Global Record

HLR5 Users: Detailed Requirements

11 June 2010

Version 0.2

Dan Martin

FINNZ
Level 6
135 Victoria Street
Wellington
New Zealand

PO Box 24441
Manners St
Wellington

Ph 04 460 9500
Fax 04 460 9590

www.finnz.com

Table of Contents

Document Version History

Version No.	Date	Author	Summary of changes
0.1	5 May 2010	Dan Martin	Initial draft
0.2	19 May 2010	Dan Martin	Updated to simplify processes
0.3	2 June 2010	Dan Martin	Updates after feedback from Shaun (FAO project manager)

Document Information

This document is stored in: \\Filer01\finnz\FINNZ Public\Global Record\Detailed Requirements\Global Record DR5 Users.docx

1 Introduction

1.1 Document purpose

The purpose of this detailed requirements document is to further define the expectations of the GR in respect to the high level requirement for Users. The detailed requirements identified identify the functionality that is required to support this HLR and a clear indication of what must be developed as part of the GR.

This detailed requirements document also outlines a number of suggested business processes to aid the understanding of the requirement and to improve the overall design of this area.

1.2 Intended audience

The audience for this document includes:

- *FAO*
- *Global record stakeholders*

1.3 Background

The need for a Comprehensive Global Record of Fishing Vessels was acknowledged as far back as 2002 in the implementation guidelines for the International Plan of Action to Prevent Deter and Eliminate Illegal, Unreported and Unregulated Fishing (IPOA-IUU) where it was acknowledged that the lack of such a tool produced a situation that undoubtedly creates opportunities for IUU vessels to escape detection. Subsequently, in the Rome Declaration on IUU Fishing, ministers called for the development of a comprehensive global record of fishing vessels within FAO, including refrigerated transport vessels and supply vessels. Following this, Proposal 2 of the Final Report “Closing the Net” produced by the High Seas Task Force (HSTF) promotes the establishment of a global information system on high seas fishing vessels. The purpose of this system is to combat the lack of access to transparent and authoritative information about the ownership, control and movements of fishing vessels. Provision of this information to Fisheries Management Organisations, Port States, Fisheries Enforcement and MCS authorities and other interested parties will enable actions to be undertaken to restrict and expose Illegal, Unregulated and Unreported (IUU) fishing activity.

It is widely recognized that one of the significant barriers to eliminating IUU fishing is a lack of transparency and traceability in the global fishing sector. States implement individual measures without the benefit of any sort of global information picture and there is no single source where useful and relevant information can be collated, stored and displayed. One of the major enablers of IUU fishing is the lack of information about the global fishing fleet or the wide range of information associated with vessel activity. To make matters worse, fishing vessels frequently change flag, ownership, registration, and fishing authorizations, enabling them to act with impunity if they choose.

The Global Record, which is being planned as an integrated global data base, offers a solution as it is intended to fill this information void. It will make available the essential information to enhance the effectiveness of regional and national monitoring, control and surveillance (MCS) tools and in particular, to support vessel inspection and surveillance programs, investigations, traceability initiatives and resource prioritization decisions, through the effective sharing of information–something that is not currently possible. The development of a GR would improve transparency and traceability of vessels, products, owners, operators, flags, authorisations and registration. It would facilitate risk assessment for industry, RFMOs and Governments and improve decision making including on fleet capacity, size and structure, management, safety, pollution, security and statistics and more.

The importance of the GR is underscored by new and growing market demands for ecolabels and other forms of product certification which require product traceability. Market forces and incentives could stimulate compliance by countries to provide information to the GR prior to any mandatory legal requirement being imposed.

The GR would support existing binding and non binding instruments to prevent, deter and eliminate IUU fishing and increase the effectiveness of port state measures and MCS activities.

This document seeks to define at a high level the requirements of the GR that will allow it to meet these goals.

1.4 Definitions and Acronyms

FAO	The Food and Agriculture Organisation of the United Nations
GR	Global Record
UVI	Unique Vessel Identifier
MCS	Monitoring Control and Surveillance
RFMO	Regional Fisheries Management Organisation
UNGA	United Nations General Assembly
FAO	Food and Agriculture Organisation of the UN
NGO	Non-governmental organisation
COFI	Committee on Fisheries
UN	United Nations
FishVIS	High Seas Fishing Vessel Information System
FINNZ	FishServe Innovations New Zealand Limited
HSTF	High Seas Task Force
MU	High Seas Fishing Vessel Information System Management Unit
TU	High Seas Fishing Vessel Information System Technical Unit
IUU	Illegal, Unregulated and Unreported Fishing Activity
IHS Fairplay	IHS Fairplay
CFR	Community Fleet Register
EMSA	European Maritime Safety Agency

2 HLR5: Users

2.1 Detailed Requirements

Requirement No.:	5.1.0 Account Creation / Registration / Activation
Requirement:	The system will allow users from contributing organisations and the general public to be created within the GR. Where the user is a public user (i.e. not associated with a contributing organisation) the same process with be followed but the Organisation is set to public The following information will be required to create a public or contributing organisational user within the GR o First Name o Surname o Email Address o Contact Phone Number o Organisation * o Role * o Reason for access *
Business Rules	o * indicates populated from a system generated list o Email Addresses must be unique. o User name is set to the email address o Temporary passwords created must conform to the password strength policy and are valid for 24 hours. o All required information must be provided before a user can be created. o Users created for public users, the user will enter the organisation; otherwise the system will set this value for Non-GR Management users or allow GR users to select the organisation from a system generated list o Only users for an organisation or from the GR management unit may create other users for that same organisation o If the user account is being created by a person not already logged onto the website, then Organisation and Role are set to Public

Suggested Process:	1. Admin or user enters the required account information, from within the GR or GR registration form. 2. The user information is submitted at which time the application will: a. Generate a temporary password and activation code with an expiry period of 24 hours; and b. Send an activation email to the user containing 1. A hyperlink containing the encrypted user activation code; and 2. The users' temporary password. 3. The user will click the link contained within the email which will navigate them to the GR where they will be required to enter: a. Their temporary password. 4. Upon successful validation of the required activation information, the user will be: a. Prompted to enter a new password; and 5. The activation process is now complete. All session information will be cleared, the user logged out and the user redirected to the login page.
Rationale:	Creating user accounts to control access to the GR is crucial in repudiating any actions performed or modifications made within the GR. Maintaining a user base also enables usage forecasting and potential scaling of the system to fulfil future capacity requirements.
Business Value:	Critical
Related Req's:	5.14
Assumptions:	1 email address will not be linked to more than 1 user

Requirement No.:	**5.2.0 User Login**
Requirement:	The system will enforce a strict user access control to vessel related screens within the GR, with a central point for positive user authentication and identification. The system will provide the facility for registered users to enter their credentials to gain access to restricted areas and functionality within the GR to the extent that their access privileges permit. The login facility with be provided over a secure connection over HTTPS (port 443) to ensure the information is only visible to the end points of the connection.
Business Rules:	○ The system must ensure any error messages returned are generic enough to prohibited malicious users from harvesting valid user credentials from the GR. e.g. if a user name is correct and the password is not, the message should state that either the username or password is incorrect ○ If a user attempts to access the login functionality via unsecured HTTTP (port 80) the system should redirect them to a secure connection over HTTPS (port 443).
Rationale:	All users' actions and data modifications within the GR are required to be non-repudiable. To enable auditing and to ensure only authorised users are granted access to their respective areas a comprehensive user login mechanism is required.
Business Value:	Critical

Related Req's:	
Assumptions:	All clients connecting to the GR will be able to connect over HTTPS. All non HTTPS connections to secure areas will be refused.

Requirement No.:	**5.3.0 User Authentication**
Requirement:	The system will follow a comprehensive positive identification of the logged in user, upon every server request where security restrictions are implemented. The authentication mechanism provided by the system must only be available using a secure connection over HTTPS (port 443) to ensure users' credentials are only visible to the end points of the connection.
Business Rules:	○ Only upon successful user authentication should the system allow access to any restricted areas.
Suggested Process:	1. The user attempts to access a restricted area, or attempts to start a process which requires positive identity or role permission authentication. 2. The encrypted GUID supplied is accessed, decrypted and validated for the particular session and user. 3. The application will then either: a. Throw an exception where failed decryption or failed GUID validation occurs, and terminate the authentication process. b. Retrieve and evaluate the users' associated role permissions for the requested resource or operation. 4. The application will then either: c. Grant access for the requested resource or operation d. Throw a custom "Insufficient Permission Error" exception
Rationale:	Users should only be granted access to view information that is confidential to an unauthorised user. They should therefore be identifiable and have access only to areas for which they have been authenticated and authorised to access.
Business Value:	Critical
Related Req's:	
Assumptions:	All clients connecting to the GR will be able to connect over HTTPS. All non HTTPS connections to secure areas will be refused.

Requirement No.:	**5.4.0 User Account Suspension**
Requirement:	The system will enforce a strict login policy to prevent unauthorised / malicious users to gain access to the GR. The system must automate the task of locking and suspending accounts within the GR. The system must provide the facility for users' to complete an automated account re-activation. The system must provide the ability for users to perform manual account re-activation.
Business Rules:	○ 3 failed attempts to log in with a valid User Name will result in the users account being suspended for 30 minutes and automatically re-activate itself after this time.

Rationale:	Users should only be granted access to view information that is confidential to an unauthorised user once they have successfully verified their identity. They should therefore be identifiable and have access only to areas for which they have been authenticated and authorised to access. The ability to prevent repetitive or structured attacks is required to ensure only users with the correct identity information can access the GR.
Business Value:	High
Related Req's:	
Assumptions:	All clients connecting to the GR will be able to connect over HTTPS. All non HTTPS connections to secure areas will be refused.

Requirement No.:	**5.5.0 Manual Account Re-Activation**
Requirement:	The system will enforce a strict login policy to prevent unauthorised / malicious users to gain access to the GR. The system must provide the facility for group administrators to perform manual account re-activation if one of their users' accounts becomes suspended.
Business Rules:	○ If a users account is suspended, a GR Management unit may unsuspended the account
Rationale:	The users who have the ability to perform tasks other than basic searching potentially have the ability to bring the GR into disrepute. Therefore, any account which has this ability should include a manual identity verification process before allowing them to re-activate their account.
Business Value:	High
Related Req's:	
Assumptions:	

Requirement No.:	**5.6.0 Password Expiry**
Requirement:	The system will enforce a strict login policy to prevent unauthorised / malicious users to gain access to the GR. The system must enforce a strong password policy to ensure passwords are changed at regular intervals to further prevent the ability to brute force passwords over long periods.
Business Rules:	○ When the password has been used for the specified period (e.g. 6 months), the next time the user logs in, they are required to change their password.
Suggested Process:	1. The user successfully logs in to the application. 2. The application identifies the current password's time span has exceeded the period. 3. The application redirects the user, and requires the user to enter: a. Their new password twice to ensure accuracy. 4. The user clicks update. At which time the application: b. Sends a password change email notifying the user they have successfully changed their password. 5. The user is redirected to the first page displayed to user through the normal log in process

Rationale:	User password strength assessments indicate users rarely change their password unless forced to do so. Regularly changing a user's password further reduces the ability for malicious users to brute force attack a users' account over a long period of time.
Business Value:	Medium
Related Req's:	
Assumptions:	

Requirement No.:	**5.7.0 Password Reset**
Requirement:	The system will enforce a strict login policy to prevent unauthorised / malicious users to gain access to the GR. The system must provide an automated facility for users' to reset their password.
Business Rules:	○ A valid username must be provided
Suggested Process:	1. The user clicks the "Forgotten Password" hyperlink. 2. The application requests the user enter: a. Their email address. 3. The user enters their email address and other requested information. 4. The user enters the value seen or heard within an accessibility friendly CAPTCHA control. 5. The user clicks 'Reset Password' at which time the application will either: a. Validate the email address provided. b. Return a generic "Password will be sent if valid details were entered" message for all incorrect password reset attempts, and log all available security audit information.
Rationale:	Different users may access the GR at different intervals, the likelihood of a user forgetting their password is likely. Therefore the GR must provide the ability for users to reset their password to allow them to continue to use the GR.
Business Value:	Critical
Related Req's:	
Assumptions:	

Requirement No.:	**5.8.0 Credential Storage**
Requirement:	The system must store all user credential information (passwords, historical passwords, secret question & answers etc), ○ Securely ○ In such a manner as to ensure the credential information cannot be retrieved, decrypted or ascertained. This also includes direct viewing access to the data stored in the database.
Business Rules:	○ All stored information used in verifying a users' identity must be one way salted and hashed to ensure credential harvesting is impossible.

Suggested Process:	1. Having the application generate strong temporary passwords, using a suitable complex pseudo random password generator. 2. Temporary passwords will only ever be valid for a maximum period of 24 hours. 3. Temporary passwords assigned will be required to be changed, upon first login by the user. 4. Passwords will be one-way hashed and stored within the database. 5. All historical passwords will be one-way hashed and stored within the database.
Rationale:	User information not classed as critical to the identification of a user with the GR may still be used in engineered attacks such as resetting user passwords and performing automated account re-activations if this information is harvested from the application. All additional information should only be known by the user.
Business Value:	Critical
Related Req's:	
Assumptions:	

Requirement No.:	**5.9.0 Credential Recycling**
Requirement:	The system must store all historical user password credential information to prevent re-use of previous passwords.
Business Rules:	○ The system should prevent the user changing their password to a password they have previously used.
Suggested Process:	1. The user clicks the "Change Password" hyperlink. 2. The application requests the user enter their a. Current password. b. Their new password twice to ensure accuracy. 3. The user clicks update. 4. The application will then either a. Send an email to the user notifying them they have changed their password. b. Inform the user, their password has not been changed due to either: i. Their password not conforming to the password strength policy. ii. They are re-using a historical password. 5. The password update process is now complete. All session information will be cleared, the user logged out and the user redirected to the login page.
Rationale:	A strong credential policy is required to prevent users from re-using passwords they have used in the past. Further reducing the risk of a brute force attack of a users' account.
Business Value:	Low
Related Req's:	
Assumptions:	

Requirement No.:	5.10.0 Idle Account Suspension
Requirement:	The system must restrict access to accounts which have remained inactive to ensure repetitive attacks are not performed against accounts to which there are no valid user.
Business Rules:	○ Any users' account that has had a period of inactivity longer than 6 months should be suspended. ○ Any suspended account due to inactivity should be able to be re-activated.
Suggested Process:	1. The user does not log in to the application for a period longer than 6 months. 2. The user successfully logs in to the application. 3. The application identifies the account has been idle for longer than 6 months, at which time the application: a. Redirects the user informing them why their account has been suspended. b. Sends an email to the user notifying them their account has been suspended and the steps required to have their account automatically re-activated. 4. The user will then be able to perform a Password rest process 5. The idle account suspension process is now complete. All session information will be cleared, the user logged out and the user redirected to the login page.
Rationale:	Users who no longer use the GR are vulnerable to long-term engineered and brute force attacks due as they may change employment or email address. Preventing any notification emails being sent, alerting them to the fact their account has been attacked.
Business Value:	Low
Related Req's:	
Assumptions:	Active users will log in at least once every 6 months.

Requirement No.:	5.11.0 Password Change
Requirement:	The system must allow users to change their password on an ad-hoc basis.
Business Rules:	○ At anytime, a user must be able to update their password via the GR website.
Suggested Process:	1. The user clicks the "Change Password" hyperlink. 2. The application requests the user enter their a. Current password. b. Their new password twice to ensure accuracy. 3. The user clicks update. 4. The application will then either a. Send an email to the user notifying them they have changed their password. b. Inform the user, their password has not been changed due to either: i. Their password not conforming to the password strength policy. ii. They are re-using a historical password. 5. The password update process is now complete. All session information will be cleared, the user logged out and the user redirected to the login page.
Rationale:	Users must be able to change their password to prevent repetitive engineered and brute force attacks against their user account.
Business Value:	Critical

Related Req's:	
Assumptions:	Active users will log in at least once every 6 months.

Requirement No.:	**5.12.0 Account Details Update**
Requirement:	The system must allow users to change their account details on an ad-hoc basis.
Business Rules:	○ At anytime, a user must be able to update their details via the GR website. ○ A user should not be able to change their email address or user name to a value that already is in use by another GR user.
Suggested Process:	1. The user successfully logs in to the application. 2. The user clicks the "Account Details" hyperlink. 3. The user updates their associated account information. 4. The user clicks "Save". 5. The application sends an email notification confirming they have updated their account information. NB: In the case of an email address change the application will i. Send an email to the new specified email address with a hyperlink containing an encrypted access code which the user must click to confirm ownership and that the new email address is valid. ii. Send an email to the old email address informing the email address associated with the user account has been changed.
Rationale:	Users must be able to change their information to allow positive identification of the individual who is accessing the account.
Business Value:	Critical
Related Req's:	
Assumptions:	Active users will log in at least once every 6 months.

Requirement No.:	**5.13.0 Account Removal**
Requirement:	The system must allow users to remove their account.
Business Rules:	○ At anytime, a user must be able to remove their account and prevent further access via the account to the GR.
Suggested Process:	1. The user successfully logs into the GR. 2. The user clicks the "Account Details" hyperlink. 3. The user selects "Remove Account" 4. The application confirms the process and implications to the user. 5. The user confirms the account removal process, at which time the application: a. Archives any relevant information. b. Sends an email to the user, notifying them of the removal of their account. c. Sends an email to the users group administrator (if applicable) notifying them of the removal of the user account.
Rationale:	Due to privacy and legal concerns, users must be able to permanently remove their account and access to the GR.
Business Value:	Critical
Related Req's:	

Assumptions:	

Requirement No.:	**5.14.0 User Roles**
Requirement:	The system is required to provide different data views and functionality depending on what role any particular user is associated with. The system is also required to allow users within any particular role group (other than the public role group) who belong to a particular organisation to administer additional users in the same organisation and role group.
Business Rules:	The following role types describe the associated functionality each role group can perform within the GR 1. Non-registered user a. Can register via the website to become a user – Public Viewer only 2. Public a. Viewer The general public's ability to log in and search the GR • Search and view functions (note: the full extent of the data to be available has yet to be confirmed) • Level of search and returned data to be confirmed – possible to have a reduced search and data provision strategy for non affiliated users 3. Contributing organisation a. Viewer • Advanced search, view and export data functions (note: full extent of functions has yet to be confirmed) • Ability to view all information related to vessel • Ability to upload photos • Create users for the same organisation • Ability to upload files 4. GR management unit a. GR User • Advanced search, view and export functions • Ability to view all information related to vessel • Ability to upload photos • Run any batch processes • Process data load errors • Create users for any organisation • Ability to upload files
Rationale:	The GR user base is required to be self maintaining. This requires administrators of groups to maintain the user base and their associated role types.

Business Value:	Critical
Related Req's:	
Assumptions:	These roles are not confirmed but have been developed to provide a brief on what may be required.

Requirement No.:	**5.15.0 Additional Features**
Requirement:	The system is also required to provide the following functionality o Providing the user the ability to view a login history, or the last date time they were logged into the application. o Implement real-time monitoring and notification of security, audit and error logs for potential intrusion attempts o Ensuring the website has a valid SSL certificate, and only allows secure connections on port 443. o Enforcing a strong password policy, forcing the user to choose at least one lower case alpha value, one upper case alpha value, at least one numeric value and requiring a password length no shorter than 8 characters.
Business Rules:	
Suggested Process:	
Rationale:	
Business Value:	Critical
Related Req's:	
Assumptions:	