

ELECTRONIC CODE OF FEDERAL REGULATIONS

e-CFR data is current as of July 13, 2017

[Title 40](#) → [Chapter I](#) → [Subchapter A](#) → [Part 3](#) → [Subpart D](#) → §3.2000

Title 40: Protection of Environment

[PART 3—CROSS-MEDIA ELECTRONIC REPORTING](#)

[Subpart D—Electronic Reporting Under EPA-Authorized State, Tribe, and Local Programs](#)

§3.2000 What are the requirements authorized state, tribe, and local programs' reporting systems must meet?

(a) Authorized programs that receive electronic documents in lieu of paper to satisfy requirements under such programs must:

(1) Use an acceptable electronic document receiving system as specified under paragraphs (b) and (c) of this section; and

(2) Require that any electronic document must bear the valid **electronic signature** of a signatory if that signatory would be required under the authorized program to sign the paper document for which the electronic document substitutes, unless the program has been approved by EPA to accept a handwritten signature on a separate paper submission. The paper submission must contain references to the electronic document sufficient for legal certainty that the signature was executed with the intention to certify to, attest to, or agree to the content of that electronic document.

(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that:

(1) The electronic document was not altered without detection during transmission or at any time after receipt;

(2) Any alterations to the electronic document during transmission or after receipt are fully documented;

(3) The electronic document was submitted knowingly and not by accident;

(4) Any individual identified in the electronic document submission as a submitter or signatory had the opportunity to review the copy of record in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or labeling of the information and had the opportunity to repudiate the electronic document based on this review; and

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each **electronic signature** was a valid **electronic signature** at the time of signing;

(ii) The electronic document cannot be altered without detection at any time after being signed;

(iii) Each signatory had the opportunity to review in a human-readable format the content of the electronic document that he or she was certifying to, attesting to or agreeing to by signing;

(iv) Each signatory had the opportunity, at the time of signing, to review the content or meaning of the required certification statement, including any applicable provisions that false certification carries criminal penalties;

(v) Each signatory has signed either an **electronic signature** agreement or a subscriber agreement with respect to the **electronic signature** device used to create his or her **electronic signature** on the electronic document;

(vi) The electronic document receiving system has automatically responded to the receipt of the electronic document with an acknowledgment that identifies the electronic document received, including the signatory and the date and time of

receipt, and is sent to at least one address that does not share the same access controls as the account used to make the electronic submission; and

(vii) For each **electronic signature** device used to create an **electronic signature** on the document, the identity of the individual uniquely entitled to use the device and his or her relation to any entity for which he or she will sign electronic documents has been determined with legal certainty by the issuing state, tribe, or local government. In the case of priority reports identified in the table in Appendix 1 of Part 3, this determination has been made before the electronic document is received, by means of:

(A) Identifiers or attributes that are verified (and that may be re-verified at any time) by attestation of disinterested individuals to be uniquely true of (or attributable to) the individual in whose name the application is submitted, based on information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization; or

(B) A method of determining identity no less stringent than would be permitted under paragraph (b)(5)(vii)(A) of this section; or

(C) Collection of either a subscriber agreement or a certification from a local registration authority that such an agreement has been received and securely stored.

(c) An authorized program that receives electronic documents in lieu of paper documents must ensure that:

(1) A person is subject to any appropriate civil, criminal penalties or other remedies under state, tribe, or local law for failure to comply with a reporting requirement if the person fails to comply with the applicable provisions for electronic reporting.

(2) Where an electronic document submitted to satisfy a state, tribe, or local reporting requirement bears an **electronic signature**, the **electronic signature** legally binds or obligates the signatory, or makes the signatory responsible, to the same extent as the signatory's handwritten signature on a paper document submitted to satisfy the same reporting requirement.

(3) Proof that a particular **electronic signature** device was used to create an **electronic signature** that is included in or logically associated with an electronic document submitted to satisfy a state, tribe, or local reporting requirement will suffice to establish that the individual uniquely entitled to use the device at the time of signature did so with the intent to sign the electronic document and give it effect.

(4) Nothing in the authorized program limits the use of electronic documents or information derived from electronic documents as evidence in enforcement proceedings.

[Need assistance?](#)