

NATIONAL MARINE FISHERIES SERVICE POLICY DIRECTIVE PD 32-110

September 7, 2006

Information Management

USE AND IMPLEMENTATION OF ELECTRONIC SIGNATURES

NOTICE: This publication is available at: <http://www.nmfs.noaa.gov/directives/>.

OPR: F/OP (E. Helm)

Certified by: F/OP (M. Holliday)

Type of Issuance: Renewed Jan 2010

SUMMARY OF REVISIONS:

Introduction: Under Sections 1703 and 1704 of the Government Paperwork Elimination Act (GPEA)¹, Executive agencies are required to provide for the use and acceptance of electronic signatures. The term “electronic signature” means a method of signing an electronic message that: (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message². GPEA specifically states that: “Electronic records submitted or maintained in accordance with the procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form”³.

The Office of Management and Budget developed guidance for Executive agencies as required under Sections 1703 and 1704 of GPEA. This guidance instructed the Departments of Justice (DOJ), Treasury, and Commerce (NIST), and the National Archives and Records Administration (NARA) to develop GPEA and electronic signature policies, practices, and standards with respect to legal considerations, payments and collections, technological requirements, and management, preservation, and disposal of Federal records respectively.

This document articulates NMFS’ policy with regard to the use and implementation of electronic signatures. The policy is consistent with GPEA and existing OMB, DOJ, Treasury, NIST, NARA, DOC, and NOAA guidance, policies, practices, and standards.

Objective: It is NMFS’ policy to use and accept electronic signatures whenever possible and to encourage agency programs to provide individuals or entities with the option of submitting information or transacting business with the agency electronically. Both the decision to use an electronic signature authentication procedure and the implementation of that electronic signature should follow applicable statutes and regulations. The evaluation process and the required elements are outlined below:

1 Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII.

2 GPEA Section 1710(1).

3 GPEA Section 1707. Also see U.S. Dep’t of Justice, Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies (November 2000) pages 13-20 on legal considerations related to e-signatures. While GPEA provides that certain electronic records or signatures shall not be “denied legal effect, validity, or enforceability because such records are in electronic form,” the Act “does not require courts to accept electronic records and signatures that are deficient in other respects merely because they are in electronic form.”

Electronic Signature Evaluation Process

1. In determining the practicability and assessing the choice among alternative electronic signature procedures for a particular application, consideration should be given to: (1) the agency's legal mandates to determine if the use of an electronic signature is contradicted by statute for the specific application; and (2) the specific legal implications of the use of an electronic signature in terms of enforceability, liability, confidentiality, and privacy.
2. A qualitative (and where possible quantitative) assessment should be conducted on the types and level of risk arising from:
 - (1) the relationships between the parties (e.g., agency to general public versus intra-agency);
 - (2) the value of and legal considerations related to the transaction (e.g., contracts or funds transfers, use in enforcement proceedings or other litigation, protected or sensitive information,);
 - (3) the potential for fraud and repudiation of the information and transactions being signed;
 - (4) the unauthorized access to, modification of, loss, or corruption of the data; and (5) the probability that a damaging event (e.g. fraud or unauthorized access) will occur.
3. NMFS should conduct qualitative analyses and to the extent possible quantify: (1) the costs associated with the risk and potential losses due to a damaging event, risk reduction and mitigation measures, implementation, operation and maintenance, and costs to the customers (e.g. need for new hardware, software, and knowledge); and (2) the benefits which stem from increased data availability, increased transaction speed, reduced transaction costs, increased customer satisfaction, and other considerations⁴.
4. The choice among the alternative electronic signature processes, which reduce risk to acceptable levels, should be informed by the maximization of net benefits to both NMFS and the other individuals and/or entities involved in the electronic transaction. If net benefits are negative it may be determined, by the implementing office, that an e-signature process is not practicable at this time.

Electronic Signature Implementation Requirements

1. The implementation of an e-signature system must contain some form of technical non-repudiation services to protect the reliability, authenticity, integrity, and usability, as well as the confidentiality, and legitimate use of the electronically-signed information.
2. The technical non-repudiation services (required in number 1 above) should tie the electronic transaction to the individual or entity in a legally-binding way.
3. The electronic signature process should include, as part of its technical non-repudiation services, audit trails that ensure the chain of custody for the transaction. These audit trails should identify the sending location, sending individual or entity, date and time stamp of receipt, and other measures that will ensure the integrity of the document. These audit trails must validate the integrity of the transaction and prove: (1) that the

⁴ The analysis of risk, costs, and benefits of the electronic signature processes is obviously impacted in large part by the type of information and documents which are being linked to the signature. Therefore, different electronic signature technologies may be warranted across differing applications.

Attachment 1 - Glossary

Authenticity: An authentic record is one that is proven to be what it purports to be; to have been created or sent by the person who purports to have created and sent it; and is protected against unauthorized addition, deletion, and alteration.

Electronic signature: A method of signing an electronic message that: (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message.

Integrity: The integrity of a record refers to it being complete and unaltered.

Non-repudiation: Steps taken by an agency to provide assurance, via the use of an audit trail, that a sender cannot deny being the source of a message, and that a recipient cannot deny receipt of a message.

Reliability: A reliable record is one whose content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.

Usability: A usable record is one which can be located, retrieved, presented, and interpreted. In any subsequent retrieval and use, the record should be capable of being directly connected to the business activity or transaction which produced it.

References

Computer Security Act, P. L. 100-235

Circular No. A-130 (Revised). Office of Management and Budget. November 28, 2000

Federal Agency Use of Public Key Technology for Digital Signatures and Authentication. NIST Special Publication 800-25

Electronic Authentication Policy. Financial Management Service, Fiscal Service, Treasury Department. January 3, 2001

Federal Records Act (44 U.S.C. 3101)

Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII

Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies. U.S. Justice Department. November 2000

Privacy Act, as amended (5 U.S.C. 552a)

Records Management Guidance for Agencies Implementing Electronic Signature Technologies. National Archives and Records Administration. October 18, 2000