UNITED STATES
POSTAL SERVICE®

Information Security for Mail Processing/Mail Handling Equipment

Handbook AS-805-G

March 2004
Transmittal Letter

Explanation

Increasing security across all forms of technology is an integral part of the Postal Service's Transformation Plan. This handbook establishes the policies and requirements for information security for the Mail Processing Equipment and Mail Handling Equipment (MPE/MHE) environment not addressed in Handbook AS-805, *Information Security.*

Distribution

This document is available on the Postal Service Intranet at *http://blue.usps.gov/cpim/hbkid* and at *http://it/security*.

Comments and Questions

Submit comments and questions to this address:

CORPORATE INFORMATION SECURITY OFFICE
UNITED STATES POSTAL SERVICE
4200 WAKE FOREST ROAD
RALEIGH NC 27668-1510

Comments may also be sent by e-mail to *iscomm@email.usps.com*. Use "AS-805-G" in the subject header.

Effective Date

This handbook is effective immediately.

Robert L. Otto

Robert L. Otto
Vice President
Chief Technology Officer

Contents

1 Introduction 1

1-1 Policy 1

1-2 About This Handbook 1

1-2.1 Purpose 1

1-2.2 Audience 1

1-3 The MPE/MHE Environment 2

1-3.1 Description 2

1-3.2 Functions 2

2 Roles and Responsibilities 3

2-1 Vice President, Engineering 3

2-2 Vice President, Network Operations Management 3

2-3 Manager, Corporate Information Security Office 4

3 Supplemental Information Security Requirements 5

3-1 About This Chapter 5

3-2 User Identification and Authorization 5

3-2.1 Logon IDs 5

3-2.2 Passwords 5

3-3 Hardware and Software 6

3-3.1 Establishing Hardware/Software Criteria 6

3-3.2 Hardening Servers 6

3-3.3 Using Only Approved Products 6

3-4 Software 6

3-4.1 Commercial Off-the-shelf Software 6

3-4.2 Third-Party Software 7

3-5 Hardware 7

3-5.1 Protection 7

3-5.2 Installation and Deployment 7

3-6 Research and Development (R&D) 7

3-6.1 Separation of Test and Production Environments 7

3-6.2 Pilots and Proofs of Concept 7

3-6.2.1 Information Security Assurance (ISA) 7

3-6.2.2 Change Management 7

3-7 Engineering Processes — Integrity Standards 8

3-8 Information Security Assurance 8

3-8.1 Initiating ISA 8

3-8.2 Reinitiating ISA 8
3-9 Secure Enclaves 9
3-9.1 Description 9
3-9.2 Implementation 9
3-9.3 Determining When a Secure Enclave is Required 9
3-10 Audit Log Requirements 10

Glossary 11

1 Introduction

1-1 Policy

It is the intention of the Postal Service to maintain a managed and integrated information security posture that protects its business and administrative objectives and responsibilities and enables it to fulfill its role as a critical national resource. These business and administrative objectives and responsibilities include those related to the Mail Processing Equipment/Mail Handling Equipment (MPE/MHE) environment.

1-2 About This Handbook

1-2.1 Purpose

This handbook:

a. Covers policies and requirements that apply to the MPE/MHE private network environment that are not addressed in Handbook AS-805, *Information Security*.

b. Acknowledges that the MPE/MHE environment, by the nature of its infrastructure, associated information resources (devices), and processes, has certain specialized requirements.

c. Presents the related information security policies and the conditions under which they can be implemented to support cost-effective and risk-based alternative processes and mitigating security controls for the MPE/MHE private network environment.

1-2.2 Audience

This handbook applies to everyone who performs activities associated with the MPE/MHE environment, including Postal Service employees, contractors, and vendors. Specific functional roles that support information security in the MPE/MHE environment are identified in Chapter 2, Roles and Responsibilities.

1-3 The MPE/MHE Environment

1-3.1 Description

The MPE/MHE environment includes the computer systems and networks that manage, monitor, and control mail processing functions; collect workload statistics from the MPE/MHE environment; and transmit control data or production statistics between the MPE/MHE environment and other Postal Service information systems.

1-3.2 Functions

The MPE/MHE computer systems and networks control such functions as facing, canceling, optical character reading, address lookup, bar code sorting, letter sorting, flat sorting, parcel sorting, sack sorting, mail tray transport, mail forwarding, mail weighing, electronic mail processing, and electronic monitoring.

2 Roles and Responsibilities

2-1 Vice President, Engineering

The vice president, Engineering, is responsible for the following:

a. Ensuring that Postal Service policies and procedures governing information resource security are followed when acquiring, developing, and maintaining the information resources used to support the MPE/MHE.

b. Protecting other Postal Service resources from the impact of the policies defined in this document and funding appropriate compensating controls.

c. Deciding which third-party software sponsored by Engineering will be accepted for use in the MPE/MHE environment, assuming responsibility for the deployment of the software, and getting the software registered with Infrastructure Tool Kit (ITK).

d. Ensuring that due diligence is applied to protect Postal Service information resources in the Postal computing environment from negative impacts that could result from testing if the test and production environments cannot be separated (see Handbook AS-805, Chapter 8, System, Applications, and Product Development).

e. Defining the criteria for audit logging for the MPE/MHE environment.

2-2 Vice President, Network Operations Management

The vice president, Network Operations Management, is responsible for the following:

a. Implementing information security for the mail and for the information resources or devices used to support MPE/MHE strategies, logistics, and operations.

b. Protecting other Postal Service resources from the impact of the policies defined in this document and funding appropriate compensating controls.

c. Deciding which third-party software sponsored by Network Operations Management will be accepted for use in the MPE/MHE environment, assuming responsibility for the deployment of the software, and getting the software registered with ITK.

d. Applying due diligence to protect Postal Service information resources in the Postal Computing Environment from negative impacts that could result if the test and production environments cannot be separated (see Handbook AS-805, Chapter 8, System, Applications, and Product Development).

2-3 Manager, Corporate Information Security Office

The manager, Corporate Information Security Office (CISO), Information Technology (IT) is responsible for reviewing the processes and procedures developed by Engineering to implement Postal Service information security policies.

3 Supplemental Information Security Requirements

3-1 About This Chapter

This chapter presents the information security requirements that supplement Handbook AS-805, *Information Security,* and that may be implemented within the MPE/MHE environment to support the secure processing and handling of mail. These supplemental requirements, which are discussed in sections 3-2 through 3-10, authorize Engineering to implement mitigating controls under specific circumstances to prevent compromises to either the MPE/MHE backbone or the Postal Service infrastructure and to ensure that both are protected.

3-2 User Identification and Authorization

3-2.1 Logon IDs

Network Operations Management may assign logon identifiers (IDs) used within the MPE/MHE environment to multiple users under the following conditions:

a. The logon ID provides only local access to an information resource (device).

b. Accounts are restricted to specific information resources (devices).

c. Accounts do not allow for any access outside the MPE/MHE environment, including other Postal Service information resources.

d. Any remote connectivity must comply with Postal standards.

(See Handbook AS-805, Section 9-6, Identification.)

3-2.2 Passwords

Where the MPE/MHE devices cannot accommodate the password criteria defined in Handbook AS-805, Engineering can define the password criteria for that device. Criteria include the selection characteristics, storage requirements, and transmission requirements. The manager, CISO, and the vice president, Engineering, together review and approve the special password criteria.

Network Operations Management may assign passwords for the logon IDs used within the MPE/MHE environment under the following conditions:

a. The operating manager or supervisor of the information resource (device) is responsible for the management and usage of passwords.

b. Passwords for privileged and maintenance accounts (e.g., system supervisors, software specialists, system administrators, or vendors) are held at a higher level of control, and account management is documented to ensure information resource integrity, availability, and confidentiality.

(See Handbook AS-805, Section 9-7, Authentication.)

3-3 Hardware and Software

3-3.1 Establishing Hardware/Software Criteria

Engineering will establish the criteria for the identification, selection, and use of hardware and software in the MPE/MHE environment. The criteria will apply to application, database, and operating system software.

3-3.2 Hardening Servers

Servers directly connecting the MPE/MHE private network to the Postal Service Managed Network Services (MNS) must be hardened to the standards approved by the manager, CISO.

3-3.3 Using Only Approved Products

MPE/MHE information resources must use only hardware and software products that have been approved by Engineering to ensure a standard Postal Service security architecture, facilitate continuity of operations and audit capability, enable regular updates to address emerging security requirements, and protect the overall integrity of Postal Service information resources. (See Handbook AS-805, Section 5-5.3, Using Approved Software, and Section 10-3.2, Using Approved Hardware and Software.)

3-4 Software

3-4.1 Commercial Off-the-shelf Software

Commercial off-the-shelf (COTS) software used in the MPE/MHE environment that is not on the ITK must be acquired and distributed from a source approved by Engineering. Computer software purchased for the Postal Service must be registered to the Postal Service (see Handbook AS-805, Section 10-6.7, COTS Software).

3-4.2 Third-Party Software

Ownership of third-party software must be clearly stated in contracts for the MPE/MHE. There is a potential risk in using software that is not the property of the Postal Service (see Handbook AS-805, Section 10-6.11, Third-Party Software).

3-5 Hardware

3-5.1 Protection

MPE/MHE servers and equipment must be protected commensurate with the level of sensitivity and criticality of the information and business function.

3-5.2 Installation and Deployment

Server and equipment installation and deployment must comply with configuration and deployment guidelines applicable for the server platform. Engineering will set the configuration standards for the devices that are unique to the MPE environment (see Handbook AS-805, Section 10-5.3, Servers). Services on general types of servers deployed throughout the Postal Service should be hardened to Postal Service standards.

3-6 Research and Development (R&D)

3-6.1 Separation of Test and Production Environments

If the size or complexity of an information resource (e.g., tray management system) does not permit exclusive testing in a test environment because of cost and feasibility constraints, due diligence must be performed to ensure that other information resources within the Postal Service computing environment are not negatively affected.

3-6.2 Pilots and Proofs of Concept

3-6.2.1 Information Security Assurance (ISA)

MPE/MHE pilot projects or proofs of concept must undergo Information Security Assurance (ISA) to be certified and accredited before full production to ensure that the project does not inadvertently expose the Postal Service to unnecessary security threats (see Handbook AS-805, Section 8-5.2, When ISA Is Required).

3-6.2.2 Change Management

Documented change management practices, as defined by Engineering, must be implemented to allow for practical cost containment during research and development exercises. Due diligence must be implemented to ensure the integrity of MPE/MHE information resources as defined by Engineering (see Handbook AS-805, Section 8-3.4, Change Control, Version Control, and Configuration Management).

3-7 Engineering Processes — Integrity Standards

Integrity thresholds for MPE/MHE information resources must ensure that the resources perform their intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Engineering is responsible for identifying the applicable integrity standards for MPE/MHE information resources (see Handbook AS-805, Section 9-9, Integrity.)

3-8 Information Security Assurance

3-8.1 Initiating ISA

The information security assurance (ISA) process will be conducted under the requirements for information resources set forth in Handbook AS-805.

3-8.2 Reinitiating ISA

The MPE/MHE environment is considered to be a stable environment consisting primarily, but not exclusively, of mail processing and mail handling equipment with long-term life cycles because of the high investment in the information resources (devices). Reinitiating ISA for recertification and reaccreditation for specialized MPE/MHE information resources (devices) will be required whenever one of the following events takes place:

a. Significant information security incident that violates an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an information resource.

b. Significant security audit findings.

c. Significant change in the operating environment, equipment operations, or the use and collection of data. Significant changes may include, but are not limited to, the following:

    (1) Change from one major application to another, such as BroadVision to WebObjects.

    (2) Change from one database application to another, such as Oracle to MS-SQL.

    (3) Change in the hosting location, such as from a Postal Service facility to an outsourced, non-Postal Service location (see Handbook AS-805, Chapter 8, Systems, Applications, and Product Development).

d. Change in network connectivity requirements.

3-9 Secure Enclaves

3-9.1 Description

Secure enclaves are network areas where special protections and access controls, such as firewalls and routers, are used to secure information resources. Secure enclaves apply security rules consistently and protect multiple systems across application boundaries.

3-9.2 Implementation

Secure enclaves must be provided for MPE/MHE information resources that are routed to or through the managed network services to support the secure processing and handling of mail and to ensure protection of the MPE/MHE processing environment and the Postal Service computing environment. Some or all of the following general secure enclave requirements may be implemented to protect both infrastructures:

a. Employ protection for the highest level of information designation in that enclave.

b. Place on network segments (subnets) separate from the remainder of Postal Service networks.

c. Use “network guardians,” such as packet filtering or application proxy firewalls, to mediate and control traffic.

d. Set enclave server rules and operational characteristics that can be enforced and audited.

e. Allow only predefined, securable information traffic flows**.**

f. Restrict administration to a small, well-defined set of system administrators.

g. Deploy intrusion detection systems based on information resource designation and technical feasibility.

h. Audit the network boundary controls through network scanning procedures on a regular basis (see Handbook AS-805, Chapter 11, Network Connections).

3-9.3 Determining When a Secure Enclave is Required

Engineering must submit an architectural diagram defining the connectivity between the MPE/MHE infrastructure and the Postal Service MNS backbone to the Network Connectivity Review Board (NCRB), who will review the request and determine appropriate enclave requirements to protect both operating environments.

3-10 Audit Log Requirements

Engineering is responsible for defining the criteria for audit logging for the MPE/MHE environment. At a minimum, each information resource (device) must be capable of generating an auditable log of events whenever one or more of following conditions apply:

a. Accountability is a requirement for an information resource.

b. The MPE/MHE information resource (device) may affect other information resources (devices) requiring accountability.

c. The MPE/MHE information resource (device) is connected to the Postal Service infrastructure (see Handbook AS-805, Section 9-12, Audit Logging).

Glossary

Access The ability or permission to enter or pass through an area or to view, change, or communicate with an information resource.

Access Controls A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and prevent unauthorized access to information resources.

Accountability The association of each logon ID with one and only one user, so that the user can always be tracked while using an information resource, providing the ability to know which user performed what system activities.

Accreditation The management approval component of the security certification and accreditation process that constitutes formal acceptance of responsibility for operating the information resource at an acceptable level of risk.

Alternate Site A location used to conduct critical business functions in the event that access to the primary facility is denied or damaged so as to be unusable.

Application A computer program or set of programs that performs one of the important tasks or business function for which the information resource is used.

Audit An independent review and examination of records and activities in order to test for adequacy of controls, ensure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Audit Logging The process of recording operational and security-related events.

Authentication The process of verifying the identity of a station, originator, or individual to determine the right to access specific categories of information. Also, a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator. During the process, the user enters a name or account number (identification) and password (authentication).

Authorization The granting to a user, program, or process the right of access. The privileges granted to an individual by a designated official to access information based upon the individual's job, clearance, and need to know.

Availability The computer security characteristic that ensures that computer resources will be available to authorized users when they need them. This characteristic addresses backups, alternate sites, disaster recovery, and denial of service.

Certification The technical analysis that establishes the extent to which the information resource meets a specified set of security requirements.

Compensating Control A cost-effective security measure implemented to protect an information resource and minimize the risk associated with the relative threats, vulnerabilities, and value of the resource. Compensating controls are alternative controls to those generally established to protect an information resource that are used because of budget, time or environmental constraints for the information resource.

Confidentiality The computer security characteristic that ensures individuals are given access to computer resources based on security clearance and need to know. This characteristic addresses the compromise and inadvertent disclosure of sensitive information.

Control Security Control; Safeguard; Mechanism; Any protective action, device, procedure, technique, or other measure that reduces the exposure of the information resource to misuse, harm, or loss.

Firewall Gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other less trusted.

Identification The process of associating a user with a unique user identifier (ID) or logon ID.

Information Resource All Postal Service information assets, including information systems, hardware, software, data, applications, telecommunications networks, computer-controlled mail processing equipment, and related resources and the information they contain.

Information Security The protection of all forms of information against unauthorized access to, modification of, or destruction, whether in storage, processing, or transit, and against the denial of service to authorized users.

Integrity The computer security characteristic that ensures that computer resources operate correctly and ensures the consistency of data structures and the accuracy of the stored information, i.e., that the data has not been inappropriately altered. This characteristic addresses the deliberate or inadvertent unauthorized manipulation of the information resource, and how to maintain the security of the information resource under all conditions.

Log File A file that lists actions that have occurred.

Logon ID An identification code (normally a group of numbers, letters and symbols) assigned to a particular user that, in conjunction with a password, identifies the user to the information resource.

Mitigating Security Control A cost-effective security measure implemented to protect an information resource and minimize the risk associated with the relative threats, vulnerabilities, and value of the resource. Mitigating controls are supplementary controls to those originally established to protect an information resource that are required because an acceptable level of risk was not been achieved. (See Security Control for examples of controls.)

Network Perimeter A clearly defined boundary established to control the traffic between external untrusted sources and the internal trusted network.

Password A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Personnel All Postal Service employees, contractors, and subcontractors, both permanent and temporary.

Pilot Project Also known as proof-of-concept project — the initial implementation of a previously untested idea or system that is intended to lend credibility to the project.

Risk The possibility of loss or injury, based on the likelihood that an event will occur and the amount of harm that could result.

Secure Enclave Intranet area that provides increased security, additional perimeter protection, and access controls for valued information resources.

Security Architecture The appearance, products, functions, locations, and resources used in the security infrastructure. A security architecture is designed with the appropriate level of administrative and technical security controls.

Security Controls The protection mechanisms and controls that are prescribed to meet the security requirements specified for an information resource. The controls may include, but are not necessarily limited to: hardware and software security features, operating procedures, authorization and accountability procedures, access and distribution controls, management constraints, personnel security, environmental controls, and physical control areas, structures, and devices. Also called security safeguards and countermeasures. To be effective, security controls will be implemented according to established security specifications.

Security Requirements The types and levels of protection necessary to adequately secure the information resource.

Security Specifications A detailed description of the safeguards required to meet the security requirements and to adequately protect an information resource from unauthorized (accidental or intentional) disclosure, modification, and destruction of information, or denial of service.

Threat A force or condition (human, physical, or environmental) that could potentially cause harm or loss by exploiting vulnerabilities.

Untrusted Characterized by absence of trusted status; assumed to be unreliable, untruthful, and inaccurate, unless proven otherwise.

User An entity attempting access to the information resource. That entity may be an individual, a computer, or another application.

Vulnerability A condition or weakness in security procedures, technical controls, or operational processes which exposes the system to loss or harm.

Workstation A terminal, computer, or other discrete resource that allows personnel to access and use information resources.