

DRAFT

Postal Service

Postage Evidencing Product Submission Procedures

AGENCY: Postal Service.

ACTION: Notice of proposed procedure; response to comments; extension of time for comments.

SUMMARY: "Postage Evidencing Product Submission Procedures," as published in the **Federal Register** on August 17, 1999, was a notification of proposed product submission procedures for all postage evidencing products, including those in the Information Based Indicia Program (IBIP). In response to the solicitation of public comments, two submissions were received. These comments were considered in making the changes incorporated in this revised version, as noted in the discussion of comments, below. In addition to these changes, this version includes new policy on the relationship between the Postal Service and the Provider regarding intellectual property issues.

The USPS, in a cooperative effort with product providers and other interested parties, is allowing 30 days for submission of any additional comments to ensure all issues are considered prior to publication of the final rule.

DATES: Comments must be received on or before 30 days from the date of this notice.

ADDRESSES: Written comments should be mailed or delivered to the Manager, Postage Technology Management, Room 8430, 475 L'Enfant Plaza SW, Washington DC 20260-2444. Copies of all written comments will be available at the above address for inspection and photocopying between 9 a.m. and 4 p.m., Monday through Friday.

FOR FURTHER INFORMATION CONTACT: Nicholas S. Stankosky, (202) 268-5311.

SUPPLEMENTARY INFORMATION: With the expansion of postage application methods and technologies, it is essential that product submission procedures for all postage evidencing products be clearly stated and defined. The Postal Service evaluation process can be effective and efficient if these procedures are followed explicitly by all suppliers. In this way, secure and convenient technology will be made available to the mailing public with minimal delay and with the complete assurance that all Postal Service technical, quality, and security requirements have been met. These procedures apply to all proposed postage evidencing products and systems, whether the Provider is new or is currently authorized by the Postal Service.

Title 39, Code of Federal Regulations (CFR) Section 501.9, Security Testing, states, "the Postal Service reserves the right to require or conduct additional examination and testing at any time, without cause, of any meter submitted to the Postal Service for approval or approved by the Postal Service for manufacture and distribution." For products meeting the performance criteria for postage evidencing under the Information Based Indicia Program (IBIP), including PC Postage products, the equivalent section is 39 CFR Section 502.10, Security Testing, published as a proposed rule in the **Federal Register**, September 2, 1998. When the Postal Service elects to retest a previously approved product, the Provider will be required to resubmit the product for evaluation according to part or all of the proposed procedures. Full or partial compliance with the procedures will be determined by the Postal Service prior to resubmission by the Provider.

The proposed submission procedures will be referenced in 39 CFR Parts 501 and 502 but will be published as a separate document titled "Postage Technology Management, Postage Evidencing Product Submission Procedures."

Discussion of Comments

A. *Scope of Review*

1. One commenter expressed concern that the scope of Postal Service review of any postage evidencing device should be limited to the boundaries of the logical security device and to the infrastructures and interfaces through which the Postal Service verifies that payment for postage has been received.

DRAFT

The Postal Service does not accept the commenter's view that the review of any postage evidencing device should be limited to the boundaries of the logical security device and to the infrastructures and interfaces through which the Postal Service verifies that payment for postage has been received. The Postal Service is concerned with other potentially security-related aspects of postage evidencing systems beyond those associated with the logical security device and postage payment, such as communications and other administrative functions. The Postal Service must also verify that all aspects of the postage evidencing system submitted for evaluation work together as specified. No revision of the procedures was made as a result of this comment.

2. One commenter had a concern with providing any copies of product software to the Postal Service, as well as with the number of copies required and the stated intent of the Postal Service to keep copies of the software.

The Postal Service agrees in part with the commenter. The requirement was changed so that the Postal Service will require only one copy of the software code, as opposed to the five copies previously requested.

However, the Postal Service does not agree with the commenter that software should be provided only to the NIST laboratory, and not to the Postal Service. A copy of the source code is required by the Postal Service because the Postal Service tests many other aspects of the product beyond the security and other features tested by the NIST laboratories. Should the Postal Service have any question about the completeness of a NIST laboratory report, it may require the source code for comparison purposes. Also, for audit and control purposes there is a need for the Postal Service to have on file a full copy of the source code of the most current version of the software for all approved products. This requirement remains unchanged.

3. One commenter had a concern about the procedures to be applied to product modifications and suggested these rules should exempt from the approval process any modifications to an approved product when the modification does not affect the boundaries of the security device or its operation.

The Postal Service does not accept the commenter's view that only certain changes to an approved product should be submitted for evaluation. The Postal Service wants to see all changes to an approved product in order to verify that the proposed modification does not affect the boundaries of the security device or its operation, or otherwise affect security. Each proposed change is evaluated to determine the level of testing required to assess the impact of the change under consideration. No revision of the procedures was made as a result of this comment.

4. One commenter was concerned that the procedures seem to allow the Postal Service to change a test plan that has been submitted by the Provider and approved by the Postal Service during the test process, for any reason or for no reason at all. The commenter also stated that re-testing should occur if, but only if, there is a known and proven defect within the security boundaries or a known, proven, and commercially viable technology has been developed that would permit breach of the security device under examination.

The Postal Service does not accept the commenter's views on limiting possible changes to an approved test plan. Postal Service findings during the test and evaluation process can result in the need for additional testing, product retesting, or even resubmission of the product.

Similarly, the Postal Service does not accept the commenter's views on putting limitations on the Postal Service's retesting of an approved product. In accordance with current regulations for metering products (CFR Section 501.9, Security Testing), and proposed regulations for IBI products (502.10, Security Testing, as published in the Federal Register September 2, 1998), the Postal Service can require retesting at any time. The text of the regulations states that the Postal Service reserves the right to require or conduct additional examination and testing at any time, without cause, of any meter/IBI system submitted to the Postal Service for approval or previously approved by the Postal Service for manufacture and distribution. No revision of the procedures or the regulations was made as a result of this comment.

B. Communication and Postal Service Response

DRAFT

1. One commenter requested that the Postal Service establish target dates for its responses at each stage of the product submission and approval process and to commit to responding to Providers' submissions within a reasonable and prompt time frame, with standardized time frames and methodologies for communication.

The Postal Service understands the commenter's concern and does in fact strive to complete each stage of the product review, test, and evaluation process in a timely manner. However, it is difficult if not impossible for the Postal Service to commit to a set timetable for response, given resource constraints, the unpredictability of product submissions, and the dependence on outside agents. The product providers can help the Postal Service to respond in a timely manner by ensuring that product submissions are complete and meet all requirements specified in the product submission procedures. No revision of the procedures was made as a result of this comment.

2. One commenter asked that a formal communication process be established between the provider and third party laboratories or consultants retained by the Postal Service in order to discuss significant findings impacting the security assessment of the product submission and communicate significant findings in a timely manner.

The Postal Service does not agree with this request. In order to evaluate postage evidencing products, the Postal Service secures the services of various third parties. These third parties are Postal Service resources paid by the Postal Service to complete tasking at Postal Service direction and to provide reports directly to the Postal Service only. We do not wish to have the efforts of these third parties and the costs of their services diverted by the need to communicate with anyone outside the Postal Service. Any communication between the provider and these third party resources shall be accomplished through discussions with the Manager, Postage Technology Management. No revision of the procedures was made as a result of this comment.

3. One commenter asked that the Postal Service communicate interim test results and bring to the immediate attention of the provider any circumstance where there is the potential for test failure.

The Postal Service does not agree with this request. Before submission of a product for Postal Service test and evaluation, the provider should ensure that the product meets all performance criteria and specifications. A product that is not ready for testing and has functional problems delays the Postal Service evaluation of the product. The Postal Service does not have the resources to act as a test laboratory for the provider, nor is it an appropriate role for the Postal Service. The Submission Procedures were amended to allow for the Postal Service to charge the Provider for the costs associated with additional testing by the Postal Service that is required as the result of an incomplete or inadequate initial product submission.

C. Requirements for FIPS 140 Certification

1. One commenter asked for clarification of the Postal Service policy and position on recognition of FIPS 140 certification for both the Postal Security Device (PSD) and the actual application running on the PSD.

The Postal Service requires only that the PSD itself receive the NIST FIPS 140 certification. The FIPS certification of the PSD is independent of the application. Additional (non-FIPS) functions required of the PSD are specified in the USPS Benchmark Test requirements. These functions will be tested in addition to FIPS-140 functions by a NIST-certified laboratory. The Postal Service has revised the product submission procedures in response to this comment.

D. Requirements for Use of AMS CD-ROM

1. One commenter questioned the requirement to use and integrate the USPS Address Matching System (AMS) CD-ROM with some IBI systems, claiming that this program does not support all the functionality required, such as coding of addresses to the delivery point and validation of exact input addresses.

DRAFT

The Postage Evidencing Product Submission Procedures that are the subject of this Federal Register notice require the provider to meet Postal Service performance criteria for specific postage evidencing products, as applicable. Any comments on the details of the performance criteria for individual products should be addressed separately to the Manager, Postage Technology Management.

1. Product Submission Procedures

In submitting any postage-evidencing product for Postal Service evaluation, the proposed Provider must provide detailed documentation and comply with requirements in the following areas:

- (1) Letter of Intent.
- (2) Nondisclosure Agreements.
- (3) Concept of Operations (CONOPS).
- (4) Software and Documentation Requirements.
- (5) Provider Infrastructure Plan.
- (6) USPS Address Matching System (AMS) CD-ROM Integration.
- (7) Product Submission/Testing.
- (8) Provider Infrastructure Testing.
- (9) Field Test (Beta) Approval (Limited Distribution).
- (10) Provider/Product Approval (Full Distribution).

The Provider shall indicate the specific requirement(s) addressed by each document submitted in compliance with these Postage Evidencing Product Submission Procedures. The Postal Service requests that the documentation include a matrix showing where each specific requirement is addressed. Documentation shall be in English and formatted for standard letter size (8.5" x 11") paper, except for engineering drawings, which shall be folded to the required size. Where appropriate, documentation shall be marked as "Confidential." The steps in the Postage Evidencing Product Submission Procedures must be completed in sequential order, except as detailed below.

1.1. Letter of Intent

The Provider must submit a Letter of Intent to the Manager, Postage Technology Management, United States Postal Service, 475 L'Enfant Plaza SW, Room 8430, Washington DC 20260-2444.

A. The Letter of Intent must include:

- (1) Date of correspondence.
- (2) Name and address of all parties involved in the proposal. In addition to the Provider, the parties listed shall include those responsible for assembly, distribution, management of the product/device, hardware/firmware/software development, testing, and other organizations involved (or expected to be involved) with the product, including suppliers of significant product components. In these procedures, the term "product" is used when referring generically to processes, etc. However, the term "product" includes "product/device."
- (3) Name and phone number of official point of contact for each company identified.
- (4) Provider's business qualifications (i.e., proof of financial viability, certifications and representations, proof of ability to be responsive and responsible).
- (5) Product/device concept narrative.
- (6) Provider infrastructure concept narrative.
- (7) Narrative that identifies the internal resources knowledgeable of current Postal Service policies, procedures, performance criteria, and technical specifications to be used to develop security, audit, and control features of the proposed product.

DRAFT

(8) The target Postal Service market segment the proposed product is envisioned to serve.

B. The Provider must submit with the Letter of Intent a proposed product development plan of actions and milestones (POA&M) with a start date coinciding with the date of the Letter of Intent. Reasonable progress must be shown against these stated milestones.

C. The Manager, Postage Technology Management, will acknowledge in writing the receipt of the Provider's Letter of Intent and will designate a Postal Service point-of-contact. Upon receipt of this acknowledgment, the Provider may continue with the sequential requirements of the product submission process.

1.2. Nondisclosure Agreements

These agreements are intended to ensure confidentiality and fairness in business. The Postal Service is not obligated to provide product submission status to any parties not identified in the Letter of Intent. After obtaining signed nondisclosure agreements, the Provider may continue with the sequential requirements of the product submission process.

1.3. Concept of Operations

A. The Provider must submit a Concept of Operations (CONOPS) that discusses at a moderate level of detail the features and usage conditions for the proposed product. The Provider should submit 10 serialized printed copies and one electronic copy on a PC-formatted 3.5" floppy disk. Additionally, the Provider must also submit a detailed process model supporting each CONOPS section.

B. At a minimum, the CONOPS should cover the following areas:

(1) System Overview.

(a) Concept overview/business model.

(b) Concept of production/maintenance administration.

(c) For Information-Based Indicia (IBI) systems, including PC Postage products, the system design overview, including:

(i) Postal Security Device (PSD) implementation (stand-alone, LAN, WAN, hybrid).

(ii) Features.

(iii) Components, including the digital signature algorithm.

(d) Product life cycle overview.

(e) Adherence to industry standards, such as Federal Information Processing Standard (FIPS) 140-1, as required by the Postal Service.

(2) System Design Details (for proposed IBI systems, including PC Postage products).

(a) PSD features and functions.

(b) Host system features and functions.

(c) Other components required for system use including, but not limited to, the proposed indicia design and label stock.

(3) Product Life Cycle.

(a) Manufacturer.

(b) Postal Service certification of product/device.

(c) Production.

(d) Distribution.

(e) Product/device licensing and registration.

(f) Initialization.

DRAFT

- (g) Product authorization and installation.
 - (h) Postage Value Download (PVD) process.
 - (i) Product and support system audits.
 - (j) Inspections.
 - (k) Product withdrawal/replacement.
 - (i) Overall process.
 - (ii) Product failure/malfunction procedures.
 - (l) Scrapped product process.
- (4) Finance Overview.
- (a) Customer account management.
 - (i) Payment methods.
 - (ii) Statement of account.
 - (iii) Refund.
 - (b) Individual product finance account management.
 - (i) Postage Value Download (PVD).
 - (ii) Refund.
 - (c) Daily account reconciliation.
 - (i) Provider reconciliation.
 - (ii) Postal Service detailed transaction reporting.
 - (d) Periodic summaries.
 - (i) Monthly reconciliation.
 - (ii) Other reporting, as required by the Postal Service.
- (5) Interfaces.
- (a) Communications and message interfaces with Postal Service infrastructure, including but not limited to:
 - (i) PVDs.
 - (ii) Refunds.
 - (iii) Inspections.
 - (iv) Product audits.
 - (v) Lost or stolen product procedures.
 - (b) Communications and message interfaces with applicable Postal Service financial functions, including but not limited to:
 - (i) Postage settings, including those done remotely.
 - (ii) Daily account reconciliation.
 - (iii) Refunds.
 - (c) Communication and message interfaces with Customer Infrastructure, including but not limited to:
 - (i) Cryptographic key management.

DRAFT

- (ii) Product audits (device and host system).
 - (iii) Inspections.
 - (d) Message error detection and handling.
- (6) Technical Support and Customer Service.
 - (a) User training and support.
 - (b) Software Configuration Management (CM) and update procedures.
 - (c) Hardware/firmware CM and update procedures.
- (7) Other.
 - (a) Change control procedures.
 - (b) Postal rate change procedures.
 - (c) Address Management System ZIP+4 CD-ROM updates, if applicable.
 - (d) Physical security.
 - (e) Personnel/site security.
- C. Supplementary requirements, CONOPS:
 - (1) The CONOPS must be accompanied by substantiated market analysis supporting the target Postal Service market segment that the proposed product is envisioned to serve, as identified in the Letter of Intent.
 - (2) The CONOPS must include a list and a detailed explanation of any proposed deviations from Postal Service performance criteria or specifications. Any proposed deviation to audit and control functions required by current Postal Service policy, procedure, performance criteria, or specification must be accompanied by an independent assessment by a nationally recognized, independent, certified public accounting firm attesting to the proposed auditing method. The report of this information is to be signed by an officer of the accounting firm.
- D. Postal Service response:
 - (1) The Postal Service will respond in a timely manner.
 - (2) For each submission, the Postal Service will appoint a Product Review Control Officer. All communications between the Provider and the Postal Service are to be coordinated through the Product Review Control Officer.
 - (3) The Postal Service will acknowledge, in writing, receipt of the CONOPS and perform an initial review. The Postal Service will provide the Provider with a written summary of the CONOPS review. In the written review, the Postal Service will provide authorization to continue with the product submission process, or a listing of CONOPS requirements that are not met.
 - (4) If, in the sole opinion of the Postal Service, it is determined that significant CONOPS deficiencies do exist, the Postal Service, at the discretion of the Manager, Postage Technology Management, may return the CONOPS to the Provider without further review. It will then be incumbent on the Provider to resubmit a corrected CONOPS.
 - (5) The Provider may continue with the product submission process upon receipt of authorization from the Postal Service to proceed.

1.4. Software and Documentation Requirements

- A. The Provider must submit to the Postal Service one copy of executable code and one copy of source code for all software included in the product.

DRAFT

B. The Provider must submit a detailed design document of the product. For IBI products, this shall include the proposed IBIP indicia design, which must be approved by the Manager, Postage Technology Management.

C. Additionally, depending on the product, the Postal Service requires design documentation that includes, but is not limited to, the following:

- (1) Operations manuals for product usage.
- (2) Interface description documents for all proposed communications interfaces.
- (3) Maintenance manuals.
- (4) Schematics.
- (5) Product initialization procedures.
- (6) Finite state machine models/diagrams.
- (7) Block diagrams.
- (8) Security features descriptions.
- (9) Cryptographic operations descriptions.

Detailed references for much of this documentation are listed in FIPS 140-1, Appendix A. The Postal Service will determine the number of copies needed of the aforementioned documentation based on the CONOPS review. The Postal Service will notify the Provider of the required number of copies. The required number of copies are to be uniquely numbered for control purposes.

D. The Provider must submit a comprehensive test plan that will validate that the product meets all Postal Service requirements and, where appropriate, the requirements of FIPS 140-1. With respect to the Provider's Internet server, the test plan shall indicate how the Provider will test to ensure the physical security of the Provider's server and administrative site and the firewall, and to ensure the security of the processes for remote administrative access and configuration control. With respect to the process for initializing customer accounts, the test plan shall describe the tests for ensuring secure distribution or transmission of software and cryptographic keys. The test plan must list the parameters to be tested, test equipment, procedures, test sample sizes, and test data formats. Also, the plan must include detailed descriptions, specifications, design drawings, schematic diagrams, and explanations of the purposes for all special test equipment and nonstandard or noncommercial instrumentation. Finally, this test plan must include a proposed schedule of major test milestones.

E. The Provider must submit a benchmark assessment plan. The Manager, Postage Technology Management will provide reference standards, performance criteria, specifications, and so forth to be used as a basis for the Provider to produce this plan.

F. Postal Service response:

- (1) The Postal Service will provide its response in a timely manner.
- (2) The Postal Service will acknowledge, in writing, receipt of the Provider's design and test plans and will perform an initial review. The Postal Service will furnish the Provider with a written summary of the design plan and test plan reviews. In the written review, the Postal Service will provide authorization to continue with the product submission process, or will provide a listing of design plan requirements or test plan requirements that are not met, and perhaps other deficiencies.
- (3) If, in the sole opinion of the Postal Service, it is determined that significant design plan or test plan deficiencies do exist, the Postal Service, at the discretion of the Manager, Postage Technology Management, may return the plans to the Provider without further review. It will then be incumbent on the Provider to resubmit revised plans that address the identified deficiencies.
- (4) The Provider may continue with the product submission process upon receipt of authorization from the Postal Service to proceed.

DRAFT

1.5. Provider Infrastructure Plan

A. The Provider Infrastructure Plan may be submitted concurrently with the design and test plans described in 1.5, Software and Documentation Requirements. At this point in the product submission process, the Postal Service will provide additional performance criteria and specifications for the IBIP public key infrastructure, if required for the product/device, for use as a basis for the applicable elements of the Provider's Infrastructure Plan.

B. The Provider must submit a Provider Infrastructure Plan that describes how the processes and procedures described in the CONOPS will be met or enforced. This includes, but is not limited to, a detailed description of all Provider-related and Postal Service-related operations, computer systems, and interfaces with both customers and the Postal Service that the Provider shall use in manufacturing, producing, distribution, customer support, product/device life cycle, inventory control, print readability quality assurance, and reporting.

C. Postal Service response:

(1) The Postal Service will respond in a timely manner.

(2) The Postal Service will acknowledge in writing the receipt of the Provider's Infrastructure Plan and will perform an initial review. The Postal Service will provide the Provider with a written summary of the Infrastructure Plan review. In the written review, the Postal Service will provide authorization to continue with the product submission process, or a listing of the Infrastructure Plan requirements that are not met, and perhaps other deficiencies.

(3) If, in the sole opinion of the Postal Service, it is determined that significant Provider Infrastructure Plan deficiencies do exist, the Postal Service, at the discretion of the Manager, Postage Technology Management, may return the Infrastructure Plan to the Provider without further review. It will then be incumbent on the Provider to resubmit a revised Infrastructure Plan to address the identified deficiencies.

(4) The Provider may continue with the product submission process upon receipt of authorization from the Postal Service to proceed.

1.6. USPS Address Matching System (AMS) CD-ROM Integration

A. The USPS AMS CD-ROM is a required component of IBIP open systems. For such systems, the Provider shall initiate and fully comply with a license agreement with the USPS National Customer Support Center (NCSC). This signed agreement shall describe responsibilities of the AMS CD-ROM supply chain process, including roles of the Provider. The only functionality of the AMS CD-ROM available through an IBIP system shall be address matching and ZIP+4 coding of input addresses.

B. The Provider shall submit a detailed description of how the USPS AMS CD-ROM will be integrated in the product, including a description of the process by which an address is ZIP+4 coded, including all possible optional and required parameters. The Provider can submit this information concurrent with submission of the Software and Documentation Requirements and/or Provider Infrastructure Plan described above.

C. Any CONOPS or products proposed for which the Provider requests a variance to the AMS CD-ROM requirements must be approved by the Manager, Postage Technology Management prior to proceeding with the next step in the submission process.

1.7. Product Submission/Testing

A. The product/device Provider must be prepared to submit up to five complete production systems of each product/device for which Postal Service evaluation is requested. The required number of submitted systems will be determined by the Postal Service. The Provider must provide any equipment and consumables required to use the submitted product/device in the manner contemplated by the CONOPS.

Thorough Provider testing prior to submission of the product to the Postal Service will avoid unnecessary delays in the review and evaluation process. If, in the opinion of the Postal Service, it is

DRAFT

determined that significant product deficiencies exist, the Postal Service, at the discretion of the Manager, Postage Technology Management, may return the product to the Provider without further review. The Provider may resubmit a corrected product.

The Postal Service reserves the right to charge the Provider for the costs associated with any additional testing by the Postal Service that is required as the result of an incomplete or inadequate initial product submission.

B. If the product contains a cryptographic module, the Provider must submit the cryptographic module to a laboratory accredited under the National Voluntary Laboratory Accreditation Program (NVLAP) for FIPS 140-1 certification, or equivalent, as authorized by the Postal Service. The Postal Service requires only that the PSD itself receive the NIST FIPS 140-1 certification. The FIPS certification of the PSD is independent of the application.

Upon completion of the FIPS 140-1 certification, or equivalent, the Postal Service requires the following to be forwarded directly from the accredited laboratory to the Manager, Postage Technology Management for review:

- (1) A copy of all information given to the laboratory by the Provider, including a summary of all information transmitted orally.
- (2) A copy of all instructions from the Provider with respect to what is or is not to be tested for.
- (3) A copy of the letter of recommendation for the product as submitted by the laboratory to the National Institute of Standards and Technology (NIST) of the United States of America.
- (4) Copies of all proprietary and nonproprietary reports and recommendations generated during the test process.
- (5) A copy of the certificate, if any, issued by NIST for the product.
- (6) Written full disclosure identifying any contribution of the NVLAP laboratory to the design, development, or ongoing maintenance of the cryptographic module or the product/device.

C. For products with a cryptographic module, non-FIPS functions required of the module are specified in the USPS Benchmark Test requirements. A NIST-certified laboratory will test these functions in addition to testing the FIPS 140-1 functions.

D. If the cryptographic module is submitted to an accredited test laboratory to meet the requirements of paragraph B or C of this section, the laboratory must meet all the requirements specified by NIST in the Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program; NIST document 150-17, Cryptographic Module Testing; and other documents issued by NIST to govern the conduct of accredited laboratories.

E. All cryptographic modules submitted to an accredited laboratory for testing under paragraph B or C of this section shall be retained by the laboratory for 3 years from date of product approval by the Postal Service.

F. The Provider may submit the product to the Postal Service for test and evaluation prior to completion of any required FIPS 140-1 testing, provided a letter is submitted from the NVLAP laboratory to the Postal Service indicating that:

- (1) The cryptographic module included in the product is being tested under FIPS 140-1 for the required security levels, in accordance with the current, relevant performance criteria.
- (2) The cryptographic module has a reasonable chance of meeting the FIPS 140-1/USPS security levels.
- (3) The timeline for FIPS 140-1 test completion.

G. The Postal Service reserves the right to require or conduct additional examination and testing at any time, without cause, of any product submitted to the Postal Service for approval or approved by the Postal Service for manufacture and distribution.

DRAFT

H. Upon satisfactory completion of the Postal Service testing and NVLAP laboratory testing (where required), the Postal Service will provide authorization to continue the product submission process. The Provider may continue with the product submission process upon receipt of authorization from the Postal Service to proceed.

I. The provider shall obtain, maintain, and comply with the certification requirements as established by the USPS in the Coding Accuracy Support System (CASS) program. The provider shall obtain, maintain, and comply with CASS certification requirements prior to product offering.

1.8. Product Infrastructure Testing

A. Prior to approval for distribution of any product/device, the Provider must achieve test and approval of all reporting requirements, including, but not limited to, Postal Service/customer licensing support, product status activity reporting, total product population inventory, irregularity reporting, lost and stolen reporting, financial transaction reporting, account reconciliation, digital certificate acquisition, product initialization, cryptographic key changes, rate table changes, print quality assurance, device authorization, device audit, product audit, and remote inspections.

B. Testing of these activities and functions includes computer-based testing of all interfaces with the Postal Service, including but not limited to the following:

- (1) Product manufacture and life cycle (including leased, unleased, new product/device stock, installation, withdrawal, replacement, key management, lost, stolen, and irregularity reporting).
- (2) Product distribution and initialization (including product authorization, product initialization, customer authorization, and product maintenance).
- (3) Licensing (including license application, license update, and license revocation).
- (4) Finance (including cash management, individual product financial accounting, refund management, daily summary reports, daily transaction reporting, and monthly summary reports).
- (5) Audits and inspections, including site audits.

C. The Provider must complete a “Product—Provider Infrastructure—Financial Institution—USPS Infrastructure” (Alpha) test involving all entities in the proposed architecture. At a minimum this includes the proposed product, Provider Infrastructure, financial institution, and Postal Service Infrastructure systems and interfaces. Alpha testing is intended to demonstrate the proposed product utility, and its functionality and compatibility with other systems. Alpha testing may be conducted in a laboratory environment.

D. Provider Infrastructure Testing (Alpha) test note: The Postal Service reserves the right to require or conduct additional examination and testing at any time, without cause, of any Provider Infrastructure system supporting a postage evidencing product/device approved by the Postal Service for manufacture and distribution. Initial Provider Infrastructure testing and (Alpha) testing schedules will be supported at the convenience of the Postal Service.

E. Demonstrable evidence of successful completion for each test is required prior to proceeding.

F. The Provider may continue with the product submission process upon receipt of authorization from the Postal Service to proceed.

1.9. Field Test (Beta) Approval (Limited Distribution)

A. The Provider will submit a proposed Field (Beta) Test Plan identifying test parameters, product quantities, geographic location, test participants, test duration, test milestones, and product recall plan. The Beta Test Plan will be in accordance with the Beta Test Strategy in effect for the given product type. The Postal Service will supply the appropriate Beta Test Strategy to the Provider upon request. The purpose of the Beta test is to demonstrate the proposed product’s utility, security, audit and control, functionality, and compatibility with other systems, including mail entry, acceptance, and processing, in a real-world environment. The Beta test will employ available communications and will interface with current operational systems to conduct all product functions. The Manager, Postage Technology Management will determine acceptance of Provider-proposed Beta Test Plans based on,

DRAFT

but not limited to, assessed risk of the product, product impact on Postal Service operations, and requirements for Postal Service resources. Proposed candidates for Beta test participation must be approved by the Postal Service. Beta test approval consideration will be based in whole or in part on the location, mail volume, mail characteristics, and mail origination and destination patterns.

B. The Provider has a duty to report security weaknesses to the Postal Service to ensure that each product/device model and every product/device in service protects the Postal Service against loss of revenue at all times. Beta participants must agree to a nondisclosure confidentiality agreement when reporting product security, audit, and control issues, deficiencies, or failures to the Provider and the Postal Service. A grant of Field Test Approval (FTA) does not constitute an irrevocable determination that the Postal Service is satisfied with the revenue-protection capabilities of the product/device. After approval is granted to manufacture and distribute a product/device, no change affecting the basic features or safeguards of a product/device may be made except as authorized or ordered by the Postal Service in writing from the Manager, Postage Technology Management.

C. The Provider may continue with the product submission process upon receipt of authorization from the Postal Service to proceed.

1.10. Provider/Product Approval (Full Distribution)

A. Upon receipt of the final certificate of evaluation from the national laboratory, where required, and after obtaining positive results of internal testing of the product/device, successful completion of Provider infrastructure testing, Alpha testing, demonstration of limited distribution activities (Beta testing), and audits of Provider site security, the Postal Service will administratively review the submitted product, the Provider infrastructure, and the Provider qualification requirements for final approval of full distribution. In preparation for the administrative review, the Provider shall update any product submission documentation submitted in compliance with the requirements of the Postage Evidencing Product Submission Procedure that is no longer accurate with respect to the product in review.

Note: Required qualifications for Providers of IBI systems can be found in draft 39 CFR Part 502, Manufacture, Distribution, and Use of Postal Security Devices and Information-Based Indicia, as published in the **Federal Register** on September 2, 1998. Copies are available by contacting USPS, Postage Technology Management, 475 L'Enfant Plaza SW, Room 8430, Washington DC 20260-2444. Copies of CFR Part 501 pertaining to manufacturer qualifications regarding postage meters are available also at the above address.

B. The Postal Service may require, at any time, that models/versions of approved products, and the design and user manuals and specifications applicable to such products, and any revisions thereof, be deposited with the Postal Service.

2. Change Control Procedure

2.1. Overview

A. After approval is granted to manufacture and distribute a product/device, no change affecting the basic features or safeguards of a product/device may be made except as authorized or ordered by the Postal Service in writing from the Manager, Postage Technology Management. The submission of a change proposal and the subsequent test and acceptance of a product change are designed to ensure not only that the changed product meets all requirements and performance criteria but also that the stated changes made to a product do not introduce any unintended, unidentified, unexpected, or undesirable changes to the form, fit, function, or security of the product.

B. Once a postage evidencing product/device has received final approval from the Postal Service, the Provider is required to submit any change(s) to that product for Postal Service approval. Changes covered by this process include, but are not limited to, the following:

- (1) Changes to the form, fit, function, or security of the product/device.
- (2) Changes resulting from new Postal Service regulations, such as an updated postal rate table.
- (3) Changes to the software or firmware.

DRAFT

- (4) Changes to the PSD, for products using such a device.
- (5) Changes to the physical configuration of the product.
- (6) Changes to the indicia design or to consumables, such as labels, that can be used with the product.
- (7) Changes to product documentation or packaging.
- (8) Changes to product distribution methods.
- (9) Changes to third party providers of significant product components.

C. For an IBI product, the changed product shall be in compliance with the IBI performance criteria and all other Postal Service regulations in effect at the time the change is implemented. All changes to previously approved products must be approved by the Postal Service before implementation. The Postal Service must also approve the timetable and procedures for implementing changes.

D. Providers are encouraged to consolidate multiple changes in a single change proposal to enable the Postal Service to expedite review of the changes.

E. The Provider shall fully document all changes, in accordance with the requirements described in the following sections.

2.2. Provider Responsibilities

A. The Provider shall be responsible for notifying the Postal Service of any proposed changes made as described in section 2.1. The Provider shall be responsible for having a Postal Service-approved process for configuration management of the versions of each approved product. The Provider's process shall ensure that no changes can be made without proper tracing of design changes, records of authorization, and notification to the Postal Service. The Provider is responsible for submitting a change proposal in accordance with the requirements of this procedure and for achieving Postal Service approval before implementing any change.

B. Detailed Provider Actions

(1) Letter of Intent to Change. The first step in the submission of a change proposal is to submit a Letter of Intent to Change, similar to the Letter of Intent described under Product Submission Procedures, above. The Letter of Intent to Change shall be submitted to the Manager, Postage Technology Management, United States Postal Service, 475 L'Enfant Plaza SW, Room 8430, Washington DC 20260-2444. The letter must include:

- (a) Date of correspondence.
- (b) Name and address of all parties involved in the change proposal, including those responsible for assembly, distribution, management of the product/device, hardware/firmware/software development or testing, and other organizations involved (or expected to be involved) with the changed product.
- (c) Name and phone number of official point of contact for each party identified above.
- (d) Change concept narrative. A description of the proposed change, identifying any changes to the form, fit, function, or security of the product.
- (e) Discussion of the reasons for the change.
- (f) Discussion of the implications of the change for product security, product identification, and Provider procedures such as distribution, operations, or financial transactions, as well as any cost impact and impact on product customers. The document shall also discuss the impact of the change on Postal procedures such as mail entry, mail acceptance, and mail processing, as well as the impact on the interfaces between the Provider and the Postal Service and/or customers.

DRAFT

(g) An outline of the actions the Provider will take in support of the change proposal, including a listing of the documentation the Provider will submit in support of the change, and the testing that will be performed to ensure the changes meet Postal Service requirements.

(h) The timetable for submission, test, acceptance, and implementation of the proposed change.

(i) The procedure for implementation of the proposed change.

(2) Additional documentation. Once the Letter of Intent to Change is submitted, the Provider shall review the following documents and submit any changes needed to ensure they are still current. Additional documentation may be required at the discretion of the Postal Service.

(a) Nondisclosure Agreements.

(b) Concept of Operations.

(c) Software and Documentation.

(d) Provider Infrastructure Plan.

(e) USPS Address Matching System (AMS) CD-ROM Integration, if required for the product.

(3) Testing. The Provider will test the product changes as described in the Postage Evidencing Product Submission Procedures to the extent required by the proposed change, in accordance with Postal Service direction. The Provider shall document the tests performed on product changes and shall submit this documentation along with verification of successful completion of the testing.

2.3. Postal Service Responsibilities

A. The Postal Service will execute its responsibilities in a timely manner.

B. The Postal Service will review the Letter of Intent to Change and accept or reject each component of the Provider's proposed approach for product change, documentation submittal, and testing, and schedule for release.

C. The Postal Service will complete testing of the changes as required to ensure the changes meet Postal Service performance criteria and provide written comments to the Provider. Approval of the change will be granted in writing by the Manager, Postage Technology Management.

D. The Postal Service reserves the right to determine if a proposed change is extensive enough to constitute a new product, rather than a change to a previously approved product. If such a determination is made, the Provider shall comply with all requirements of the Postage Evidencing Product Submission Procedures, including field-testing.

3. Intellectual Property and License Policy

Product Service Providers who choose to produce a postage evidencing product or service must comply with USPS Intellectual Property (IP) Requirements as a condition for receiving and maintaining regulatory approval. If a Product Service Provider is unable or unwilling to meet the IP Requirements, it should not offer the product or service.

Product Service Providers do not have authorization or consent from the USPS under 28 U.S.C. 1498(a) or otherwise to make or use any patented invention.

The USPS reserves the right and authority to discontinue a Product Service Provider's authorization to distribute a postage evidencing device or service if the USPS or a court determines that the manufacture of the device or service, the use of the device or service by mailers, or the validation of the indicia produced by the device or service, requires use of patented inventions for which Product Service Provider has not procured appropriate licenses.

This requirement applies to all aspects of the Product Service Provider's product or service, including those required or specified under applicable performance criteria.

DRAFT

4. Request for Comment

It is emphasized that the proposed procedures for initial product submission and changes to already approved products are being published for comments and are subject to final definition.

Although exempt from the notice and comment requirements of the Administrative Procedure Act (5 U.S.C. 553 (b), (c)) regarding proposed rule making by 39 U.S.C. 410 (a), the Postal Service invites public comments on the proposed procedures.

Stanley F. Mires,

Chief Counsel, Legislative.