed in acceptable rules of behavior before being allowed access to the system. The training program should also inform the user on how to identify a security incident.

2.2.7.1 Initial User Briefing

Training should be provided to all new users of a system. This training should include general security awareness issues, such as viruses and hackers, as well as an awareness of

system specific security requirements. Users should also be allowed to review a copy of the EBT Security Policies document.

2.2.7.2 System Security Refresher Training

Periodic, but at least annual, training should be provided to all system users. Training should include reminders and updates of computer security awareness and system specific security requirements. Periodic system security training will be documented and maintained on file.

2.3 Technical Controls

The *Technical Controls* section focuses on security controls that the computer system executes. These controls depend on the proper configuration and functionality of the system. The implementation of technical controls, however, always requires significant operational considerations. These controls should be consistent with the management of security within the organization. The EBT technical controls consist of:

Technical Controls	❑ **Identification and Authentication** ❑ **Logical Access Control** ❑ **Auditing** ❑ **Internet/Web Security** ❑ **Network Security** ❑ **Database Security** ❑ **Virus Protection Controls** ❑ **Penetration Testing**

2.3.1 Identification and Authentication (I&A)

User Identification (User ID) is used to identify persons working on EBT systems. This is the method for ensuring that the person who is logging on to the desktop, network or an EBT application is in fact that person. For this reason, all User IDs should be unique throughout the system. A password is something that only the user should know. Passwords should also be unique within the system. The User ID and password combination is known as a single factor I&A. The User ID and password for each individual identifies that individual to the system and must be protected to ensure that no one can impersonate that individual.

2.3.1.1 Passwords

Use of passwords should be required within EBT systems. Passwords provide access to EBT systems and resources for authorized users while denying access to unauthorized users. Password policies for EBT systems should consist of the following:

- Minimum password length (eight (8) alphanumeric characters recommended)
- Password history kept to prevent reuse of current passwords
- Limit on number of incorrect password attempts (three (3) unsuccessful attempts is recommended)
- Procedures for password changes (every 60-90 days recommended)
- Account lockout procedures established (after three invalid attempts)
- Procedures for password changes
- Procedures for handling lost or compromised passwords
- Auditing for inactive accounts (30 days of inactivity).

The password policies should be communicated to all EBT system users during the initial security training and periodically during refresher training.

2.3.2 Logical Access Control

Limiting access to EBT systems to authorized users is an important part of good security practices. This is accomplished in several ways. First, access is controlled through the use of a user ID/password combination. If you do not have a valid user ID and password, you are denied access to the EBT system.

Second, limiting permissions or privileges to only those necessary to perform specific job functions within EBT systems. This is known as the principle of "least privilege" and is implemented by assigning appropriate rights or privileges to each user or group of users. The rights assigned to an individual are determined by the job functions they perform and the permissions requested and approved by management. EBT supervisors and managers shall continuously assess the privileges granted to employees and contractors and submit the necessary requests to change or remove access to those system and network resources that are no longer required.

Finally, access to the EBT systems should be controlled through the use of access control devices designed to restrict connections to the EBT network and its resources. Access control devices such as firewalls and routers are deployed within the network infrastructure to restrict traffic into and out of the EBT network.

2.3.2.1 System Accounts

To establish an EBT account, a supervisor or manager should request the account and password, in writing.

- No more than one system account should be permitted unless the position or job function requires multiple accounts. For example, a system administrator should have two accounts: an administrator account used when performing system administration functions, and a user account for routine day-to-day use.

- All guest accounts should be disabled on EBT systems.
- All default system accounts should be disabled or removed.

2.3.2.2 Workstation Security

All EBT workstations should require password-protected screensavers. Workstation screensavers should be configured to activate when the keyboard or mouse is not used for a configurable period of time (15 minutes recommended), requiring reentry of a password before access is granted. This limits unauthorized access to the workstation and the network while the workstation is unattended. Users should not be allowed to download and install screensavers. A default screensaver should be automatically selected to ensure optimum performance, low system resource utilization (e.g., memory and CPU resource utilization), and prevention of the introduction of malicious code from screensavers downloaded over the Internet.

Users should be required to log off their workstations every night to shutdown the system. Users should be instructed to lock or log off their workstations if they are going to leave it unattended for a significant period of time.

2.3.2.3 Warning Banner

Warning banners should be displayed before any access to an EBT system is authorized. Where technically feasible, warning banners should be displayed upon logon to any EBT system. Warning banners are an important legal instrument and should be crafted to inform users that they are accessing a government system and are subject to legal penalties for unauthorized access or misuse.

2.3.3 Auditing

Audit trails document the actions that have been taken on the system. Audit trails allow for the investigation and detection of system misuse and can aid in the conviction of individuals who illegally access an EBT system.

Audit trails should capture the following information:

- System start-up and shutdown
- Successful and unsuccessful login attempts
- User actions to access files or applications
- Actions taken by system administrators and security personnel
- All administrative actions performed on an EBT system.

Audit trails should record the following information for each event:

- Date and time of event
- Type of event

- Success or failure of an event
- Name of file or application accessed.

2.3.3.1 Audit Trail Maintenance

Audit trail logs should be properly secured with access limited to system administrators and the ISSO. The ISSO should regularly review the audit logs. The following procedures should be required for maintaining audit trails:

- Review of audit trails is a function of the ISSO or designee.
- Audit trails should be reviewed weekly at a minimum, but preferably daily. Depending on the size of the system, the review can consist of the entire audit trail, a review of customized reports, or using an automated audit-monitoring tool.
- Access must be controlled to prevent unauthorized access, modification, or loss.
- Audit trails should be maintained for one (1) year in either paper or electronic form.
- Paper copies of audit trails should be treated as **FOR OFFICIAL USE ONLY** and shredded when no longer needed. Electronic copies must be cleared in some manner before disposal. (*See Section 2.2.1 Media Protection*.)

2.3.4 Internet/Web Security

The proliferation of the Internet has grown exponentially. It has rapidly become an essential tool for nearly every organization. Since Internet access exists on almost every desktop, allowing employees to access a wealth of information, it is imperative that security controls be applied to Internet connections to enforce the confidentiality, integrity and availability of EBT information.

Because of the easy access users have to Web sites, the Web and its servers have become a focus for those individuals who wish to steal or damage information and systems. The Web and its associated servers have become the new means by which a hacker can gain access to and damage, systems, and information. A web server can be attacked directly or be used as a node to attack an organization's internal networks. There are many functional areas of Web technology that must be secured, including:

- The Operating System
- Web Server
- Web Browsers.

2.3.4.1 Operating System Security

Since the application software runs on top of the operating system (OS), it is imperative that it be secured. If the OS is compromised due to weak security, then the applications

that run on the system will also be breached. The OS is solely responsible for controlling the machine's resources, and access to those resources is usually secured through the OS. Additionally, the software or applications that the operating system controls also needs to be secure, along with the physical host machine itself. If there is a vulnerability in an application that has been granted high enough access rights (administrator or root), that application can easily be exploited to gain full control over the operating system. Once the operating system has been compromised, all the software it controls has also been compromised. However, nothing is safe if the physical machine itself is not secured. To reduce these risks, it is necessary to secure the operating system and physically secure the host system that runs the applications. This process is referred to as "hardening." The following procedures are used in the "hardening" process:

- Eliminate unnecessary programs and services
- Close all unused ports on the system
- Change default file permission to be more restrictive
- Enable verbose logging on the system (auditing)
- Require a CMOS/PROM password
- Disable file-sharing features
- Adhere to password and user account policies and guidelines
- Apply the most current system patches for the operating system.

The default installation of an OS will leave the system in an unsecured state. It is recommended that you follow the vendor's recommendation for securing your particular operating system. The ISSO should also provide the appropriate guidance for removing specific services and closing unused system ports. The recommendations and security controls outlined in this guide will also aid in securing the operating system.

2.3.4.2 Web Server Security

Securing the OS that the Web server runs on is the initial step in providing security for the Web server. The Web Server software only differs in functionality from other applications that reside on a computer. However, since the Web server usually provides public access to the computer, it should be securely configured to prevent the Web Server and the host computer from being compromised from intruders.

One of the precautions to take when configuring a Web server is to never run the web service as a "root" or administrative user (superuser). The Web service should be run with the permissions of a normal user. This situation would prevent the escalation of privilege if the Web server were ever compromised. Also, do not configure the file system of the Web server (directories and files) to have write access for any users other than those internal users that require such access. Other precautions and secure configuration issue to consider when configuring a public Web server are:

- The Web server should be on a separate local area network (DMZ) from other production systems

- The Web server should never have a trust relationship with any other server that is not also an Internet-facing server or server on the same local network.
- The Web server should be treated as an untrusted host
- The Web server should be dedicated to providing web services only
- Compilers should not be installed on the Web server
- All services not required by the Web server should be disabled
- The latest vendor software should be used for Web server including all the latest hot fixes and patches.

2.3.4.2.1 CGI Scripts

Common Gateway Interface (CGI) is a protocol used to create programs for Web applications. There is a possibility of compromising security when using CGI scripts. Some input can cause the CGI program to crash or behave in an unexpected way. The danger is reduced if the CGI script is vendor-supplied. The following is a list of CGI best practices that should be implemented:

- CGI Scripts should not be installed on a web server without the knowledge and consent of the ISSO.
- The directory containing CGI scripts must have permissions of read/write/execute for owner and execute-only for group and others.
- All CGI scripts should be owned by root or administrator.
- All CGI scripts should have permissions of read/write/execute for owner and execute-only for group and others.
- All backup copies of CGI scripts that are automatically generated should be removed from the system.
- CGI scripts should not be available for FTP by users.
- The ISSO should document all CGI used on the web server.
- Each CGI script should use a common directory for temporary files and once that task is completed, the temporary file will be deleted.
- The ISSO should ensure that no CGI script source files exist in the web server document directories.
- All CGI scripts should be centrally stored in the cgi-bin (or equivalent) directory.

2.3.4.2.2 Improper Input

Hyper Text Markup Language (HTML) includes the ability to display selection lists, limit the length of fields to a specific number of characters, embed hidden data within forms, and specify variables that should be provided to CGI scripts. These are a great help in reducing how much error checking must be included in scripts, but an outsider can run a CGI script by accessing the script's URL. To limit improper input, the following activities should be performed:

- Error checking should be performed on all input data.
- Browser-dependant code, to include Active X, should not be allowed.
- The following input should never be accepted by a CGI script:

  - Any cookie or special tag not created by your server.
  - Input that exceeds the maximum length of the defined variable.
  - Any non-alpha or non-numeric characters except special characters.
  - Values that are outside the defined scope of the expected value parameters.

2.3.4.2.3 Server Side Includes

Server Side Includes (SSIs) provide web pages with the content of system commands. This is done by examining files with an extension of shtml (or any other extension requested) and replacing SSI commands with the results of the evaluation of those SSI commands prior to serving the page to the requester. SSI also provides the capability to execute commands or CGI scripts. The capability to execute commands and scripts can pose a significant security exposure. Unless there is a valid business need SSI should not be enabled on the web server.

2.3.4.4 Web Browser Security

The Web browser is usually a commercial client application that is used to display information requested from a Web server. There should be a standard browser that has been approved by the ISSO for use within the EBT system environment. Due to the security holes in scripting languages such as JavaScript and Active X (Microsoft), it is recommended that all scripting languages not required for official EBT systems operation be disable within the Web browsers.

2.3.4.4.1 Mobile Code

Mobile code is the term for code obtained from remote systems, transmitted across a network, and executed on a local system. Mobile code also refers to Web-based code downloaded and run by the user's web browser.

Executable content is a subset of mobile code that is largely invisible to the user and operates in the background. Executable code is automatically activated upon retrieval without user interaction. Users may not be aware that a separate executable has been downloaded to their systems.

Hostile mobile codes or executable content are completely different from the more-traditional malicious codes, such as viruses and worms. Detection by standard antiviral software is more difficult, and such codes should be used with caution. EBT users should be encouraged to avoid downloading, executing, or visiting sites that employ untrusted mobile code. Some of the requirements for mobile code should include:

- Mobile code should be digitally signed
- Mobile code should only be accepted from trusted sources
- EBT systems should be configured to block mobile code from untrusted sources
- Protections against malicious forms of mobile code shall be implemented in developed software and configured in COTS applications.

2.3.5 Network Security

Network Security addresses requirements for protecting sensitive data from unauthorized disclosure, modification, and deletion. Requirements include protecting critical network services and resources from unauthorized use and security-relevant denial of service conditions.

2.3.5.1 Firewalls

Firewalls provide greater security by enforcing access control rules before connections are made. These systems can be configured to control access to or from the protected networks and are most often used to shield access from the Internet. A firewall can be a router, a personal computer or a host appliance that provides additional access control to the site. The following firewall requirements should be implemented:

- Firewalls that are accessible from the Internet are configured to detect intrusion attempts and issue an alert when an attack or attempt to bypass system security occurs.
- EBT firewalls are configured to maintain audit records of all security-relevant events. The audit logs are archived and maintained in accordance with applicable records retention requirements and security directives.
- Firewall software is kept current with the installation of all security-related updates, fixes or modifications as soon as they are tested and approved.
- EBT firewalls should be configured under the “default deny” concept. This means that, for a service or port to be activated, it must be approved specifically for use. By default, the use of any service or communications port without specific approval is denied.
- Only the minimum set of firewall services necessary for business operations is enabled and only with the approval of the ISSO.
- All unused firewall ports and services are disabled.
- All publicly accessible servers are located in the firewall DMZ or in an area specifically configured to isolate these servers from the rest of the EBT infrastructure.
- EBT firewalls filter incoming packets on the basis of Internet addresses to ensure that any packets with an internal source address, received from an external connection, are rejected.
- EBT firewalls are located in controlled access areas.

2.3.5.2 Routers and Switches

Routers and switches provide communication services that are essential to the correct and secure transmission of data on local and wide area networks. The compromise of a router or switch can result in denial of service to the network and exposure of sensitive data that can lead to attacks against other networks from a particular location. The following best practice solutions should be applied to all routers and switches throughout the EBT environment:

- Access to EBT routers and switches is password-protected in accordance with FNS guidance.
- Only the minimum set of router and switch services necessary for business operations is enabled and only with the approval of the ISSO.
- All unused switch or router ports are disabled.
- EBT routers and switches are configured to maintain audit records of all security-relevant events.
- EBT router and switch software is kept current by installing all security-related updates, fixes or modifications as soon as they are tested and approved for installation.
- Any dial-up connection through EBT routers must be made in a way that is approved by the ISSO.

2.3.6 Database Security

The goal of database security for EBT systems is to protect critical and sensitive EBT data from unauthorized access. Unauthorized access entails changing, deleting or disclosing EBT data in the database. Access to EBT databases must be controlled in order to preserve the integrity, consistency, and availability of EBT information.

The integrity of all data within a Relational Database Management Systems (RDBMS) is the primary responsibility of the Database Administrator (DBA) and the ISSO. Application developers also play a key role in database design, development, and implementation, ensuring data integrity. To ensure data integrity, it is important to perform database administration correctly, regularly, and reliably. Some of the duties that will be performed to ensure data integrity are as follows:

- Correct and successful physical backup of all database data
- Correct and successful logical backup of all database data
- Recovery operations
- Database performance analysis
- Enabling of auditing
- Analysis of audit data.

2.3.6.1 Database File Integrity

To ensure the integrity of the database files the following procedures should be incorporated into the database security plan. These requirements should be derived from the EBT system-specific security policies.

- Database COTS software should not be modified from its installation defaults to be more permissive.
- All directories created by the installation of a RDBMS should not be modified to be more permissive.
- Any groups created by the installation of a RDBMS should not be modified to be more inclusive.
- Any file permissions created by the installation of a RDBMS should not be modified to be more permissive.
- End users should never be allowed to change any directory names, file permissions, or group information associated with the database software.
- All default and vendor installation accounts should be deleted from the system.

2.3.6.2 Database File Backup and Recovery

A tested and verifiable backup strategy must be implemented for all EBT databases. The DBA can create scripts or uses vendor-supplied scripts or utilities to perform backup and recovery operations. These scripts or utilities associated with backup and recovery should be available for review during the security review. The database backup and recovery operations should be incorporated into the overall continuity of operations plans for the facility.

2.3.7 Virus Protection Controls

All EBT systems should use antivirus (AV) utilities or programs to detect and remove viruses or other malicious code. The AV software must be kept current with the latest available virus signature files installed.

AV programs should be installed on workstations to detect and remove viruses in incoming and outgoing email messages and attachments, as well as actively scanning downloaded files from the Internet. Workstation and server disk drives should be routinely scanned for viruses. The specific restrictions outlined below should be implemented in order to reduce the threat of viruses on EBT systems:

- Traffic destined to inappropriate websites should not be allowed.
- Only authorized software should be introduced on EBT systems.

- All media should be scanned for viruses before introduction to an EBT system. This includes software/data from other activities and programs downloaded from the Internet
- Original software should not be issued to users, but should be copied for use within copyright agreements. At least one copy of the original software should be stored according to configuration management controls.

2.3.8 Penetration Testing

Penetration testing is highly specialized field and requires staff knowledgeable in various testing methodologies, experienced in all levels of testing, and trained in the use of various testing tools. A systematic and analytical process must be used to evaluate computer resources for exploitable vulnerabilities. Penetration testing involves real-world hacking techniques to identify security weaknesses and validate the overall security posture of a network.

As part of the security assessment for EBT systems, penetration testing should be incorporated to effectively evaluate the overall security posture of the network. The penetration test should be approached from a hacker's perspective. A combination of both commercial and freeware hacking tools should be used to scan the network to uncover any inherent vulnerabilities. Once all the vulnerabilities are found, they should be documented along with the mitigation strategies to resolve each discovered vulnerability.

Penetration testing is accomplished in four phases:

- Planning
- Vulnerability Analysis
- Attack Execution
- Analysis and Reporting.

2.4 EBT Specific Controls

The EBT Specific Controls section will highlight those controls that are specific to the EBT network infrastructure. These controls will cover the following two technical implementations within the EBT system:

EBT Specific Controls	❑ **EBT Access Card Security** ❑ **POS Terminal and ATM Security**

2.4.1 EBT Access Card Security

EBT access card security consists of card management functions, including the issuance and control of EBT cards. Four types of access cards can be used in EBT pilot and operational systems: magnetic stripe cards, smart cards, hybrid cards, and optical cards. The vast majority of operational EBT systems use magnetic stripe cards and this will likely continue as the standard for EBT systems.

- *Magnetic stripe cards* contain information on benefit recipients (e.g., personal account number, name), which is verified by a central processor before benefit transactions are authorized.

- *Smart cards* are different from magnetic stripe cards in that they contain a microprocessor and a memory chip that processes transactions "off-line." With smart cards, the transaction is authorized between the chip and the POS terminal. There is no on-line communication with a central processor at the time of transaction.

- A *hybrid card* may contain a combination of different technologies, but in this document, a hybrid card is defined as a smart card with a magnetic stripe. The magnetic stripe may be used to access one type of benefit account and the smart chip accesses another.

- An *optical card* uses a recording medium similar to that of an audio compact disc. The card uses write-once-read-many (WORM) technology and has sufficient capacity to store megabytes of data. It is suitable for off-line processing and has the capability for extended applications such as health care processing.

Security issues associated with EBT access cards have been raised due to the high frequency of maintenance activities associated with them. Access cards are continually issued, activated, replaced, and destroyed. Therefore, the potential for fraud exists at many points in the life cycle of the cards. To mitigate the risk of fraud, several security measures should be incorporated into the cards.

- **Magnetic Stripe Card Security** – includes requirements for conformance to International Organization for Standardization (ISO) standards, and policies for

card inventory management, card activation and deactivation, PIN mailings, and card lifecycle.

- **Smart Card Security –** includes requirements for the operating system, the ability to disable and enable chips, key management, expiration dates, encryption, biometrics verification and security for multi-application cards.

- **Hybrid Card Security –** includes the same requirements for magnetic stripe cards and smart cards. It also includes controls to prevent security loopholes such as the ability to use the magnetic stripe to access benefits when the smart chip is not functional.

- **Optical Card Security –** includes requirements for the confidentiality of data stored on optical cards, the use of data encryption, and the use of anti-counterfeit features.

2.4.2 POS Terminal and ATM Security

Recipients gain access to their benefits through POS terminals and ATMs. Benefit transactions can be performed through on-line processing, off-line processing, and manual processing.

- **On-line Processing –** On-line processing uses a central processor to verify PINs and authorize transactions. Requirements include cashier ID and password verification, settlement controls, integrity of transmitted data, and on-line biometric verification.

- **Off-line Processing –** Off-line processing performs PIN verification and transaction authorization at the point-of-sale. Depending on how off-line processing is implemented, transactions can be processed in one of two forms. They can either be pre-authorized at the POS (i.e., stored locally and then forwarded at a later time in a batch to the central processor for authorization), or they can be authorized at the point-of-sale by a secure POS terminal (i.e., transactions are stored on the smart cards only and are never forwarded to a central processor). Requirements for this security element may include mutual authentication between the smart card and the POS terminal, non-repudiation controls for transactions, and off-line biometric verification.

- **Manual Processing –** refers to backup procedures for either on-line or off-line processing. It includes paper vouchers and manual entries. Security requirements include policies and controls for sales vouchers, suspense accounts, and settlement

3.0 Developing a Security Plan

The purpose of the *EBT System Security Plan* is to allow the State to comply with computer security planning activities required by the Computer Security Act of 1987, and to identify the security safeguards that are in place and planned for the EBT System in order to mitigate potential risks that could result in unauthorized disclosure, modification, or destruction of sensitive information stored and processed on an EBT System

A security plan identifies security measures that have been incorporated and will be implemented into the EBT System to reduce or eliminate the risks and harm to the system. The security plan presents a complete picture of the security aspects of an EBT System.

The *Food and Nutrition Service (FNS) Handbooks 701, 702 and 901*; and Office of Management and Budget Bulletin 90-08 provide detailed guidance on developing security plans for Federal systems. The information provided in section 2 of this Security Handbook should be used as a guide for providing content for system security plans. The information provided below will outline the steps that should be followed when developing a security plan. Depending on the complexity of your system, your outline may be more extensive than the one provided below.

Step 1—System Identification. Characteristics of an EBT System should be defined, including the responsible organization, personnel responsible for the EBT System security, operational status, system functions, and system connectivity.

Step 2—Sensitivity of Information Handled. Sensitivity level of information processed on the system should be defined (e.g., sensitive but unclassified).

Step 3—System Security Measures. During this step, various types of security measures incorporated and planned in the EBT System should be identified.

3.1 System Identification

The first section of an Information Systems Security Plan consists of the information necessary to describe the system. This information includes:

- System Name and Title
- Responsible Organization – organization responsible for system operation
- Designated Points of Contacts – individuals to contact for system information
- System Category – Major Application or General Support System
- System Status – Under Development or Operational
- System Description – brief description of the system configuration
- System Environment – any environmental factors that cause special concern.

3.2 Sensitivity Of Information Handled

This section describes the degree of sensitivity of information assessed by an EBT system considering the requirements for:

- **Confidentiality**
- **Integrity**
- **Availability**

In addition, applicable laws and regulations that require protection of sensitive information, a description of EBT data sensitivity, and data protection requirements for integrity, confidentiality, and availability should be identified and described. This process should occur at the beginning of the information system's life cycle and be re-examined during each life cycle stage.

3.3 System Security Measures

This section describes the system security measures in-place or planned that is intended to meet the protection requirements of the EBT system. The security control measure should also be explained in general terms regarding its applicability to the EBT system. The following sections should be covered in section 3 of the security plan:

- *Management Controls*
- *Operational Controls*
- *Technical Controls*
- *EBT Specific Security Controls*

3.3.1 Management Controls

This section should include the information for management controls that should be identified and documented.

- Develop security policy and procedures that enforce EBT System security.
- Create local written procedures for implementing existing FNS policies at the regional and field office level.
- Designate an information system security officer (ISSO) in writing who is responsible for performing day-to-day security operations.
- Establish configuration controls for reviewing and approving security changes made to the EBT System hardware, software, and applications.
- Create procedures for reporting security incidents or irregularities (e.g., virus, hackers, software bugs).
- Conduct inventory of EBT System components.

- Determine status of a security program to be established for the EBT System.

- Designate a security manager responsible for overseeing the security program.

- Ensure security activities are incorporated in the security program, including:

  – Incorporate security specifications in the EBT System design documents
  – Conduct risk assessments, ST&E, and system security reviews
  – Develop of security documentation such as EBT System design document, security plan, contingency plans, and documents resulting from the security activities (e.g., risk assessment report, ST&E report)

- Determine status of the EBT System certification and accreditation (e.g., certified and accredited, interim approval to operate).

3.3.2 Operational Controls

This section should provide information for protecting computer output and electronic media.

a. Media Controls

- Computer Output Controls

  - Controls for handling, distributing, and storing computer output containing sensitive information
  - Methods for disposing computer output.

- Electronic Media Controls

  - Types of media to be used for the EBT System (hard disk, floppy diskettes, tapes)
  - Controls for labeling media
  - Procedures for destroying media when they are no longer needed.

b. Personnel Security

- Screening EBT personnel before they are authorized to work on the EBT system

- Screening contractors before they are authorized to work on the EBT System.

c. Physical Security

- Security mechanisms and features that provide access control to the facility and computer center (e.g., guards, keys, electronic access device)
- Visitors' access controls (e.g., visitors' log, temporary visitor badge, and escort).

d. Contingency Planning

- Status of the development of the EBT System contingency plan
- Individuals and organizations responsible for maintaining the contingency plan
- Regular testing schedules of the contingency plan.
- Periodic data backup (e.g., incremental, full)
- Storage of backup tapes
- Redundancy in communication devices and lines.
- Off-site storage facilities for backup tapes
- Alternate facilities within agency
- Hot sites.

e. Security Training

- Establish a security training program for the EBT System users that operate, use, and maintain the EBT System
- Create time frame of security training (e.g., initial training, periodic refresher training).

Identify subjects to be addressed during the security training sessions (e.g., protection of EBT cards, user IDs, PINs, passwords, EBT privacy act information).

3.3.3 Technical Controls

This section should include information for I&A, access controls, audit trail, network security and virus protection that should be identified and documented.

a. Identification and Authentication

- A list of the EBT System components (e.g., eligibility system, EBT processing terminals) that will use I&A mechanisms (e.g., user ID, password, biometrics)
- A diagram of system architecture including network connectivity
- Type of I&A to be used at each location (e.g., user name/password on the eligibility system, magnetic stripe card/PIN at POS terminals)
- Secure configuration of authentication mechanisms (e.g., periodic password change, password history and age, user account lockout after a specified number of invalid login attempts)
- Protection of authentication data
- User account maintenance to delete accounts of users no longer requiring access to the EBT System.

b. Access Control

- A list of EBT System components implementing access control measures
- An EBT System diagram detailing the relationships of all system components
- Type of access control measures to be used (e.g., user profile, limited access privileges)
- Controls to restrict access to the system from remote terminals (e.g., timeout feature)
- Separation of duties for dividing critical functions (e.g., operations, reconciliation, fund transfers) among different individuals

c. Audit Trail

- Status of audit mechanisms (e.g., enabled, disabled)
- Security events to be recorded in the audit trails
- Policy for reviewing audit trails and reporting suspicious system activity

d. Virus Protection

- Installation of anti-viral software in the EBT System
- Time frame of upgrading the anti-viral software
- Procedures for reporting virus incidents.

e. Communications Security

- Data Transaction Controls
  - Controls to detect and correct data errors in transmission
  - Controls to detect duplicate transactions
  - Availability of tools to detect deviations from the expected transaction patterns.
- Remote Controls
  - Security controls to restrict dial-in access (e.g., user ID, password, authentication devices)
  - Measures to monitor and/or restrict remote control of system components
  - Controls to terminate modem connections after a specified number of invalid login attempts
  - Methods for protecting the EBT System from unauthorized external networks (e.g., firewalls, and routers).
- Encryption
  - Controls to provide data confidentiality and integrity (e.g., Message Authentication Code [MAC])
  - Status of password and PIN encryption when they are stored and transmitted
  - Type of encryption algorithm used.
- Key Management
  - For protecting encryption keys when generated, distributed, and stored
  - For changing keys in a secure manner
  - For protecting keys from unauthorized access in the system and on the network while being retrieved.

f. Network Security

- For controlling access of data and software applications by user privileges.
- For determining sensitive and critical resources that need to be backed up on the network servers.
- For performing periodic review of network security using audit logs.

3.3.4 EBT System-Specific Controls

This section provides information regarding card generation, distribution, and destruction that should be identified and documented.

3.3.4.1 EBT Access Card Security

- Type of card(s) employed (e.g., magnetic card, smart card, hybrid card, laser card) and specific industry standards
- Card inventory controls
- Controls and procedures used in the storage, issuance, and disposal of EBT access cards, including blank cards, temporary card, and active cards
- Procedures for handling lost and stolen cards.

3.3.4.2 POS Terminal Security

This section provides information regarding on-line, off-line, and manual processing that should be identified and documented.

a. On-Line Processing

- Security mechanisms provided by the POS terminal(s) to restrict access to the terminals (e.g., user ID, password)
- Security mechanisms used to identify and authenticate recipients (e.g., card, personal identification number [PIN], biometrics).
- The detailed information to be contained in receipts.
- The controls to prevent fraudulent transactions in terms of settlement, refund transfer, and batch clearance (e.g., manager password).

b. Off-line Processing

- Securing transactions by using smart cards
- Protecting refund transactions
- Securing transactions by using biometrics.

c. Manual Processing

- Verification procedures for authorizing use of vouchers (e.g., retailer's FNS code)
- Maximum amounts to be used for manual processing
- Procedures for balancing, settlement, and reconciliation of a user's account after performing manual processing transactions

APPENDIX A1

CHECKLIST FOR ASSESSING SECURITY CONTROLS

Food & Nutrition Service Electronic Benefits Transfer System	**MANAGEMENT CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
IT Security Roles and Responsibilities			
1) Has an EBT System security program been established to conduct necessary security activities (i.e., development of a security plan, contingency plan, risk assessment, etc.)			
2) Is there a well-defined security plan enforced for EBT Systems?			
3) Is the security plan implemented throughout the life-cycle of the EBT System?			
4) Is the security plan reviewed and updated annually?			
5) Are security standards established for all aspects of the EBT processing environment?			
IT Security Program and System-Specific Policies			
1) Has an ISSO responsible for the EBT security program been designated in writing?			
2) Have the duties and responsibilities of the ISSO been defined in writing?			
3) Has the ISSO received sufficient training to perform his or her duties?			
4) Does the ISSO have sufficient time to perform his or her duties?			
Risk Management			
1) Has a specific timetable for conducting risk assessments been established (e.g., every 3 years, whenever a significant change to the EBT System hardware or software occurs and whenever changes occur in the security environment)?			
2) Has a risk assessment been performed prior to the approval of the EBT System design plan?			
3) Have the results of the risk assessment been documented and taken into consideration when implementing the EBT System?			
4) Are risk assessment reports kept in a secure location?			
5) Are action plans formulated to correct weaknesses after a risk assessment is performed?			
6) Is the system certified in writing by a management official before it becomes operational and after every subsequent risk assessment?			

Food & Nutrition Service Electronic Benefits Transfer System	**OPERATIONAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
Media Protection			
1) Are sensitive materials (e.g., retailer data) labeled properly when they are delivered or mailed?			
2) Are procedures for distributing, storing, and disposing computer output containing sensitive information established?			
3) Is computer output containing sensitive information distributed only to authorized personnel with need to know?			
4) Is computer output containing sensitive information stored in a secure environment (e.g., locked file cabinet)?			
5) Is computer output containing sensitive information shredded when it is no longer needed?			
6) Are sensitive reports containing EBT security features stored and distributed in a secure manner?			
7) Are copyright regulations applied to the EBT System?			
8) Are procedures in place to protect electronic media (e.g., diskettes, tape backups and CD-ROMs) containing sensitive data?			
9) Is access to the library limited to authorized personnel (e.g., librarian)?			
10) Are external labels affixed to tapes and diskettes indicating the contents of the tapes/diskettes?			
11) Is each magnetic tape marked with a serial number?			
12) Are electronic media inventory records maintained and updated regularly?			
13) Are procedures established so that electronic media are completely free of data before being reallocated or reassigned (e.g., reformatting and degaussing of hard drives)?			
Personnel Security			
1) Have personnel security policies been established and implemented?			
2) Has each personnel member been informed of his/her duties and responsibilities for protecting the EBT System and its resources?			
3) Are the consequences of violating system security clearly			

Food & Nutrition Service Electronic Benefits Transfer System	**OPERATIONAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
established?			
4) Are personnel informed of the risks to the system of both intentional and unintentional security breaches?			
5) Have all system users been screened before they are authorized to access the EBT System?			
6) Have all contractors been screened before they are authorized to access the EBT System?			
7) Are nondisclosure agreements established between the State and contractors?			
Physical Security			
1) Have appropriate facility security measures been incorporated to restrict access to the facility (e.g., security guards, electronic access devices)?			
2) Are public access points marked with visible signs informing people that the area is restricted?			
3) Is access to the computer center restricted to only authorized personnel and controlled through keys or electronic access devices?			
4) Is access to the computer center controlled through keys or electronic access devices?			
5) Are keys and access cards distributed to only authorized personnel?			
6) Are all keys and access cards taken away from employees within 24 hours of termination of employment?			
7) Are combinations changed regularly and whenever an employee who had access departs?			
8) Are the facility and the computer center locked when authorized personnel are not present?			
9) Is a visitors log in place at the computer center and the facility entrance(s)?			
10) Are all visitors required to sign into the visitors log?			
11) Are all visitors required to wear a temporary badge for identification?			
12) Are all visitors escorted by authorized personnel at all times?			

Food & Nutrition Service Electronic Benefits Transfer System	**OPERATIONAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
13) Are network file servers located in an area where access is restricted?			
14) Is unused and spare POS equipment stored in a controlled environment?			
15) Is access to the card storage facility restricted?			
16) Are controls in place to secure personal computers for the multilane POS retailer system?			
17) Are all telephone jacks, cables, and circuits labeled?			
Contingency Planning			
1) Has responsibility been assigned for the development and maintenance of a system contingency plan?			
2) Has a system contingency plan been developed?			
3) Does the contingency plan contain detailed information addressing emergency response, backup processing, and recovery actions?			
4) Are contingency plans tested regularly and then updated based on test results?			
5) Is the contingency plan consistent with the site disaster recovery program?			
6) Have critical applications and system elements been identified?			
7) Has critical equipment been inventoried and maintained?			
8) Are there notification procedures that provide hazard warnings, announcements, instructions, and locations of emergency services?			
9) Are telephone numbers and procedures to contact local law enforcement and emergency personnel readily available to all personnel?			
10) Are proper equipment maintenance schedules in place?			
11) Are standard operating procedures for bomb threats established and readily available to all personnel?			
12) Are all new employees required to have a “walk through” to become acquainted with emergency procedures?			

Food & Nutrition Service Electronic Benefits Transfer System	**OPERATIONAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
13) Are all employees trained for emergency procedures periodically to ensure that they stay current?			
14) Are critical data and system resources backed up regularly (e.g., incremental backup, full backup)?			
15) Is redundancy provided for communications, including communication devices and lines?			
16) Are all backup tapes labeled properly?			
17) Are all backup tapes stored in a secure environment?			
18) Are backup tapes regularly sent to the off-site facility (e.g., once per month)?			
19) For leased lines, is an automatic backup capability used to ensure that when a line fails, an automatic switchover is accomplished for the length of the outage?			
20) Is the Host system a fully fault-tolerant system (e.g., all components are duplicated and all files are mirrored)?			
Incident Response			
1) Has an incident reporting process been established to report breaches within EBT systems?			
2) Have all the employees who access EBT systems been trained to identify and report security incidents to the appropriate personnel?			
3) Are escalation procedures in place to report incidents to the appropriate law enforcement agencies?			
4) Are security incidents documented by the ISSO and appropriately resolved?			
5) Are incident reports protected based on the sensitivity level of the affected system or type of breach?			
Security Awareness, Training and Education			
1) Is a statewide security training program conducted for all persons involved in the use or management of EBT Systems?			
2) Are all employees required to complete security training before being allowed to use the system?			
3) Is the training program reviewed and revised periodically to correct deficiencies or reflect changes in EBT System security policies and procedures?			
4) Is a detailed record of security training for personnel kept			

Food & Nutrition Service Electronic Benefits Transfer System	**OPERATIONAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
that includes the person's name, the content of the training, and the date it was completed?			
5) Is there periodic security training after the initial training (e.g., every year)?			
6) Does training include users' responsibilities for protecting their passwords?			
7) Are all personnel given a review of their security responsibilities to keep EBT Privacy Act and other sensitive information confidential?			
8) Are the consequences of intentional and unintentional security breaches clearly explained?			
9) Are benefits recipients trained in the use of security features (e.g., do not reveal PINs, do not write PINs on cards)?			
10) Are benefit recipients provided with documents that inform them that they must abide by the rules of the EBT System (e.g., send out a pamphlet describing system rules and regulations)?			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
Identification and Authentication			
1) Has the ISSO been assigned responsibility for issuing, maintaining and deleting user accounts?			
2) Does the EBT System require users to identify themselves and provide proof of their identity (e.g., user identification (ID), password)?			
3) Is there a list of authorized users of the EBT System?			
4) Is the list of user accounts updated regularly?			
5) Is an individual user uniquely identified?			
6) Are shared passwords prohibited?			
7) Are users required to change their password at their first login and regularly thereafter (e.g., every 3 months)?			
8) Are all user IDs and passwords that are provided by contractors changed immediately?			
9) Does the system require minimum password length (e.g., 6 to 8 characters)?			
10) Are users required to select alphanumeric characters for their password?			
11) Is the clear-text representation of the password blotted out on the data entry device?			
12) Does the system prevent users from reusing old passwords for a specified period of time (e.g., 12 months)?			
13) Are user accounts disabled after a specified number of invalid login attempts (e.g., 3 times)?			
14) Are controls provided to protect authentication data from unauthorized deletion?			
15) Are user accounts disabled after a specified period of time of inactivity?			
16) Are user accounts and their passwords deleted immediately after a user is no longer authorized access to the system?			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
17) Are GUEST accounts disabled?			
18) Are procedures established for handling forgotten passwords?			
19) Are authorized users able to temporarily lock/disable user accounts?			
20) Are all recipients identified and authenticated before they access their benefits (e.g., card, personal identification number [PIN], biometrics)?			
21) Are controls in place for selecting PINs by the system or recipients (e.g., minimum PIN length, requirement for combination of alphanumeric characters)?			
22) Is a card deactivated after a specified number of unsuccessful PIN attempts (e.g., 3 times)?			
23) Is a recipient's account disabled immediately when the recipient is no longer eligible for benefits?			
24) Does the automated response unit (ARU) verify the identity of recipients when they call for forgotten PINs and lost or stolen cards?			
Logical Access Controls			
1) Is there a list of authorized users of the EBT System? Is the list up-to-date?			
2) Is access to files and/or processes restricted based on a user's functions and on a need-to-know basis?			
3) Is access canceled when the need to know no longer exists?			
4) Are warning banners displayed before users access sensitive information?			
5) Are system administrator privileges limited to specific authorized functions?			
6) Is *root* access limited only to a minimum number of personnel?			
7) Are users required to log off when they leave the system?			
8) Is a timeout feature provided to automatically log off a user after an extended period of inactivity (e.g., 20 minutes)?			
9) Are controls in place to prevent users from bypassing security checks to access the system?			
10) Are controls in place to prevent anyone but authorized staff from loading software onto network file servers?			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
11) Are user functions separated among system, security, and database administrators?			
12) Are system operations, reconciliation, and fund transfer duties segregated?			
13) Are all program changes controlled by a production turnover of the program to the operations staff which recompiles the programs into production?			
14) Are controls in place that no application development person is permitted to update any production file or program?			
15) Are duties that affect the account balance separated or controlled during processing?			
16) Are groups that authorize card replacement different from the groups that process the card replacement transactions?			
Auditing			
1) Is the EBT System enabled to generate audit trails?			
2) Do the audit trails record security-related events (e.g., unsuccessful logon attempts, changes to security policy and file access events)?			
3) Does the audit record of each event provide sufficient information, including date/time, user ID, terminal ID, type of access, and success/failure?			
4) Is access to audit trails restricted to authorized personnel (e.g., ISSO)?			
5) Are audit trails restricted to read-only access?			
6) Does the ISSO review audit trails regularly?			
7) Are controls in place to selectively audit the actions of one or more users based on individual identity?			
8) Are network audit tools used to detect unauthorized network activities?			
9) Does a mechanism exist for detecting unusual account activity?			
10) Is time period established to retain audit trails?			
11) Is a log of transmissions reviewed for accuracy by end users, security personnel, and auditors?			
12) Does the system provide a mechanism to log all transmission errors and retransmissions?			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
13) Does the system provide velocity reports that report exceptional usage on a card or retailer level?			
14) Have fraud detection methods been developed and incorporated into the EBT System to detect deviations from the expected pattern of benefits transactions?			
15) Do fraud detection methods incorporate a number of detection techniques instead of relying on only one or two techniques?			
Internet/Web Security			
Operating System			
1) Are all unnecessary programs and services eliminated?			
2) Are all unused ports on the system closed?			
3) Are default file permission more restrictive?			
4) Is verbose logging on the system (auditing) enabled?			
5) Is a CMOS/PROM password enabled?			
6) Is file-sharing features disabled?			
7) Does password and user accounts adhere to policies and guidelines?			
8) Have the most current system patches for the operating system been applied?			
WEB SERVER			
1) Is the Web server on a separate local area network (DMZ) from other production systems?			
2) Does the Web server have a trust relationship with any other server that is not also an Internet-facing server or server on the same local network?			
3) Is the Web server treated as an untrusted host?			
4) Is the Web server dedicated to providing web services only?			
5) Are compilers installed on the Web server?			
6) Are all services not required by the Web server disabled?			
7) Is the latest vendor software used for the Web server including all the latest hotfixes and patches?			
CGI SCRIPTS			
1) Is the ISSO aware of all CGI Scripts installed on a web server?			
2) Does the directory containing CGI scripts have permissions of			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
read/write/execute for owner and execute-only for group and others?			
3) Are all CGI scripts owned by root or administrator.			
4) Does all CGI scripts have permissions of read/write/execute for owner and execute-only for group and others?			
5) Are all backup copies of CGI scripts that are automatically generated removed from the system?			
6) Has the ISSO documented all CGI used on the web server?			
7) Does each CGI script use a common directory for temporary files and once that task is completed, delete the temporary file?			
8) Does the ISSO ensure that no CGI script source files exist in the web server document directories?			
9) Are all CGI scripts centrally stored in the cgi-bin (or equivalent) directory?			
Network Security			
Firewalls			
1) Are firewalls that are accessible from the Internet configured to detect intrusion attempts and issue an alert when an attack or attempt to bypass system security occurs?			
2) Are EBT firewalls configured to maintain audit records of all security-relevant events? Are the audit logs archived and maintained in accordance with applicable records retention requirements and this guidance handbook?			
3) Is firewall software kept current with the installation of all security-related updates, fixes or modifications as soon as they are tested and approved?			
4) Are EBT firewalls configured under the "default deny" concept. (*This means that, for a service or port to be activated, it must be approved specifically for use*.)			
5) Are the minimum set of firewall services necessary for business operations enabled and only with the approval of the ISSO?			
6) Are all unused firewall ports and services are disabled?			
7) Are all publicly accessible servers located in the firewall DMZ or in an area specifically configured to isolate these servers from the rest of the EBT infrastructure?			
8) Does EBT firewalls filter incoming packets on the basis of Internet addresses to ensure that any packets with an internal source address, received from an external connection (IP Spoofing), is rejected?			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
9) Are EBT firewalls located in controlled access areas?			
Routers and switches			
1) Access to EBT routers and switches is password-protected in accordance with FNS guidance.			
2) Only the minimum set of router and switch services necessary for business operations is enabled and only with the approval of the ISSO.			
3) All unused switch or router ports are disabled.			
4) EBT routers and switches are configured to maintain audit records of all security-relevant events.			
5) EBT router and switch software is kept current by installing all security-related updates, fixes or modifications as soon as they are tested and approved for installation.			
6) Any dial-up connection through EBT routers must be made in a way that is approved by the ISSO.			
Database Security			
DATABASE FILE SYSTEM INTEGRITY			
1) Are procedures in place to ensure that Database COTS software is not modified from its installation defaults to be more permissive?			
2) Are procedures in place to ensure that all directories created by the installation of a RDBMS are modified to be more permissive?			
3) Are procedures in place to ensure that any groups created by the installation of a RDBMS are not modified to be more inclusive?			
4) Are procedures in place to ensure that any file permissions created by the installation of a RDBMS are not modified to be more permissive?			
5) Are procedures in place to ensure that End users are never allowed to change any directory names, file permissions, or group information associated with the database software?			
6) Have all default and vendor installation accounts been deleted from the system?			
DATABASE BACKUP AND RECOVERY			
1) Has a database back			
2) Are scripts or vendor supplied scripts available for use to back			
3) Has the database back			

Food & Nutrition Service Electronic Benefits Transfer System	**TECHNICAL CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
4) Has the database back			
Virus Protection			
1) Is an anti-virus program installed on the EBT System?			
2) Are all software applications scanned for viruses prior to installation?			
3) Are the virus definitions of the anti-virus program continually updated to protect the EBT System from the most recent viruses?			
4) Are system users notified regarding virus threats and incidents?			
5) Are system users required to run anti-virus software regularly?			

Food & Nutrition Service Electronic Benefits Transfer System	**EBT SPECIFIC CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
EBT Access Card Security			
1) Are EBT access cards manufactured following International Organization for Standardization (ISO) procedures (e.g., materials, card dimensions, encoding of tracks, embossing, and magnetic stripes)?			
2) Are inventory control procedures in place for blank, voided, spoiled, or unusable card stock?			
3) Is the card inventory log updated regularly?			
4) Is EBT blank card stock stored in a secure and restricted access environment?			
5) Are internal controls established to prevent employees from creating duplicate cards or mailing cards to unauthorized addresses?			
6) Do temporary cards show only a card and generation number?			
7) Are temporary cards removed from the system after they expire?			
8) When a card is reported as lost or stolen, is it deactivated immediately?			
9) Are lost or stolen cards replaced and never reissued?			
10) Are lost, stolen, and damaged cards blocked before being replaced?			
11) Is card embossing and encoding equipment tamper resistant?			
12) Are card number prefixes registered with the appropriate agencies?			
13) Are controls in place for returned or recycled cards (e.g., wiped of transactions)?			
14) Are card numbers generated for all card orders?			
15) Are cards and PINs mailed to recipients separately and on different days?			
16) Are cards and PINs that do not reach their delivery destination deactivated and destroyed properly?			
17) Is a card's lifetime determined (e.g., 2 years)?			
Is card usage determined (e.g., 200 transactions over the card's lifetime)?			
SMART CARDS			
1) Does the smart card operating system (COS) follow ISO 7816 standards for interfacing to card acceptor devices?			
2) Can the COS detect and stop duplicate posting of			

Food & Nutrition Service Electronic Benefits Transfer System	**EBT SPECIFIC CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
transactions?			
3) Is bi-directional verification and authentication provided by the COS between the smart card and a card acceptor device?			
4) Does the COS incorporate Data Encryption Standard (DES) based encryption and decryption capability? Public key?			
5) Is the COS capable of generating a message authentication code based on DES security algorithms?			
6) Does the COS employ a secure method to replace the smart card's key used in security processing?			
7) Does the COS control all access to data stored within the card based on access rules?			
8) Does the COS disable the chip after a number of repeated presentation of invalid PINs?			
9) Does a method exist for performing bulk erasure of the smart card's chip memory?			
10) Are keys that allow value-adding transactions stored only on the EBT Host and the smart card itself?			
11) Does each card have a unique key so that the rest of the card population is not jeopardized if the key is broken?			
12) If a multi-application card is used, does the COS facilitate having different security keys for each application on the card?			
13) In case of multi-application cards, do all applications expire on the same date?			
14) Are separate read/write keys available for each application on the card?			
15) Does each transaction created using the smart card generate a unique number to be used in reconciliation and audit purposes?			
16) Are cards given expiration dates?			
17) Are master keys and private keys replaced at least as frequently as the card’s expiration cycle?			
18) Is there a secure procedure to wipe out the memory and to destroy the chip before cards are destroyed?			
19) When cards are recycled, does a procedure exist to effectively delete previously stored data on the card so no residual information (e.g., encryption keys, PINs) remains?			
20) Once used by the biometric verification unit, is the biometrics template discarded so its data are not retrievable?			
21) Is the biometric template on the card stored in encrypted form?			

Food & Nutrition Service Electronic Benefits Transfer System	**EBT SPECIFIC CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
22) Is the backup method of authentication (e.g., PIN, password) used if the biometric verification unit is not functional?			
HYBRID CARD			
1) Does the hybrid card confirm to the most recent applicable ISO standards?			
2) Are controls in place to reload additional benefits on the hybrid card chip memory?			
3) Are controls in place to change or delete the recipient's information written on the card chip in a secure manner?			
4) Does the hybrid card support PIN encryption and decryption by software on the smart chip?			
5) Are controls in place to prevent loopholes that allow the magnetic stripe to be used as a secondary access technology in case smart card is not functional?			
OPTICAL CARD			
1) Are the data on the card encrypted?			
2) Are the encryption keys stored in a secure manner by the system (e.g., PC, Host)?			
3) Are techniques, such as laser etchings, being used to make the card more counterfeit proof?			
POS Terminal and ATM Security			
1) Are POS terminals validated before commencing on-line operations?			
2) Can authorization or rejection of purchase amounts be obtained at the POS terminal?			
3) Is the POS terminal restricted from displaying benefit balances?			
4) Does the receipt print any failed message (e.g., void) to acknowledge transaction failure?			
5) Does the POS terminal receipt contain sufficient information to help track any fraudulent transactions?			
6) Does the POS receipt include a cashier/clerk identification to help track any fraudulent transactions?			
7) Are error messages displayed at POS devices (e.g.,			

Food & Nutrition Service Electronic Benefits Transfer System	**EBT SPECIFIC CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
insufficient funds)?			
8) Is manager password required for refund transactions, batch clearance, end of day settlement, and system maintenance to prevent unauthorized transaction processing?			
9) Is the POS terminal authenticated at the beginning of every settlement call to the EBT host?			
10) Are controls in place to render a suspected fraudulent retailer POS terminal(s) inoperable in a specified period of time (e.g., terminal deactivation parameter)?			
11) Does the terminal incorporate self-diagnostics so that it can inform the central system of any malfunction or attempt to tamper with it?			
12) In case of using one-to-many matching with biometrics, is the biometric template encrypted as it is sent on-line to the central verification unit?			
OFF-LINE PROCESSING			
1) Are POS terminals validated before commencing on-line operations?			
2) Can authorization or rejection of purchase amounts be obtained at the POS terminal?			
3) Is the POS terminal restricted from displaying benefit balances?			
4) Does the receipt print any failed message (e.g., void) to acknowledge transaction failure?			
5) Does the POS terminal receipt contain sufficient information to help track any fraudulent transactions?			
6) Does the POS receipt include a cashier/clerk identification to help track any fraudulent transactions?			
7) Are error messages displayed at POS devices (e.g., insufficient funds)?			
8) Is manager password required for refund transactions, batch clearance, end of day settlement, and system maintenance to prevent unauthorized transaction processing?			

Food & Nutrition Service Electronic Benefits Transfer System	**EBT SPECIFIC CONTROLS**		
Security Controls	**YES**	**NO**	**Comments**
MANUAL PROCESSING			
1) Does the POS voucher include a cashier/clerk identification to help track any fraudulent transactions?			
2) Does the POS voucher contain the transaction type, purchase amount, remaining balance, date of transaction, and account code or receipt code?			
3) Is a "ceiling-limit" policy used that limits the amount of the purchase when the POS voucher is used?			
4) Are there controls of the timely submission of vouchers within a specified period of time (e.g., 7 to 10 days)?			
5) Are manual authorization forms stored in a secure environment?			
6) Is there a placement of "holds" on an account until the paperwork is received?			
7) Are "suspense" accounts used that do not disburse funds to the merchant until the transaction amount can be reconciled with the paper voucher?			
8) Does the ARU verify cardholders before manual processing is authorized?			

APPENDIX A2

SAMPLE ELECTRONIC BENEFIT TRANSFER SYSTEM RISK ASSESSMENT REPORT OUTLINE

This sample risk assessment report outline provides the general content guidelines of suggested major sections of a risk assessment report. Remember that this is a guideline; some sections may not be applicable, and additional sections may be necessary. Section 2 of the EBT Security Guideline Handbook explains how to collect the information used to develop the risk assessment.

APPENDIX A2-SAMPLE ELECTRONIC BENEFIT TRANSFER

SYSTEM RISK ASSESSMENT REPORT OUTLINE

EXECUTIVE SUMMARY

Provide a brief description and purpose of the EBT System. State the objectives of the risk assessment and provide a summary of whether the information processed on the EBT System is adequately protected from identified risks. Finally, provide information concerning the findings and countermeasures taken or recommended to be taken. This information may be presented in the form of a chart as in Table ES-1.

Table ES-1
Risk Assessment Findings Summary

Finding	Risk Level	Recommendation
In this cell, state how the security consideration was found to be in noncompliance and how it is a threat or vulnerability.	*In this cell, rate the risk level associated with the finding in terms of high, medium or low.*	*In this cell, cite recommended countermeasures to minimize or eliminate the risk.*

1.0 INTRODUCTION

Provide organizations and names of those conducting the risk assessment. Provide type (i.e., design, implementation) of current risk assessment. Briefly describe the existing security profile, including known threats prior to this risk assessment and existing security countermeasures. Provide disposition of previous findings.

1.1 Purpose

Discuss the purpose of the risk assessment.

1.2 Scope

Describe to what extent of the EBT System the risk assessment encompassed. For example, the scope may have been the entire system or may have been specific, focusing on geographic area, type of threat, or security considerations of a major security element (i.e., computer security).

1.3 Document Layout

Briefly describe the purpose and contents of the remaining sections of the report.

2.0 RISK ASSESSMENT METHODOLOGY

Briefly describe the approach or methodology used to perform the risk assessment. Provide a list of the steps taken in performing the risk assessment with detailed descriptions of how the steps were accomplished provided in subsections. A possible organization of these steps might be the following:

2.1 System Identification

2.2 Threats Identification

2.3 Vulnerabilities Determination

2.4 Risks and Impacts Determination

2.5 Countermeasures Selection

3.0 SYSTEM DESCRIPTION - Describe the EBT System in detail. A possible organization of this section might be as follows:

3.1 System Components

3.2 System Connectivity

3.2.1 Network Topology
3.2.2 Connections to Services

3.3 Information Attributes

3.4 System Users

4.0 SECURITY SAFEGUARDS

4.1 Computer Security—Describe security controls in place for the EBT System in the areas of identification and authentication, discretionary access control, audit, and object reuse.

4.2 Communications Security—Describe security controls in place for the EBT System in the areas of data transmission protection, access to routers and communications servers, dial-in access restrictions, and key management.

4.3 Administrative Security—Describe security controls in place for the EBT System in the areas of security policy and procedures, security program, security training, periodic data backup, virus protection, and security documentation.

4.4 Physical Security—Describe security controls in place for the facility and the computer center housing the EBT System components in the areas of security guards, a visitors log, visitor badges and escort, and key/combination controls.

5.0 RISK ASSESSMENT RESULTS

The suggested organization of this section is as follows:

- Finding
  - Detailed description of the specific finding

- Risks/Impact
  - Discussion of threats and vulnerabilities resulting from non-compliance
  - Discussion of the risk/impact to the agency

- Risk Analysis
  - Determination of the risk level based on the following:
  - The likelihood that a threat will exploit a vulnerability
  - The impact that the successful exploitation of the vulnerability will have on the agency.

- Risk Mitigation (countermeasures) to minimize or eliminate the risk. These recommendations should be cost-effective procedural and/or technical security controls.

6.0 CONCLUSION

Provide a brief statement concerning the adequacy of the security measures provided for the EBT System based on the compliance with security considerations throughout the system's life cycle. Provide information concerning the findings and countermeasures taken or recommended to be taken. This information may be presented in the form of a chart as in Table 6-1. Finally, rate the overall risk to the organization's operations in terms of *high*, *medium*, or *low*.

Table 1
Risk Assessment Findings Summary

Finding	Risk Level	Recommendation
In this cell state how the security consideration was found to be in noncompliance and how it is a threat or vulnerability.	In this cell, rate the risk level associated with the finding in terms of high, medium, or low.	In this cell, cite recommended countermeasures to minimize or eliminate the risk.

Appendices

Possible appendices could include a list of threats that apply to the organization, a copy of the checklist of security considerations, and any worksheets used to the conduct the risk assessment.

APPENDIX A3

SAMPLE ELECTRONIC BENEFITS TRANSFER CONTINGENCY PLAN OUTLINE

This contingency plan outline provides the general content guidelines of suggested major sections of a contingency plan. Remember that this is a guideline; some sections may not be applicable and additional sections may be necessary. Section 2 of the EBT Security Guideline Handbook explains how to collect the information used to develop the contingency plan.

APPENDIX A3-SAMPLE ELECTRONIC BENEFITS TRANSFER SYSTEM CONTINGENCY PLAN

1. INTRODUCTION

Describe the organizational structure (including names) of personnel developing the contingency plan, the mission of the organization, and the primary functions of the EBT System.

1.1 SCOPE

Describe the EBT System components to which the contingency plan applies.

1.2 PURPOSE

Describe the purpose and objectives of the contingency plan.

1.3 ASSUMPTIONS

Describe a list of disaster scenarios, both natural and manmade, that could most likely affect the EBT System and that may cause the contingency plan to be put into effect.

1.4 CLASSIFICATION OF THE EBT SYSTEM

Describe the sensitivity level of the EBT System (e.g., sensitive but unclassified) and the criticality level of the system in terms of critical, essential, important, or non-critical.

Classification			Description
	1	Critical	• Can only be performed by computers. • No alternate manual processing capability exists.
√	2	Essential	• Can be performed manually. • Manual procedures are available and would be implemented until the computer application or system is restored.
	3	Important	• No computer system or application is needed. • Can be performed manually. • Manual procedures are available. • Will revert totally to manual procedures.
	4	Non-Critical	• Can be delayed until the damaged site is restored and/or a new computer system is purchased.

1.5 RESPONSIBILITIES

Provide a list of personnel responsible for developing, executing, and maintaining the EBT System Contingency Plan and their responsibilities.

1.6 DOCUMENT CONTROL

Describe document controls throughout the life cycle of the EBT System, including the distribution and storage of the document.

2.0 PREPARATORY ACTIONS

Describe detailed information on critical resources that need to be maintained and updated to provide for the continuity of operations in case of an emergency.

2.1 KEY PERSONNEL

Provide a list of key EBT administrative and technical personnel, including names, addresses, and phone numbers. Also include a description of their responsibilities when they receive notification of an emergency.

2.2 DATA

Provide a list and description of critical EBT data needed to continue processing in the event of a disaster or system failure. Include the frequency of and procedures for performing backups of critical files.

2.3 SOFTWARE

Provide a list and description of critical EBT software needed to continue processing in the event of a disaster or system failure. Include the frequency of and procedures for performing backups of critical files. Also include a list of vendors' names, points-of-contact, and phone numbers.

2.4 HARDWARE

Provide a list and description of critical EBT software needed to continue processing in the event of a disaster or system failure. Include a list of vendors' names, phone numbers, and serial or product numbers of each hardware item.

2.5 COMMUNICATIONS

Provide a description of on-site and backup facility communication requirements. This description should also include alternate communication requirements in case the primary system fails.

2.6 SUPPLIES

Provide a list of critical EBT supplies by name and stock number. Include both the vendors responsible for providing the supplies and the location of the supplies at the backup site.

2.7 TRANSPORTATION

Describe the procedures for emergency transportation of personnel and equipment to the backup site. List who is responsible and what equipment is needed for providing the transportation.

2.8 OFF-SITE FACILITIES

Describe the location of the off-site storage facilities that store backup tapes and personnel responsible for maintaining the backup tapes. In addition, describe backup site's space requirements, including a layout of the facilities, needed for mission-essential operations only.

2.9 POWER AND ENVIRONMENTAL CONTROLS

Identify power requirements, temperature controls, and humidity controls necessary for continued EBT operations.

2.10 SYSTEM MAINTENANCE

Describe preventive maintenance and remedial maintenance that will be provided by a contractor during the prime period of maintenance (PPM), 7:00 a.m. to 5:00 p.m. Monday through Friday.

2.11 DOCUMENTATION

List EBT System documentation that contains information related to critical EBT System functions and security features, and that needs to be kept at off-site storage facilities.

2.12 TESTING

Provide testing plans and schedule for the EBT contingency plan to ensure that an effective recovery is possible. Provide personnel responsible for testing the contingency plans and their responsibilities.

2.13 AGREEMENTS AND CONTRACTS

List and describe any agreements and contracts executed with vendor representatives to run and maintain the EBT processing facility at the backup location.

3.0 ACTION PLANS

Provide descriptions of identified contingency scenarios. Include step-by-step, detailed procedures on what actions are required to continue EBT operations in the event of an emergency, when those actions are to be initiated, and who performs the actions.

3.1 EMERGENCY RESPONSE

Provide instructions for responding to emergencies. This section may contain various actions, including immediate actions to be taken, situation assessment, and notification procedures.

3.2 BACKUP PROCESSING

Describe detailed actions to be taken on an interim basis until full capacity is restored in case when a computer center is disabled temporarily, or hardware/software is destroyed. Identify and prioritize the minimally acceptable level of operation of the system's essential functions so that the contingency plan accomplishes the priorities.

3.3 RECOVERY ACTIONS

Describe detailed procedures to be taken to resume normal operations, including requisition of hardware, retrieve and installation of backup software and data, or proper configuration of security mechanisms.

4.0 REPORTING REQUIREMENTS

Describe any requirements for reporting to local, state, and federal agencies.

APPENDIX A4

GLOSSARY

APPENDIX A4—GLOSSARY

Access Control

Procedures designed to limit access to EBT system information and physical components to authorized users.

Audit Trail

A chronological record of system activities that is sufficient to reconstruct and review the sequence of events surrounding or leading up to all transactions and actions performed on or by the system.

Authentication

A protective measure designed to verify the identity of the originator of information transmitted, received or processed by the EBT System.

Batch

Multiple transactions that have been grouped into a single file representing the transactions for a single accounting period (typically 24 hours).

Benefit Period

Time frame that EBT food stamp benefits are authorized.

Biometrics Verification System

A system that uses a physical characteristic of an individual such as a fingerprint or retinal scan to uniquely identify the individual

Code

A set of rules governing the way in which data may be represented.

Communications Security

Protection provided to the EBT System to protect data that is transferred using communication lines. This includes ensuring that transactions are not invalid, incomplete, or altered.

Confidentiality

The process of ensuring that data is not disclosed to individuals not authorized to access it.

Configuration Control

The process of controlling modifications to the EBT System and to System documentation. Configuration Control protects the System against unintended and unauthorized modifications.

Contingency Plan

A plan of action to restore the EBT system's critical functions in case normal processing is unavailable for reasons such as fire, flood or civil disturbance.

Data

A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing.

Data Structures

A system of relationships between items of data.

Default

In programming and operating systems, pertaining to the choice selected in the absence of specific instructions by the user.

Electronic Benefits Transfer

An electronic payments system that uses electronic funds transfer, automated teller machines, and point of sale technology for the delivery and control of public assistance benefits.

Electronic Funds Transfer

A system designed to conduct the exchange of funds electronically.

Electronic Media Control

Procedural control of computer output, diskettes, and other storage media.

Encrypt

To convert plain text into unintelligible form by means of a cryptographic system. The process disguises information so unauthorized individuals cannot understand it.

Encryption

See Encrypt

Hacker

An individual whose interests – either benign or malicious – concern "breaking into" computer systems.

Host
A computer – usually a mainframe – that processes on-line transactions.

Identification

A code, user name, cards or token that identifies an individual.

Issuer

The issuer is a financial institution that issues payment cards and is responsible for payment to entities that accept the card instead of cash payment. Issuer often describes the contractor responsible for operation of an EBT system.

Key

When used in the context of encryption, a series of numbers which are used by an encryption algorithm to transform plain text data into encrypted (cipher text) data, and vice versa.

Manual Processing

Transactions that are processed using non-electronic processing methods such as paper vouchers and manual entry of transactions into the system.

Media Control

Protection against the unauthorized disclosure, manipulation destruction or alteration of information. Includes the storage, retrieval and disposal of data used by the EBT system.

Object

As defined by the DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria* (the "Orange Book"), an object is a 'passive entity that contains or receives information.' Examples include bits and bytes, records, files, databases, buffers, increases in memory size to devices such as printers, and even complete systems.

On-line Processing

Processing that involves transactions communicated over a communications line.

Off-line Processing

A system for transactions relayed to a processor for payment without immediate deduction from the user's account. Transactions of this type include those originated with smart cards or vouchers.

Need-to-Know

The need to have access to, knowledge of or possession of specific information in order to carry out official duties.

Password

A protected word, phrases, or a string of characters that is used to authenticate the identity of a user.

Personnel Security

Procedures established to ensure that all personnel that have access to any sensitive information have the required authorization as well as appropriate clearances.

Personal Identification Number (PIN)

A unique alphanumeric code assigned to a recipient and used to control access to individual accounts.

Point of Sale

Refers to the location where a purchase is made.

Point of Sale (POS) Device

Typically refers to equipment (e.g., terminal, PIN pad and printer) deployed at a retail location used to electronically submit financial transactions and record the results of the

approval process. Typically, a POS device will contain certain administrative functionality.

Read Protected

A control utilized to protect information from modification by allowing users the right to read the information but not write to it.

Reconciliation

The process that accounts for transactions that have occurred over a logical period of time, typically 24 hours. The reconciliation process usually reads records of transactions placed into independent log files and prints a report that shows either the transactions matched in all details, or where discrepancies were found.

Risk Assessment

The assessment of the vulnerabilities of and threats to people and systems involved in storing and processing sensitive data.

Security Plan

A document which depicts a State's plan for securing its EBT System.

Security Testing

The process of testing the security safeguards that have been implemented into the EBT system.

Sensitive Information

Information that if improperly used or disclosed could adversely affect the ability of the EBT system to protect EBT funds or to ensure that Privacy Act information about individuals and retailers is not disclosed.

Settlement

The process of transmitting funds to parties after transactions have been posted to accounts.

Smart Card

A type of plastic card that uses an embedded microprocessor chip to store information about an individual and to process and store transactions.

State(s)

A term that will refer to any State, County, region or consortium that is developing an EBT program.

State Administrative Representative

Any person that has been delegated responsibility for the State's FNS program and for controlling the expenditure of FNS funds on the EBT System.

Subject

Active entity that can make a request to perform an operation on an object (e.g., a process or device acting on behalf of a user, and in certain cases the actual user.)

System Security Review

An evaluation of the security controls that are in place to protect an electronic system based on an examination of applicable regulations and the risk assessment document for the system.

Terminal

An electronic device consisting of a visual display unit and keyboard or keypad that allows a user to interact with the EBT System (includes administrative terminals, POS Devices, ATMs).

Third-party processor

A company that acquires transactions from its customers and forwards those transactions to the issuer. The third-party processor operates and maintains retailer POS terminals, authorizes and processes transactions, and settles retailer accounts.

Threat

Any circumstance or event with the potential to cause harm to a system or activity.

Virus

A self-executing program that is hidden from view and that secretly makes copies of itself in such a way as to "infect" parts of the operating system and/or application programs. Viruses may sometimes be benign (e.g., display a message or a picture on the screen), but are usually intended to cause harm to the system (e.g., erase files, change dates).

Vulnerability

A weakness in a system's design or procedure that could be exploited by a threat to gain unauthorized access to a system.

APPENDIX A5

ACRONYMS

APPENDIX A5—ACRONYMS

AIS	Automated Information System
ATM	Automated teller machine
AV	Antivirus
CI	Configuration Item
CM	Configuration Management
CMDB	Configuration Management Database
CPU	Central Processing Unit
DES	Data Encryption Standard
DMZ	Demilitarized Zone
EBT	Electronic benefits transfer
EFT	Electronic funds transfer
FNS	Food and Nutrition Service
ID	Identification
ISSO	Information System Security Officer
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PC	Personal Computer
PIN	Personal Identification Number
POS	Point of Sale
RDBMS	Relational Database Management System
USDA	United States Department of Agriculture

APPENDIX A6

REFERENCES

APPENDIX A6—REFERENCES

Department of Agriculture. FCS Handbook 701, FCS Information Systems Security Policy Handbook. October 1996.

Department of Agriculture. FCS Handbook 702, FCS Information Systems Security Standards and Procedures Handbook. November 1997.

Department of Agriculture. FCS Handbook 901, Advance Planning Document (ADP) Handbook, Number 92-3, April 7, 1992.

Department of Agriculture. Guidelines for Preparation and Review of On-line EBT System Design Plans. April 1993.

Department of Agriculture. Price Waterhouse, EFT Security Assessment and Implications for EBT. April 1, 1994.

Department of Agriculture. Guidelines for Preparation and Review of EBT System Acceptance Test Plans. April 1993.

Department of Agriculture. ADP Security Guide for State and Local Agencies (Draft).

Department of Agriculture. EBT Smart Card Commands - A Functional Specification (Draft). September 19, 1994.

Code of Federal Regulations (CFR) Title 7 - Agriculture part 235. "State Administrative Expense Funds". Revised January 1, 1994.

Code of Federal Regulations (CFR) Title 7 - Agriculture part 246. "Women, Infant and Children (WIC)". Revised January 1, 1994.

Code of Federal Regulations (CFR) Title 7 - Agriculture part 271. "Food Stamp Program". Revised January 1, 1994.

Code of Federal Regulations (CFR) Title 7 - Agriculture part 274. "Issuance and use of coupons". Revised January 1, 1994.

Code of Federal Regulations (CFR) Title 7 - part 3015. "Uniform Federal Assistance Regulations". Revised January 1, 1994.

Code of Federal Regulations (CFR) Title 7 - part 3016. "Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments". Revised January 1, 1994.

National Institute of Standards and Technology (NIST), Special Publication 800-12, *An Introduction to Computer Security:* The NIST Handbook, October 1995

National Institute of Standards and Technology (NIST), Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, January 2002

Office of Management and Budget. Circular Number A-130, "Management of Federal Information Resources". Revised February 8, 1996.