NATIONAL MARINE FISHERIES SERVICE INSTRUCTION 32-110-01
JUNE 25, 2007

Information Management
Use and Implementation of Electronic Signatures

EVALUATION 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 March 2013

SUMMARY OF REVISIONS:

/s/ 06/11/07
Signed _____
Mark Holliday, Ph. D.
Director, Office of Policy Date

Evaluation and Implementation of Electronic Signatures - Procedural Directive

Section I Overview

NMFS adopted on September 7, 2006 a policy with respect to the "Use and Implementation of Electronic Signatures" (32-110). This policy directive outlined both an electronic signature evaluation process and implementation requirements. This document expounds on the specific steps listed under both the evaluation and implementation headings. This procedural directive is organized in three sections: the overview, the electronic signature evaluation process, and the electronic signature implementation requirements. The number of each sub-section in this document corresponds to a defined step in the policy document (which is reprinted in italics in this document).

This document expounds on the steps and requirements that are necessary to fulfill the evaluation and implementation components of the policy directive. It does not outline the process by which the headquarters, regional, and science center offices initially identify e-signature projects and the process for giving preliminary, partial, and final approval/disapproval for the project. These "Evaluation, Approval, and Implementation Plans" should be developed by the specific offices in consultation with F/CIO, GCF, and GCEL. An example of one possible approach an office may take is a four step process consisting of: (1) a brief scoping document; (2) a more detailed business plan; (3) an evaluation of the business plan; and (4) the implementation of the e-signature process. The program manager within an office may start internally with a brief scoping document designed to give an explanation of the transaction targeted for an e-signature; who wants the electronic signatures in this case; the benefits to NMFS and its partners; the estimated cost and timeframes; and a plan (staff, schedule) to build a more detailed business plan for the project. This scoping document would be used to obtain the support and approval of the office's management and support from needed outside offices. With approval, the second step would be to develop a business plan for the electronic signature project. The business plan should explain why the electronic signature for a transaction is beneficial and "practicable." It would include: the current (as is) process; demand for electronic signature support; the new electronic process including the implementation requirements (Section III below); a risk assessment (based on Section II below); cost estimates; a benefits statement; the cost-benefits analysis; and an implementation plan outline (timeline, milestones, and staffing). The business plan would then be evaluated by office management with input from F/CIO, GCF, and GCEL based on the criterion outlined in the policy directive and this procedural directive. If approved the final step in the process would be the implementation of electronic signature process as described in the business plan.

Section II Electronic Signature Evaluation Process

1. Determination of Electronic Signature Acceptability and Legal Implications

In determining the practicability and assessing the appropriateness of alternative electronic signature procedures for a particular application, consideration should be given to: (1) the

agency's policies and legal mandates to determine if the use of an electronic signature is acceptable 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.

Whenever NMFS interacts with outside parties, it faces the question of how its actions make it legally liable to affected parties. The case of electronic signature authentication is no exception, therefore the implementing office should consider the legal implications of moving to an electronic system and the ways in which that system may be designed to minimize the negative and maximize the positive legal implications for the agency. The Department of Justice (DOJ) guidance document entitled "Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies" provides a helpful overview of potential legal issues that could arise under an e-signature process. Additional legal requirements and guidance which need to be considered by the implementing office are documented throughout this procedural directive.

In addition, the implementing NMFS office in coordination with GCF and GCEL should consider whether the agency's legal mandates, current policies, or programmatic regulations support the use and enforceability of the electronic signature alternatives and the necessary electronic record keeping. If the implementing office finds that NMFS polices or programmatic guidance should and can be revised to achieve the goal of moving toward the use of electronic signatures they should coordinate with F/CIO, GCF, and GCEL to make the necessary improvements to the existing NMFS policies and guidance.

2. Assessment of the Types and Levels of Risk

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, acceptability of e-signature for transaction); (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.

A Qualitative Approach to Assessing Risk

NMFS has adapted its qualitative electronic signatures risk assessment approach from OMB's 2003 memorandum "E-Authentication Guidance for Federal Agencies" (M-04-04) and DoC, NIST's Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." These documents deal with the larger issue of determining people or entities identity through electronic means, but with minor modification apply very well to the specific case of electronic signatures.

There are two components to the total risk which NMFS faces in transacting with outside parties:

1. the potential harm or impact from one or more damaging events
2. the probability of those damaging events occurring

The NMFS implementing office, with input from GCF, GCEL, and F/CIO, should follow the steps outlined below in the qualitative analysis of the risk involved in implementing an e-signature process. Additional information which is helpful in determining the level of risk and probability of occurrence faced by the agency and the other parties involved in the transaction is provided in a text box at the end of this section. Also, information on the quantification of these risks can be found in sub-section 3 (entitled "Cost Benefit Analysis").

STEP 1:

The implementing office should define the set of possible damaging events which could occur in connection with the utilization of the proposed electronic signature authentication process. (NOTE: This "process" includes not only the signature verification but the long term storage and access policies.) It is important to remember that when the set of events is compiled the Office must consider the type of transactions, documents, and information which are being linked to the signature. The signature itself can be used: (1) to simply identify the sender of a document and/or data, or (2) to identify the sender and indicate the intent of the sender. These differing purposes of the electronic signature may lead to different sets of possible damaging events. Examples below:

- fraud and repudiation of the information and transactions
- the unauthorized access to the document or information
- modification of the information
- loss or corruption of the data

STEP 2:

The NMFS office should determine the impacts of each of the damaging events which have been defined in STEP 1. Each damaging event may have one or more types of impacts of varying severity and they may accrue to the agency and/or one or more of its transacting parties. The potential harm or impacts of damaging events may be subdivided as follows (NOTE: The implementing office should consider defining additional case specific impact categories.):

1. Inconvenience, distress, or damage to standing or reputation to any party
2. Financial loss to any party
3. Agency liability
4. Harm to agency programs or public interests
5. Unauthorized release of sensitive information
6. Personal safety
7. Civil or criminal violations

The implementing office should assess the potential harms and impacts of a damaging event, whether direct or indirect, for each of the categories defined in the previous step. As part of this qualitative approach NIST has established three levels of potential harm or impact - low, moderate, and high (there may also be "no" impact). These three levels are defined, for each of

the eight categories above, in Table A. It is important to note that a qualitative risk analysis depends on the expertise, experience, and good judgment of the project managers conducting the analysis. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. (NOTE: If additional case specific impact categories are defined, the implementing office, with input from GCF, GCLE, and F/CIO, should develop the criteria which determine low, moderate, and high levels of potential impacts.)

Table A: Summary of the Potential Impacts of E-signature Process Failures

POTENTIAL IMPACTS			
TYPES OF IMPACTS	**LOW**	**MODERATE**	**HIGH**
Inconvenience, distress, or damage to standing or reputation	at worst, **limited**, short-term inconvenience, distress or embarrassment to any party	at worst, **serious** short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	**severe or serious** long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals)
Impact of financial loss	at worst, an **insignificant** or inconsequential unrecoverable financial loss to any party	at worst, a **serious** unrecoverable financial loss to any party	**severe or catastrophic** unrecoverable financial loss to any party
Impact of agency liability	at worst, an **insignificant** or inconsequential agency liability	at worst, a **serious** agency liability	**severe or catastrophic** agency liability
Impact of harm to agency programs or public interests	at worst, a **limited** adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests	at worst, a **serious** adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets	a **severe or catastrophic** adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets

		or public interests	or public interests
Impact of unauthorized release of sensitive information	at worst, a limited unauthorized release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with an expected **limited** adverse effect on organizational operations, organizational assets, or individuals	at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with an expected **serious** adverse effect on organizational operations, organizational assets, or individuals.	a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with an expected **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals
Impact to personal safety	at worst, **minor** injury not requiring medical treatment	at worst, moderate risk of **minor** injury or **limited** risk of injury requiring medical treatment	a risk of **serious** injury or death
Impact of civil or criminal violations	at worst, a risk of civil or criminal violations of a nature that would **not ordinarily be subject to enforcement** efforts	at worst, a risk of civil or criminal violations **that may be subject to enforcement** efforts	a risk of civil or criminal violations that **are of special importance to enforcement** programs

STEP 3:

The implementing office needs to finally determine the probability of potential occurrence for each of the possible impacts determined in STEP 2 above. In this qualitative assessment we are adopting a threshold approach. For each of the damaging events that were defined in STEP 1 the implementing office, with input from GCF, GCEL, and F/CIO, should define a level or rate of occurrence that would be considered to be "significant". The implementing office should then determine if a significant probability of occurrence exists for each of the potentially damaging events defined in STEP 1. This determination of significant/not significant probability must then be carried over to the list of potentially negative impacts (defined in STEP 2) which can arise from the damaging events. (NOTE: It is important to keep in mind there may be multiple damaging events that also have more then one potential impact. The implementing office should therefore pay special attention to cumulative impacts.) A "significant" probability of a potential negative impact is the rate at which the project managers believe more stringent e-signature

authentication and/or storage procedures should be implemented to decrease the total potential harm caused to NMFS and its transacting partners.

Additional information which is important to determining the level of risk and probability of occurrence faced by the Agency and the other parties involved in the transaction is provided in OMB guidance for E-authentication ("E-Authentication Guidance for Federal Agencies," 2003) and GPEA implementation ("Implementation of the Government Paperwork Elimination Act," 2000). These guidance documents offer information on assessing the severity of risk based on the properties of both the e-signature authentication process as well as its corresponding document. They also discuss the determination of the probability that a damaging even will occur.

Given the determination of the level of potential impacts and significance of probability the implementing office can use the information contained in Section 3.1 of the implementation section of this document to determine which if any e-signature process can reduce the level of risk to acceptable levels.

3-4. Cost-Benefit Analysis

The "Use and Implementation of Electronic Signatures" policy directive states that:

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 considerations.

Further:

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.

The cost and benefit components in the electronic signatures evaluation process are important for determining which of the electronic signature processes should be implemented of those that have been determined to reduce risk to acceptable levels. The cost benefit assessment will help with the identification of the particular technologies and management controls that will minimize the cost (given the reduction of risk to acceptable levels), both to NMFS and its partners, and maximize the benefits to the parties involved. This cost-efficiency concept is derived from the Computer Security Act which gives agency managers the responsibility to select an appropriate combination of technologies, practices, and management controls to minimize risk cost-effectively while maximizing benefits to all parties to the transaction. The implementing office should note that the decision process should be documented, not only as part of the e-signature

process, but this documentation may also have to be included in the agency's system security plan (see the NIST "Guide for Developing Security Plans for Information Technology Systems," Special Publication 800-18 (December 1998)) for later review and adjustment. To the extent possible the assessment should be quantitative, but some factors (i.e. those related to risk analysis) may need to be assessed qualitatively. Some of the potential costs and benefits of moving from a paper to an electronic signature process are discussed in the following two sub-sections.

Costs

In estimating the cost of the e-signature authentication and data storage system, the implementing office, to the extent possible, should estimate the costs that may result from a failure in the e-signature system to the agency and its transacting partners. The potential areas of negative impact have been defined in the qualitative risk analysis that would be conducted under Section 2.2 above. Based on the assessed severity of the potential impacts the office may be able to value the potential (1) cost to the transacting parties for inconvenience, distress, or damage to standing or reputation; (2) the financial loss faced by the agency and/or transacting parties; (3) agency liability costs; (4) the harm to agency programs or public interests; (5) the negative impacts from the unauthorized release of sensitive information; (6) threats to personal safety; and (7) the negative costs of civil or criminal violations. All of the potential categories (plus those categories additionally defined by the implementing office) would then be tempered by the estimated probability of occurrence when determining the final estimated cost of risk.

In addition to the estimated cost of the potential risk, the implementing office should also include costs associated with hardware, software, administration, and support of the system, both short-term and long-term. With greater projected impacts and probability of occurrence (defined in Section 2.2 above), there comes a greater level of complexity to ensure mitigation of the risk for both the agency and the transacting party. This will translate into additional hardware and software requirements for both NMFS and the other parties to the transaction, greater transaction time, greater processing time, greater data storage requirements, additional energy requirements, a higher level of training for the transacting parties, a higher level of training for staff involved with the development and maintenance of the application, greater potential repair times and more monitoring and testing for security issues.

Benefits

The implementing office should identify all the categories through which the agency and its transacting partners may receive benefits and, to the extent possible, estimate the value derived from enacting a secure e-signature process, thereby automating certain transactions within a NMFS' program. Some of the benefits categories may include; (1) those resulting from increased transaction speeds; (2) greater customer satisfaction and increased participation rates; (3) higher transaction completion rates; (4) improved record keeping efficiency and data analysis opportunities (Data being easier to store and access for analysis can enhance program effectiveness and evaluation, expand awareness of the impact of the government program, and aid enforcement efforts); (5) increased employee productivity and improved quality of the final

product; (6) greater information benefits to the public; and (7) potentially improved security resulting from a properly designed authentication process.

Section III Electronic Signature Implementation Requirements

1. Technical Non-repudiation Services

The implementation of an e-signature system must contain some form of technical non-repudiation services in order to protect the reliability, authenticity, integrity, and usability, as well as the confidentiality, and legitimate use of the electronically-signed information.

OMB ("E-Authentication Guidance for Federal Agencies") and NIST ("Standards for Security Categorization of Federal Information and Information Systems") describe four identity authentication assurance levels for e-government transactions that are applicable to the case of NMFS use of electronic signatures. Each assurance level describes the agency's degree of certainty that the transacting party has presented an identifier or token (a credential) that refers to their identity. Assurance is defined as (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. There are four assurance levels:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

In order to determine the assurance level necessary to mitigate the risk that was characterized in the "electronic signature evaluation process" the implementing office should use Table B (or a similar table that would be developed with input from GCF, GCLE, and F/CIO for a specific implementation) below. Having determined the degree of potential harm (low, moderate, or high) under each of their defined impact categories along with making the determination of whether there is a significant probability of occurrence within a category, the implementing office may then chart the assurance level (1-4) that would mitigate the risk within an impact category. To determine the required assurance level for the e-signature project, find the lowest assurance level that can mitigate the degree of potential harm over all the impact categories. In some cases (as shown in Table B), the potential degree of impact may correspond to multiple assurance levels. For example, Table B shows that a moderate risk of financial loss corresponds to assurance levels 2 and 3. In such instances, the implementing office should use the context of the specific case and their best professional judgment to determine the appropriate assurance level.

Table B – Maximum Potential Impacts for Each Assurance Level

Assurance Level Profiles (Impact)				
Potential Impact Categories	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High

Financial loss or agency liability	Low	Mod	Mod	High
Agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High
Assurance Level Profiles (Impact with a Significant Probability of Occurrence)				
Inconvenience, distress or damage to standing or reputation	N/A	Low	Mod	Mod High
Financial loss	N/A	Low	Mod	Mod High
Agency liability	N/A	Low	Mod	Mod High
Harm to agency programs or public interests	N/A	N/A	Low	Mod High
Unauthorized release of sensitive information	N/A	N/A	Low	Mod High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	N/A	Low	Mod High

After the implementing office has determined the required assurance level by choosing the lowest level of authentication that will mitigate to acceptable levels the potential impacts identified in the risk assessment, the agency should refer to the NIST e-authentication technical guidance ("Electronic Authentication Guideline," SP 800-63) to identify and implement the appropriate technical requirements. A brief outline of the technologies available for each assurance level is presented below:

Assurance Level 1: This level allows the use of the following token types; (1) personal identification numbers (PIN); (2) Strong password; (3) one-time password device; (4) soft cryptographic tokens; and (5) hard cryptographic tokens. Which are to be used in conjunction with the following cryptographic authentication protocols; (1) challenge-response; (2) tunneled password; (3) zero knowledge password; (4) systematic key proof of possession (PoP) protocol; or (5) private key PoP protocol. Transactions at this assurance level must be protected against on-line guessing and replay using the transacting party's credentials.

Assurance Level 2: Level 2 restricts the allowed tokens by removing the opportunity to use PINs in the authentication process, leaving; (1) Strong password; (2) one-time password device; (3) soft cryptographic tokens; and (4) hard cryptographic tokens. The protocols for authentication are restricted to; (1) tunneled password; (2) zero knowledge password; (3) systematic key PoP protocol; or (4) private key PoP protocol. Transactions at this assurance level must be protected against; (1) on-line guessing; (2) replay; and (3) eavesdropping.

Assurance Level 3: This level allows the use of (1) one-time password device; (2) soft cryptographic tokens; and (3) hard cryptographic tokens. You may use the (1) systematic key PoP authentication protocol; or (2) the private key PoP authentication protocol. Transactions at this assurance level must be protected against; (1) on-line guessing; (2) replay; (3) eavesdropping; (4) verifier impersonation; and (5) man-in-the-middle interceptions.

Assurance Level 4: This highest level of assurance only allows the use of hard cryptographic tokens and the systematic and private key PoP authentication protocols. Transactions at this assurance level must be protected against; (1) on-line guessing; (2) replay; (3) eavesdropping; (4) verifier impersonation; (5) man-in-the-middle interceptions; and (6) session hijacking.

2. Legally Bind the Electronic Transaction to the Individual or Entity

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.

In order to minimize the likelihood of repudiation NMFS implementing offices should develop well-documented mechanisms and procedures to tie transactions to an individual in a legally binding way. One way to help link transactions to submitters is to ensure, at the outset, that all conditions of submission and receipt of the electronically signed data are known and understood by the submitting parties. This could be accomplished through the use of a document referred to as a "terms and conditions" agreement that would require a willful act by the recipient that demonstrates that they have read, understand, and accept the material they have been presented. As a additional precaution, it would be helpful to establish that the transacting individual or entity is fully aware of obligations they are agreeing to by signing the electronic document (e.g. permit or logbook), at the time of signature. This can be accomplished by programming the appropriate ceremonial banners into the software application's "signing ceremony" that alert the individual of the seriousness of the action they are about to undertake. These banners must present the sending entity with an additional "terms and conditions" agreement related to the specific implications of signing the document, which they must approve, and a completed document for review during the signing ceremony, which they must also confirm to be correct. And the signing of the document must make the transacting party take willful action to indicate their desire to sign the document.

While the above text provides general suggestions, the specific components needed for binding an electronic transaction to the transacting party may vary with regard to the risk assessment evaluation and the purpose/use of the electronic submission program, be it data collection or law enforcement related. See OMB's "Implementation of the Government Paperwork Elimination Act" procedures and guidance for more details.

3. Chain of Custody Audit Trails

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 connection between the submitter and NMFS has not been tampered with; and (2) how the document was controlled upon receipt by NMFS.

Electronic audit trails must provide a chain of custody for the secure electronic transaction that can be used to ensure the integrity of the document. This is a critical component in the protection of the agency and its transacting partners from potential fraud and privacy violation claims, as well as allowing for a strong defense against repudiation, and strong enforcement of agreements and laws. The audit trail information may be needed for audits, disputes, or court cases many years after the transaction itself took place and long-term retention of not only the signed document but the accompanying audit trail should be addressed (See Sub-section 6 below).

Based on the risk analysis results completed in Section 2.2 of the evaluation process, which led to the designation of a required minimum assurance level, the implementing office may chose to require different audit trail component. As a general rule when the risk associated with a transaction increases the number of components tracked as part of the audit trail should increase.

There are two parts to the audit trail documentation. The first addresses the integrity of the transaction as it occurs. The second records how NMFS handles the information after it has been received. In order to validate the initial transaction the tracking system needs to record the sending location, sending individual or entity, date and time stamp of receipt, proof that the agency sent a "receipt" acknowledging the arrival of the document and signature, and a confirmation of the individual receiving the agency "receipt." If approved changes are made to the signed document all of the information that is collected as part of the audit trail for the original transaction should be collected again with respect to the revised document. The original document along with it audit trail should not be deleted from the agency's records. It is equally important for insuring the reliability of a document to carefully control the electronic data and track any approved or not approved changes and access to the document and its associated audit trail once in NMFS hands. The audit trail for tracking any changes to the document and signature package once at NMFS should include identification of the individual or entity that is making a change, a date and time stamp of the change, and all of the documentation prior to the change should be maintained in the audit trail.

Additional information on audit trails can be found in the NARA guidelines for records management with regard to implementing electronic signatures ("Records Management Guidance for Agencies Implementing Electronic Signature Technologies").

4. Electronic Receipt or Acknowledgement of Successful Submission

An electronic receipt or some form of electronic acknowledgement of a successful submission of the electronic record and signature should be provided.

Section 1703(b)(D) of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII specifically states that the agency's system for receiving electronic signed transactions is required to have a mechanism for acknowledging receipt of the transactions received and

acknowledging confirmation of transactions sent. This electronic "receipt" should be printable and should also be electronically storable. It should also specifically indicate the parties involved in the transaction, summarize the agreement made, and contain a "confirmation code" that would allow the parties involved to easily interact with the agency regarding the transaction in the future. If the electronic submission to the agency is made by e-mail and the signature process allows for the acceptance of data from alternate e-mail addresses a "receipt" should be sent to both the address from which the transaction was initiated and the address of record for the transacting party (the address obtained in the initial registration and identity proofing). An audit trail should also track the fact that a "receipt" was sent and received by the parties.

5. Use of Information Collected in the Electronic Signature Authentication Process

The fifth point under the "Electronic Signature Implementation Requirements" of the NMFS policy directive reads as follows:

Section 1708 of GPEA states that information collected from individuals and entities as part of an electronic signature authentication process may only be use to facilitate that electronic communication process between the individual or entity and a federal agency.

This point was expanded upon in OMB's "Implementation of the Government Paperwork Elimination Act" document that directs agencies and their staff and contractors not to use such information for any purpose other than for facilitating the communication. Exceptions exist if the person (or entity) that is the subject of the information provides affirmative consent to the additional use of the information, or if such additional use is otherwise provided by law. As a result of GPEA and OMB's guidance, the NMFS implementing office should follow several privacy principles:

1. Electronic signatures should only be required when needed. For transactions where no funds are transferred, no financial or legal liability is involved and the identity of the transacting entity is not necessary to fulfill the agency's mission identifying or other personal information about an individual or entity should not be required.
2. When electronic signatures are required for a transaction, agencies should not collect more information from the user than is required for the electronic signature process. When appropriate, agencies are encouraged to use methods of electronic signing that do not require individuals to disclose their identity. This includes the ability of individuals in a group to be identified by a group identifier.
3. If the user finds the electronic authentication process made available is not acceptable, the user should be able to opt out to a paper process.
4. The implementing NMFS Office should ensure, and users should be informed, that information collected for the purpose of issuing or using electronic means of authentication will be managed and protected in accordance with applicable requirements under the Privacy Act, the Computer Security Act, and any other relevant laws or Executive Branch and DOC, NOAA, and NMFS specific privacy policies.

6. Long-term Retention and Access Policy

The implementing office should incorporate a long-term retention and access policy for the use of electronic signatures in electronic records with particular attention paid to the preservation of legal rights.

All Electronic signature record retention must meet the requirements of the Federal Records Act (44 U.S.C. 3101) and NARA's "Records Management Guidance for Agencies Implementing Electronic Signature Technologies." If an electronically signed record needs to be preserved, whether for a finite period of time or permanently, then the agency needs to ensure its trustworthiness. NARA defines a record to be trustworthy if it is reliable, authentic, maintains its integrity, and is useable. The methodological components that ensure a trustworthy signature are discussed in Section III Parts 1-4 above.

It is also important to recognize that the implementation of the electronic signature requirements of GPEA will produce new types of records and/or additional component to existing records. Therefore, the implementing office should develop records schedules with proposed retention periods for these new records, based on their operational needs and the estimated level of risk calculated during the evaluation process. These newly developed schedules may result in the agency modifying their records disposition authorities for existing records. A step which must be reviewed and approved, by DOC OGC and NARA, before disposal of any records takes place.

Electronically-signed records documenting legal rights and all other electronically-signed records that are permanently retained by the agency must include, as part of any human readable form (on screen display or printout) of the record, the printed name of the signer and the date of signature. The agency must also plan for software obsolescence when storing legally binding electronic material for long periods of time. The agency will need to address how records will by migrated to newer versions of software (or how current software will be maintained for future use) without adversely affecting the recognition and enforceability of the legal rights conveyed in the documents.

7. Review and Re-evaluation of the Electronic Signature Process

Periodic review and re-evaluation of the electronic signature process must be performed with particular attention paid to continuing changes in technology, law, and policy guidance.

The NMFS implementing office, with the input of F/CIO, GCF, and GCEL, should develop as part of their implementation strategy a quality assurance plan which outlines the timeline and criterion by which the electronic signature program shall be evaluated. The criterion should include not only technical indicators such as the number of logins, the average completion time and rate, and the number of data resubmissions, but measures of the effectiveness of the e-signature at forwarding programmatic goals. The implementing NMFS office in conjunction with F/CIO will conduct this review and re-evaluation of the implemented electronic signature process to determine the effectiveness of the process and whether changes are warranted. The results of this assessment process must be fully documented.

F/CIO will determine based on the results of these reviews across implementing offices if changes need to be made to the agency's electronic signature policy directive and other NMFS

guidance documents. These documents will also be revised and updated by F/CIO in response to changes in technology, law, and other government agencies' policy guidance.

References

Computer Security Act, P. L. 100-235

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

E-Authentication Guidance for Federal Agencies. Office of Management and Budget. December 16, 2003

Electronic Authentication Guideline. NIST Special Publication 800-63

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

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

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

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

Implementation of the Government Paperwork Elimination Act. Office of Management and Budget. April 25, 2000

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