

**NORTHWEST AND SOUTHWEST REGION**

**ELECTRONIC FISHTICKET  
E SIGNATURE BUSINESS PLAN**

**Contents**

West Coast E-fishticket Background ..... 3

E-signature Business Plan Introduction ..... 4

Current "As is" Process ..... 4

Demand for Electronic Signature Support ..... 5

Proposed Electronic Process ..... 6

E-Signature Risk Assessment ..... 7

    E-signature Risk Mitigation ..... 17

Cost Estimates ..... 18

Benefits Statement ..... 18

Cost Benefits Analysis ..... 19

Implementation Details ..... 20

Implementation Plan Outline ..... 29

## **West Coast E-fishticket Background**

Along the Pacific coast of the U.S., the coastal states of Washington, Oregon, and California have longstanding state fish ticket programs. These programs were originally developed for revenue purposes, but the fish tickets have become multi-purpose documents, functioning as a receipt between buyer and seller, as a record of catch (and sometimes of effort) for fisheries management, as documentation of participation in a fishery, as a record of gross profit for calculation of crew shares, as documentation of value for economic analysis, and of course the original purpose of government tax records. Examples of state fish tickets include whiting in Washington and salmon in California. The information captured on fish tickets has been standardized to the point that PACIFIC FISHERIES INFORMATION NETWORK (PACFIN) can aggregate fish ticket data from each state into a regional database.

Whiting fisheries in the Northwest Region have been operating under an Exempted Fishing Permit through the 2009 season. Amendment 10 to the Pacific Groundfish fishery management plan (FMP) will bring this fishery under Federal regulation in 2010. In 2009 Amendment 15 identified qualified vessels for a whiting endorsement to their limited entry trawl permit. The whiting EFP, Amendment 10, and Amendment 15 recognize a need to track bycatch on a near real-time basis, and specify electronic reporting, or an e-ticket program, as the mechanism. This e-ticket reporting is in parallel with the states of Washington, Oregon, and California traditional paper fish tickets. PSMFC is currently developing, implementing, and evaluating this e-ticket program, emulating and coexisting with state fish ticket programs, capturing data into the database directly from participating processors. This parallel approach is emulating state programs with no change in management approach, data elements, etc. and allows states flexibility and time to adopt at their convenience.

For the Whiting fishery an e-ticket provides the most effective mechanism for acquiring near real-time catch and bycatch information. Fish ticket record-keeping and reporting regulations require processor and vessel operator signatures for accountability. An e-signature feature is required to make e-ticket reporting (without a corresponding paper document for signatures) feasible. By near real-time we mean an elapsed time of less than 48 hours from the completion of the vessel offload to data analysis in the agencies catch and bycatch monitoring systems.

The trawl fleet (whiting) is the most technology sophisticated fleet in the Northwest Region, but, by regulation fish tickets are reported by processors. Whiting processors are large permanent shoreside facilities which are completely

comfortable with this type of technology. The current whiting fishery fish ticket volume is approximately 40 boats for up to 20 days of fishing, for a ceiling of approximately 800 transactions. The potential of e-ticket transactions would eventually approach the total volume of fish tickets on the West Coast.

## **E-signature Business Plan Introduction**

The Electronic Signature Business Plan is the second phase of a four phase process required by the NMFS procedural directive for e-signatures to allow NMFS applications to use electronic signatures. This phase is designed to explain why an electronic signature for a transaction is beneficial and "practicable", both to NMFS and its end users. The business plan also discusses the current process that will be replaced by the e-government application, the demand for electronic signatures in the application, how NPS plans to implement electronic signatures in this context, the various costs and benefits, and an implementation plan outline. The remaining two phases in implementing electronic signatures required by the procedural directive are:

1. Evaluation and Approval of the Business Plan, and
2. Implementation of the Electronic Signature Process.

NMFS manages fishing in waters of the United States and international waters under authority of various statutes and laws, primarily the Magnuson-Stevens Fishery Conservation and Management Act (Public Law 94-265, as variously amended, most recently by the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act (P.L. 109-479)) (MSA) and the High Seas Fishery Management and Conservation Act.

Moving to an electronic system for the collection of West Coast Fishticket data has many beneficial and practicable benefits in the form of increased NMFS efficiency, data accuracy, and burden reduction for operators over the current paper process.

## **Current "As is" Process**

Per 50 CFR part 660.303 operators of Pacific Whiting vessels delivering whiting during the primary season, and buyers of Pacific Whiting, are required to report deliveries on state fish tickets. In addition the buyer submits an electronic fish ticket for that delivery. To include as part of each electronic fish ticket submission, the actual scale weight for each groundfish species as specifies by requirements at 66.373 (j)(2) and the Pacific whiting shoreside vessel identification numbers. The

first receiver submits a completed electronic fishticket for every landing that includes whiting no later than 24 hours after the date the fish are received, unless a waiver of this requirement has been granted.

The original purpose of the state paper fishticket program(s) were to record catch for the purposes of imposing and collecting an excise tax on the landed product. As fisheries management matured, the landing data began to be used for fisheries management purposes. Currently, all landing data generated under this system is housed in the PSFMC data base, which is the primary tool for managing commercially caught fish on the West Coast.

Although the current state paper fish ticket data collection system works relatively well, it does not provide the timely data necessary to manage the West Coast Pacific whiting fishery, nor does it take advantage of emerging technology that could improve the efficiency of reporting and record keeping while reducing human error and improving data accuracy.


## **Demand for Electronic Signature Support**

The shore-based Pacific whiting fishery needs to have a catch reporting system in place that: improves NMFS's ability to effectively monitor the Pacific whiting shoreside fishery catch of Pacific whiting and incidentally caught species, including overfished groundfish species; does not result in a species' optimum yield (OY), harvest guideline, allocations, or bycatch limits being exceeded due to reporting time lag or errors; provides for timely reporting of Chinook salmon take as specified in the Endangered Species Act (ESA) Section 7 Biological Opinion for Chinook salmon catch in the Pacific groundfish fishery; and remains consistent with the conservation goals and objectives of the Pacific Coast Groundfish Fishery Management Plan (FMP).

E fishtickets are part of an ongoing process to develop a maximized retention program for the Pacific whiting shoreside fishery. First receivers (1<sup>st</sup> buyers of fish) will provide the computer hardware, software, and internet access necessary to support the NMFS-approved software and provide for e-mail transmissions. The electronic fish tickets are used to collect information similar to information currently required by the States of Washington, Oregon, and California on fish receiving tickets or landing receipts (state fish tickets). The West Coast electronic fishticket will be in addition to the existing state fish ticket requirements, and will not replace any state recordkeeping or reporting requirements.

Electronic reporting without e-signature has been considered. Several jurisdictions have implemented electronic reporting under a conventionally signed agreement "to electronically submit accurate and complete data...". It is unknown whether this model of a single blanket agreement covering electronic reporting for a certain period of time has been tested in court. Along with concerns with its efficacy in the event of litigation there is also concern that the conventional signing agreement model will not provide the same motivation for true and accurate reporting that is provided by an affirmed signature under penalty of law. For these reasons it has been concluded that an e-signature feature is required to make e-fishticket reporting feasible.

## Proposed Electronic Process

Per [50 CFR part 660.303|<http://law.justia.com/us/cfr/title50/50-8.0.1.1.9.html#50:8.0.1.1.9.3.1.3>] operators of Pacific Whiting vessels delivering whiting during the primary season, and buyers of Pacific Whiting, are required to report deliveries on state fish tickets. In addition the buyer submits an electronic fish ticket for that delivery. Included as part of each electronic fish ticket submission are the actual scale weight for each groundfish species as specified by requirements at 66.373 (j)(2)  and the Pacific whiting shoreside vessel identification numbers. The first receiver submits a completed electronic fishticket for every landing that includes whiting no later than 24 hours after the date the fish are received, unless a waiver of this requirement has been granted.

Under the proposed system when the first receiver completes the electronic fishticket submission, the program will present the following signing ceremony:

---

### Terms and Conditions

By typing my name in the indicated fields, I hereby certify that all of the information submitted in, and in support of, this application is true, accurate and complete. I am also agreeing to conduct business electronically with the National Oceanic and Atmospheric Administration in accordance with the **Government Paperwork Elimination Act (GPEA) (P.L. 105-277, 44 U.S.C. 3504 note)**. I understand that transactions and/or signatures in records may not be denied legal effect solely because they are conducted, executed, or prepared in electronic form, and that if a law requires a record or signature to be in writing, an electronic record or signature satisfies that requirement. I further understand that false statements made knowingly and willfully on this submission, including any documents

submitted with or in support of this submission, are punishable by fine and/or imprisonment under the provisions of 16 U.S.C. §1857 and 18 U.S.C. §1001.

 I have read and understand the statement above

---

The first receiver completes an e-signature by typing his/her name and password in the box(s) and pressing the ***Electronically Sign*** button, at which point the e-fishticket program records the e-signature and concludes the data entry session.

## **E-Signature Risk Assessment**

### ***Business Risk in the Permit Context***

Business risk was evaluated using categorization found in FIPS 199, which provides a common framework for expressing information security concerns throughout the federal government. This system has a FIPS 199 security categorization as follows:

- Low confidentiality requirements -- loss of confidentiality would be expected to have a limited adverse effect on organizational operations, assets, or individuals. A breach of confidentiality would damage our relationship with our constituency and could impact our ability to collect accurate data with which to manage fisheries. This could cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced. It could also expose us to litigation and professional disrepute.
- Moderate integrity requirements -- among other things data from this system could be used to establish individual fishing quotas based on historical participation in a fishery. Individual fishing quotas have value, and it is critical to maintain access controls, change tracking, and audit ability. The moderate level is specified to recognize that loss of integrity could result in significant financial harm to individuals.
- Low availability requirements -- a temporary loss of availability would be expected to have a limited adverse effect. Transactions dependent on this

data are not particularly time-sensitive, and business requirements could be met via manual methods during a temporary system outage.

NIST 800-30: Risk Management Guide for Information Technology Systems defines risk as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. The threat and vulnerability identification process that follows is based on NIST 800-30.

### ***Data sensitivity and security***

Information collected pursuant to requirements of the MSA is protected by its confidentiality provisions at § 402 and under its implementing regulations at 50 CFR Part 600 Subpart E, including NOAA Administrative Order (NAO) 216-100. Additional protections of the Privacy Act and FOIA apply to such data as well as those collected under the Halibut Act.

### ***Mitigating controls***

Perhaps the most significant mitigating control is that in commercial fisheries transactions, both parties to the transaction (typically the fisher and the fish processor) are permitted entities and each has some responsibility for accurate and complete record-keeping and reporting. For example; the fisher is required to keep a logbook showing fishing efforts and catch, while the processor is required to report fish purchased. In these transactions it is typical for the parties to the transactions to have opposite and balancing interests, as when a fisher is selling fish to a processor, the fisher wants the amount paid to be high, while the processor wants the amount paid to be low. These multiple sources of information and counter-balanced incentives tend to make deception more difficult to initiate and sustain.

Another mitigating control is that under the authority of the Debt Collection Improvement Act (31 U.S.C. 7701), NMFS would collect Tax Identification Number information from individuals in order to issue, renew, or transfer fishing permits or to make non-permit registrations.

The vessels and processors involved are permitted and therefore have a prior "trusted relationship" with NMFS. In many cases this prior relationship involves confirming vessel ownership with the US Coast Guard, verifying participation in prior fisheries through previously submitted state or federal fish tickets or logbooks, confirmation of business ownership, etc.



### ***Threat and Vulnerability Identification***

<b>Vulnerability</b>	<b>Threat-source</b>	<b>Threat Action</b>	<b>Category of Harm</b>	<b>Likelihood of Occurrence</b>	<b>Impact of Harm</b>	<b>E-signature Cost Benefit Assessment</b>
System unavailability	Error, component failure, or act of God	Power failure, network failure, computer component failure, operator error, software failure, capacity constraint, etc.	Inconvenience, distress or damage to standing or reputation	Moderate: failures will happen, but competently managed systems typically have availability records of 99% or better	Low: for fishery management decision support typical availability is adequate. Even in the event of a systemic failure fishery management decision-making would continue and unavailability would be a short-term inconvenience. Smaller scale failures, for instance a failure that prevents reporting from one processor, would be a minor inconvenience.	N.A. (E-signature has no effect, positive or negative, on this vulnerability) N.A. (E-signature has no effect, positive or negative, on this vulnerability)
System unavailability	Vandalism	Internet security exploit such as denial-of-service attack	Inconvenience, distress or damage to standing or reputation	Low: this is not an high-profile Internet system and should not be a particularly attractive target. Also, if necessary, the system could be hosted in a data center with an incident response capability	Low: even in the event of a systemic failure fishery management decision-making would continue and unavailability would be a short-term inconvenience	N.A.

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
				that could deal with all but the most sophisticated attacks.		
System misuse	System administrator, operator, or other agency user	Abuse of insider knowledge and access for unauthorized use or release of information	Unauthorized release of sensitive information	Low: agency staff have significant incentives to behave appropriately and periodic training in ethics and computer security	Moderate: at worst, a release of personal or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with an expected serious adverse effect on organizational operations.	N.A.
"	"	"	Civil or criminal violations	Low: agency staff have significant incentives to behave appropriately and periodic training in ethics and computer security	Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts	N.A.
System compromise	Vandal	Internet security exploit circumventing security controls	Unauthorized release of sensitive information	Low: agency staff use due diligence to secure systems and reduce vulnerabilities. Also this is not an high-profile Internet system and should not be a particularly attractive	Moderate: at worst, a release of personal or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with an expected serious	N.A.

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
				target. If necessary, the system could be hosted in a data center with an incident response capability that could deal with all but the most sophisticated attacks.	adverse effect on organizational operations.	
"	"	"	Civil or criminal violations	Low: agency staff use due diligence to secure systems and reduce vulnerabilities. Also this is not an high-profile Internet system and should not be a particularly attractive target. If necessary, the system could be hosted in a data center with an incident response capability that could deal with all but the most sophisticated attacks.	Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts	N.A.
Failure to report	Processor or processor in collusion with fisher	Processor fails to report, either through negligence, or with intent to	Harm to agency programs or public interests	Low: permitted parties know the rules and understand the risks of non-compliance	Moderate: most individual trip reports would be inconsequential in overall impact, but	Benefit: failure to report would be detectable quickly, resulting in more responsive

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
		mislead fisheries managers and evade fisheries management controls or enforcement actions			some would be consequential, and any widespread or long-term failure to report would facilitate overfishing.	enforcement and potentially a higher rate of compliance
"	"	"	Civil or criminal violations	Low: permitted parties know the rules and understand the risks of non-compliance	Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts	Benefit: failure to report would be detectable quickly, resulting in more responsive enforcement and potentially a higher rate of compliance
Under-reporting or misreporting catch	Fisher and processor in collusion	Fisher and processor collude to under-report or misreport, to mislead fisheries managers and evade fisheries management controls	Harm to agency programs or public interests	Low: permitted parties have a lot to lose and there are enough checks and balances in the system to discourage fraud	Moderate: at worst, a serious adverse effect to public interests. For example, in a commercial landing the species could be misreported from an overfished species to a less restricted species to evade a fisheries closure action, with potentially significant damage to the	Benefit: e-reporting and e-signature can result in more immediate feedback for detectable errors, and more immediate feedback facilitates more accurate reporting

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
					overfished species, i.e., public interests	
"	"	"	Civil or criminal violations	Low: permitted parties have a lot to lose and there are enough checks and balances in the system to discourage fraud	Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts	Benefit: misreporting problems might be detected quickly, resulting in more responsive enforcement and potentially a higher rate of compliance
Impersonation in e-ticket transactions	Common criminal/identity thieves	Impersonation using stolen identity credentials, to receive full market price for stolen fish	Inconvenience, distress or damage to standing or reputation	Low: e-ticket transactions take place in a context of fish delivery, and the fisher and processor are normally known to each other	Low: someone would be likely to notice and when detected, the impact could be effectively mitigated. The impact would be limited to the parties whose identity and fish have been stolen	No net cost or benefit: inconvenience, distress or damage is not significantly different in electronic transactions than it is in paper transactions
"	"	"	Civil or criminal violations	Low: e-ticket transactions take place in a context of fish delivery, and the fisher and processor are normally known to each other	Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts	Cost: criminal e-signature forgery, falsification or misrepresentation will provide new challenges for enforcement investigation and litigation

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
Impersonation in e-ticket transactions	Competitor	Impersonation using stolen identity credentials, to sell fish without debiting own quota	Inconvenience, distress or damage to standing or reputation	Low: a competitor might have a motive, but is unlikely to have means or opportunity	Low: impersonated parties would be likely to notice and when detected, the impact could be effectively mitigated	No net cost or benefit: inconvenience, distress or damage is not significantly different in electronic transactions than it is in paper transactions
"	"	"	Civil or criminal violations	Low: a competitor might have a motive, but is unlikely to have means or opportunity	Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts	Cost: criminal e-signature forgery, falsification or misrepresentation will provide new challenges for enforcement investigation and litigation
Repudiation to escape accountability	Customer (fisher or processor)	Signer claims "I didn't sign that"	Inconvenience, distress or damage to standing or reputation	Low: in most cases a customer who repudiated an e-ticket document submission could then be prosecuted for fishing or processing without meeting record-keeping and reporting obligations. There will generally be independent evidence	Low: agency might expend effort to resolve, but the distress would be limited and short-term	Cost: despite e-signature's legal standing and agency instructions, there is likely to be a tendency to regard a holographic signature as more significant or more binding. It is likely that the requirement to sign a filing with a

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
"	"	"	Civil or criminal	Low: in most cases a	Moderate: at worst, a	<p>holographic signature has more influence on the signer's behavior with respect to their consideration of what they are submitting, their commitment to reporting the truth, and their expectation of being held accountable. Persons signing with an e-signature are likely to understand that it would be difficult to prove what individual executed the e-signature (because credentials are transferable). This is likely to motivate some people to repudiate their e-signature if they are being held accountable for something signed with an e-signature.</p> <p>Cost: criminal e-</p>

of the fishing or processing activity (follow the fish.)

Vulnerability	Threat-source	Threat Action	Category of Harm	Likelihood of Occurrence	Impact of Harm	E-signature Cost Benefit Assessment
			violations	customer who repudiated an e-ticket document submission could then be prosecuted for fishing or processing without meeting record-keeping and reporting obligations. There will generally be independent evidence of the fishing or processing activity (follow the fish.)	risk of civil or criminal violations that may be subject to enforcement efforts	signature forgery, falsification or misrepresentation will provide new challenges for enforcement investigation and litigation



## E-signature Risk Mitigation

### *Risk Mitigation Analysis Worksheet*

Impact Categories	Significant Probability of Occurrence?	Impact Category	Assurance Level From Table B
Inconvenience, distress or damage to standing or reputation	No	Low	1
Financial loss or agency liability	N/A	N/A	
Agency liability	N/A	N/A	
Harm to agency programs or public interests	No	Moderate	3
Unauthorized release of sensitive information	No	Moderate	3
Personal Safety	N/A	N/A	
Civil or criminal violations	No	Moderate	3

### *Appropriate OMB Assurance Level to Mitigate Business Risk*

Lowest Assurance Level that Mitigates All Impact Categories	Mitigating Controls	Appropriate Assurance Level with Consideration of Mitigating Controls	Proposed E-signature Alternative
Level 3--- ...appropriate for transactions needing high confidence in the asserted identity's accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.	<p>Multiple sources of information, some with counter-balancing incentives.</p> <p>Buyers reporting are permitted and have an ongoing "trusted relationship" with NMFS.</p> <p>E-reporting systems will detect failure to report more quickly, resulting in more responsive enforcement and potentially a higher rate of compliance.</p> <p>E-reporting and e-signature can result in more immediate feedback for detectable errors, and more immediate feedback facilitates more accurate reporting.</p>	<p>Level 2---On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).</p>	NPS-like (NatI NMFS permit system)

## Cost Estimates

The cost of incorporating e-signatures into the existing and proposed WCEFT software application(s) is expected to be relatively minimal in the short-term, and no new funds are required for this implementation. The e-signature requirements include maintenance of a username/password database for buyers and the addition of the terms and conditions language described under the WCEFT Implementation Details page of this document.

While the current e-fishticket capture and submission application is based on the State paper fishtickets, the electronic fishticket system is only mandatory in the Federally managed Pacific whiting fishery. While it is difficult at this point to predict what costs may be incurred in the States fishticket systems as they further embrace the e-ticket technology the expectation is that costs of adherence to the described e-signature protocols will be manageable.

## Benefits Statement

Most of the benefits from enabling e-signatures gained by NMFS and NMFS' end users are qualitative in nature. In large part, the benefits to e-signatures accrue from making it easier for end users to report or file electronically thereby minimizing paper reporting and filing of information. Some of the following benefits apply generally to the use of e-signatures in the shift from paper to electronic filing and some are specific to using e-signatures to improve the West Coast Fishticket application.

- ***Reduced cycle time for submitting catch data.*** The reduction in cycle time is expected to be dramatic. Under the previous paper-based system lag times from vessel landing until catch data was available for analysis were typically measured in months. Based on the fish ticket pilot and experience from other jurisdictions lag time will be reduced to a few days. Pacific whiting is an overly constrained fishery because some bycatch species which have historically been a part of this fishery have been determined to be over-fished stocks. Under the MSRA, NMFS is committed to ending overfishing, establishing recovery plans for overfished stocks, and ultimately executing the recovery plans to restore the viability of the overfished stocks. Timely reporting will reduce the chance of over fishing because fisheries managers will have an opportunity to monitor the fishery and intervene if necessary.

- ***Reduced reporting burden.*** Compared to traditional paper fish ticket reporting, the electronic reporting process should be more convenient and take less time. Many buyers already use technology to track their purchases. This electronic reporting alternative may allow those buyers to leverage their investment in technology to also address their record keeping and reporting obligations. The potential also exists for independent software vendors to provide integration with business systems to provide some unspecified benefit to the buyer.
- ***Improved efficiencies due to more accurate and consistent data.*** Having the fish ticket collected electronically, with comprehensive edit-checks for valid or reasonable data, rigorously controlled data codes, and immediate feedback on detection of questionable data, will ensure cleaner data. With previous paper-based reporting dealer/processor reporting was frequently inconsistent. For example, catch species could be identified by ambiguous common names. A fully electronic reporting system will ensure consistency and improve accuracy, eliminating much of the labor of edit/correction cycles and improving analytical accuracy.
- ***Increase in employee productivity.*** Receiving the data electronically obviates the need to key in fish ticket data by the regulatory agencies (because the buyers are keying it in) to be used for analysis. Also, edit checks and immediate feedback on detectable errors make for more efficient data entry.
- ***Greater information benefits to the public.*** Because this is an overly constrained fishery due to overfished stocks, the fishing public is likely to have a high degree of interest in this data. Electronic data capture will provide potential for in-season analysis, and possibly modeling differing fishing behaviors.

## Cost Benefits Analysis

The benefits from enabling e-signatures gained by NMFS and NMFS' end users are qualitative in nature. Benefits accrue from making it easier for end users to report or file electronically thereby minimizing paper reporting and filing of information. Some of the following benefits apply generally to the shift from paper to electronic filing and some are specific to using e-signatures to improve the West Coast E-fishticket application.

- ***Reduced cycle time for submitting catch data will contribute to additional opportunity to access the Pacific whiting TAC.*** Under the previous paper-based system lag times from vessel landing until catch

data was available for analysis were typically measured in months. Under the MSRA NMFS is committed to ending overfishing, establishing recovery plans for overfished stocks, and ultimately executing the recovery plans to restore the viability of the overfished stocks. Over-harvest of bycatch species can result in closure of the Pacific whiting fishery before the Pacific whiting total-allowable-catch (TAC) has been reached. Timely catch reporting will allow the Pacific whiting fishery to continue, reducing the chance of over fishing to acceptably low levels.

- **Reduced reporting burden.** Compared to traditional paper fish ticket reporting, the electronic reporting process will be more convenient and take less time.
- **Improved efficiencies due to more accurate and consistent data.** Having the fish ticket collected electronically, with comprehensive edit-checks for valid or reasonable data, rigorously controlled data codes, and immediate feedback on detection of questionable data, will ensure cleaner data. There will be a reduction in data correction overhead for both NMFS and seafood processors.
- **Increase in employee productivity.** Receiving the data electronically obviates the need to key in fish ticket data by the regulatory agencies (because the buyers are keying it in). Also, edit checks and immediate feedback on detectable errors make for more efficient data entry.
- **Greater information benefits to the public.** Because this is an overly constrained fishery due to overfished stocks, the fishing public is likely to have a high degree of interest in this data. Electronic data capture will provide potential for in-season analysis, and possibly modeling differing fishing behaviors.

## Implementation Details

The National Marine Fisheries Service Policy Directive 32-110, "Use and Implementation of Electronic Signatures" outlines the following requirements for an approved electronic signature system:

1. Technical non-repudiation services
2. Legally binding the electronic transaction to an entity
3. Providing chain of custody audit trails
4. Providing an electronic receipt or acknowledgment of a successful submission
5. Collecting only necessary information in the electronic signature authentication process
6. Create a long-term retention and access policy

## 7. Periodic review and re-evaluation of the electronic signature process

This sections documents design details that address these requirements.

### ***Binding the Transaction to an Entity and Non-repudiation***

Requirements 1 and 2 above are addressed in the design of three component parts of the system:

- identity assertion, person proofing, and registration
- terms and conditions and signing ceremony
- document binding and document integrity

The WCEFT E-Signature Risk Assessment has concluded that OMB Assurance Level 2 (confidence exists in the asserted identity) was appropriate for the West Coast E-fishticket. This was a considered decision justified by low likelihood of occurrence, low and moderate impact of harm, and multiple and strong mitigating controls, including: multiple and sometimes counter-balancing sources of information; permitted entities with an ongoing trusted relationship with NMFS; faster detection of reporting omissions; and immediate feedback for detectable errors. Note that the identity is established from association with an existing processing permit, and not through the registration to submit fish tickets electronically.

### ***Recognition Terms and Conditions***

The proposed identity assertion, person proofing, and registration starts with a permit holder completing an electronic fish ticket agreement, establishing a linkage between the processing permit, the permit holder, and the processor employee(s) who is/are authorized to submit electronic fish tickets for that permit. Information obtained in the agreement includes:

- Name of Applicant
- Date of Application
- Name of Processor/Buyer
- Operation Name
- Operation Type
- Processor Code
- Federal Permit Number
- Buyer Registration Number
- City and State
- Business Telephone Number
- Business Facsimile Number
- Business Email Address
- Requested UserID

- o User is limited to viewing and updating only reports that they themselves created.
- o User can view and update all reports for authorized operation.

Terms and conditions presented during registration and the signing ceremony contribute to binding the transaction to the entity and non-repudiation. Terms and conditions specified during the registration process include the following statement on the paper form just above the required signature block:

By signing this document under penalty of perjury, you affirm that all information submitted is true and correct to the best of your knowledge, and that you have read and understand this agreement and consent to the terms and conditions described herein.

User Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

By signing this document under penalty of perjury, you affirm that all information submitted is true and correct to the best of your knowledge, and you hereby designate the User identified above as an agent of your business for the purpose of submitting accurate fishery landing and production data on behalf of your business.

Manager/Owner Signature: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Manager/Owner Name (Print) \_\_\_\_\_

***Signing Ceremony Terms and Conditions***

Terms and conditions presented during the signing ceremony, where when the processor has entered fish ticket data into the program and is submitting the data to NMFS, includes the statement below just above the required signature block:

Under the proposed system, when the first receiver completes the electronic fishticket submission, the program will present the following signing ceremony:

By typing my name in the indicated fields, I hereby certify that all of the information submitted in, and in support of, this fish ticket is true, accurate and complete. I am also agreeing to conduct business electronically with the National

Oceanic and Atmospheric Administration in accordance with the **Government Paperwork Elimination Act (GPEA) (P.L. 105-277, 44 U.S.C. 3504 note)**. I understand that transactions and/or signatures in records may not be denied legal effect solely because they are conducted, executed, or prepared in electronic form, and that if a law requires a record or signature to be in writing, an electronic record or signature satisfies that requirement. I further understand that false statements made knowingly and willfully on this submission are punishable by fine and/or imprisonment under the provisions of 16 U.S.C. §1857 and 18 U.S.C. §1001.

The signer must make a willful act to demonstrate that they have read and agreed with the statement above. They must place a check mark in a check box that is labeled "I have read and understand the statement above." In addition to placing a check mark in the check box, the applicant must also type their name and their password to complete the electronic signing ceremony. Attempting to proceed to the next step of the electronic transaction without completing the above steps will cause the system to display a message instructing the applicant that they must read the terms and conditions statement, enter their name, and their password before their information will be accepted.

Technically the transaction data is bound to entity identity data by the signer's name captured in the electronic signature and also specified in the registration data, and by a shared identifier (permit number) in the registration data (electronic fish ticket agreement), the processor permit database, and the e-ticket submission.

No authentication token and protocol issues are involved in this non-repudiation. Technical controls for document integrity and audit trails contribute to binding the transaction to the entity and non-repudiation, but those controls are more appropriately discussed in the next section.

### ***Providing Chain of Custody Audit Trails***

NMFS policy directive 32-110 specifies "...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."

The proposed design implements the following audit trail controls for submission of e-tickets via web services:

1. Upon completion of the signing ceremony a web service will accept an XML document containing Fish Ticket information from a dealer.
2. The service will authenticate the dealer, check the information for errors, and return error codes and descriptions if necessary. If there are no errors, the service will insert the fish ticket data into the main database.
3. Once the data has been inserted into the main database the web service will return the receipt date and time, and a unique ticket reference number for each ticket.
4. In the event the new ticket information contains edits of existing fishtickets the system will move the old fishticket data into an historical database and insert the new fishticket data in the main database. A version number will be assigned to these transactions to allow for later analyses.
5. The unique reference number assigned to each ticket will be used to help minimize errors and discrepancies between data on a printed fishticket and data submitted to the web services. Until the receipt at the buyers end of the unique reference number, indicating that the data has been successfully submitted, all printed fishticket will have a watermark indicating they are 'Draft' or 'Unsubmitted'. Once the reference number is received the watermark will switch to 'Final' or 'Submitted'. In the event the buyer later edits a fishticket, the watermark will revert back to its 'Draft' state.
6. The web service will log audit activity into a data table for subsequent monitoring and diagnostic purposes. These audit trail data items will be written to audit trail tables by the email interface application using a database account which has insert privileges to the database but does not have update or delete privileges. (And update and delete privileges on the audit trail tables will be carefully controlled by the database administrator.)

### ***Providing an Electronic Receipt or Acknowledgment of a Successful Submission***

After the data import program has interpreted (or attempted to interpret) the submitted e-fishticket data, the data import program writes a receipt file. The receipt will consist of:

1. Assuming that the data import was successful, or at least successful enough that the e-ticket's permit could be ascertained, the receipt file will also be emailed directly by the data import program to the address of record for the permit holder



2. If the receipt file cannot be emailed directly to the address of record for the permit holder the operator executing the data import program is notified so that they can take steps to inform the submitter

### ***Collecting Only Necessary Information in the Electronic Signature Authentication Process***

Since the proposed system relies heavily on mitigating controls, no additional information is collected specifically for the e-signature process.

### ***Create a Long-Term Retention and Access Policy***

Retention and access policies already exist for this logbook data under NOAA file series 1505-11, Catch Statistics Files. This section discusses the special records management considerations which arise due to incorporation of an electronic signature.

NMFS policy directive 32-110 specifies:

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. 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).... 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.... The original document along with its audit trail should not be deleted from the agency's records.... 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.

NARA's Records Management Guidance for Agencies Implementing Electronic Signature Technologies section 4.1 establishes characteristics of trustworthy records in terms of reliability, authenticity, integrity, and usability. NARA advises that these characteristics are a matter of degree. Transactions that are critical to the agency business needs may need a greater assurance level that they are reliable, authentic, maintain integrity and are usable than transactions of less critical importance.

- Reliability is established by capturing the content and context of the transaction and recording that content and context in database tables

through a mechanism which allows inserts but which disallows updates or deletes.

- Authenticity is established by checking ticket-related data elements against permit-related data elements, and adding the results of that validity check as a part of the context of the ticket record, stored in the database through a mechanism which allows inserts but which disallows updates or deletes.
- Integrity is established by the database mechanism which allows database inserts but which disallows updates or deletes.
- Usability is established by the linkages among the permit records and the ticket records and the e-signature receipts. Using these linkages it is possible to connect the signer and the time of the signature with the details of the signed transaction.

The guidance document section 4.2 states "for a record to remain reliable, authentic, with its integrity maintained, and usable for as long as the record is needed, it is necessary to preserve its content, context, and sometimes its structure."

The proposed e-signature enabled system preserves content (ticket data), context (audit trail data and permit data), and structure (links among related tables) by maintaining a historical record of all changes to its database tables. Updates to the data result in inserts into history tables, leaving the prior values intact in the history records. Tickets will have version numbers to help track historical changes. Deletions of data result in insertions into history tables that indicate that the prior data is no longer valid. But in all cases, the history records allow reconstruction of a point-in-time view of the data.

The guidance document section 4.3 describes two approaches to ensuring the trustworthiness of electronically-signed records over time. This e-signature implementation will maintain documentation of record validity (including trust verification records, or audit trails) gathered at or near the time of record signing (the first approach specified).

The guidance document section 4.4 describes steps to ensure trustworthy electronically-signed records as follows:

- ***Create and maintain documentation of the systems used to create the records that contain electronic signatures.***

The West Coast E-fishticket system will be thoroughly documented with

particular attention to e-signature aspects and audit trails that establish the trustworthiness of the e-signature.

- Ensure that the records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.

The fish ticket data, and the audit trail data supporting the trustworthiness of the e-signature, are implemented with the history mechanism described above to protect the records from unauthorized alteration or deletion. Furthermore the database is secured according to industry norms for important government data, including regular offsite backup and periodic permanent archiving of backups.

- ***Implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain adequate written documentation of those procedures.***

Standard operating procedures will be implemented for the creation, use and management of these records.

- ***Create and maintain records according to these documented standard operating procedures.***

The new standard operating procedures will be diligently followed.

- 
- ***Obtain official disposition authorities from NARA for both the records that contain electronic signatures and for the associated records which are necessary for trustworthy records.***

Electronic data submission adds audit trail data to the fish ticket records already covered under file series 1505-11 (Catch Statistics Files), and, establishes a link to an associated file series 1504-11 (Fishing Vessel Permit Files). File series 1505-11 is sufficiently broad to accommodate the addition of audit trail data. The existing retention and access policies do not need to be revised, as the new audit trail data elements are component parts of the same database which stores the fish ticket records. File series 1504-11 provides disposition authority for the associated permit records which are used to establish confidence in the identity of the party applying an e-signature, and that file series needs no changes as a result of this new association.

Other considerations raised in the guidance document include:

- ***5.1 What new records may be created by electronic signature technology? and 5.2 How do agencies determine which of these electronic signature records to retain?***

The e-signature proposed does not create new types of records. It does add new data elements to existing records and create new associations between existing file series, but in this case the file series involved have been reviewed and no changes to existing retention and access policies are necessary.

- ***5.3 Transferring electronic signature record material from contractors to agencies.***

Not applicable.

- ***5.4 When must an agency modify its records schedule to cover electronic signature records?***

No modification to the record schedule is necessary, as new records are not created by this e-signature, the e-signature itself requires no change to retention periods, and the e-signature does not significantly change the character of the record.

- ***5.5 Special considerations relating to long-term, electronically-signed records that preserve legal rights.***

The e-signature proposed does not depend on technologies or formats which are likely to become obsolete. The e-signature, its associated audit trails, and the receipt are all stored as human readable text in relational database tables.

- ***5.6 NARA requirements for permanent, electronically-signed records.***

These are not permanent records, but, note that the receipt, which is stored as part of the e-signature, does contain the printed name of the signer as well as the date when the signature was executed.

### ***Periodic Review and Re-Evaluation of the Electronic Signature Process***

The proposed e-signature system should be reviewed annually for several years, as this technology is unfamiliar to the agency and our customers and we expect to learn from experience.

### ***Implementation Plan Outline***

The e-fishticket was developed as a pilot project beginning in 2007. Since that time, it has been used in the Pacific whiting fishery. It is currently being evaluated by Washington and Oregon for broader adoption. The pilot e-fishticket did not include an e-signature, but, technically, e-signature requires only minor enhancements to the existing system.

<b>Task/Milestone</b>	<b>Due Date</b>	<b>Staffing</b>
develop specifications for required changes	complete	PSMFC
develop test plan	complete	PSMFC
implement changes	fall 2009	PSMFC
execute test plan and correct defects	winter 2009	PSMFC
production readiness review	May 2010	PSMFC
go live	May 2010	PSMFC