POSTAL SERVICE

39 CFR Part 501

Revisions to the Requirements for Authority to Manufacture and Distribute Postage Evidencing Systems

AGENCY: Postal Service™.

ACTION: Final rule.

SUMMARY: This rule establishes the responsibility of the providers of Postage Evidencing Systems (PES) to notify the U.S. Postal Service® of any cyber attacks to their systems.

DATES: This rule is effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION].

ADDRESSES: Mail or deliver written comments to the Manager, Payment Technology, U.S. Postal Service, 475 L'Enfant Plaza SW, Room 3436, Washington, DC 20260-0911. Copies of all written comments will be available for inspection and photocopying between 9 a.m. and 4 p.m., Monday through Friday, at the Payment Technology office.

FOR FURTHER INFORMATION CONTACT: Marlo Kay Ivey, Business Programs Specialist, Payment Technology, U.S. Postal Service, at 202-268-7613.

SUPPLEMENTARY INFORMATION: Providers currently must disclose all findings or results of any testing concerning the security or revenue protection features, capabilities, or failings of any PES, as well as all potential security

weaknesses or methods of tampering with the PES. This rule applies the same standard to cyber attacks against the provider's systems.

List of Subjects in 39 CFR Part 501

Postal Service

Accordingly, for the reasons stated, 39 CFR Part 501 is amended as follows:

PART 501 — AUTHORIZATION TO MANUFACTURE AND DISTRIBUTE POSTAGE EVIDENCING SYSTEMS

1. The authority citation for 39 CFR Part 501 continues to read as follows:

Authority: 5 U.S.C. 552(a); 39 U.S.C. 101, 401, 403, 404, 410, 2601, 2605, Inspector General Act of 1978, as amended (Pub. L. 95-452, as amended); 5 U.S.C. App. 3.

2. Section 501.11 is amended by adding paragraph (b)(3) as follows:

§ 501.11 Reporting Postage Evidencing System security weaknesses.

* * * * *

(b) * * *

(3) Cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from

highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access. Cyber security risk disclosures reported must adequately describe the nature of the material risks and specify how each risk affects the Postage Evidencing System.

* * * * *

Stanley F. Mires,

Attorney, Legal Policy & Legislative Advice.

[END DOCUMENT]

[FR Doc. 2012-9396 Filed 04/18/2012 at 8:45 am; Publication Date: 04/19/2012]