INTERNATIONAL
MARITIME
ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Circ.1603
26 June 2019

GUIDANCE FOR THE ELECTRONIC TRANSFER OF INFORMATION INTO AND FROM THE MARITIME SECURITY MODULE OF GISIS

Purpose

1 This Guidance provides relevant procedures and conditions for SOLAS Contracting Governments willing to implement an electronic data transfer mechanism for communication of information into the Maritime Security module of the Global Integrated Shipping Information System (GISIS), directly from their national databases. The implementation of such a mechanism is optional and can coexist with the existing manual updating process.

2 Information in the Maritime Security module of GISIS has so far been updated by nominated points of contact for security-related matters designated by SOLAS Contracting Governments by logging on to the GISIS website. The information is updated periodically according to the requirements of SOLAS regulation XI-2.13 on communication of information. Relevant guidance related to the appointment of national focal points is provided in Circular Letter No.3338.

Functional overview

3 Information in the Maritime Security module is presented under four different sections:

.1 national points of contact;

.2 organizational contacts;

.3 port facilities; and

.4 security arrangements.

4 Information on national points of contact for maritime security should continue to be communicated to the Organization in accordance with Circular Letter No.3338 and is not included as part of the electronic data transfer mechanism described below.

5 Functions that can be implemented as part of the electronic data transfer mechanism are contained in table 1 below. In addition, the existing information contained in the module under each section can also be retrieved electronically.

Table 1 – Functions available for the electronic data transfer of information into the Maritime Security module of GISIS

Section	Functions
Organizational contacts	- adding new contact details, or updating/removing existing contact details, of proper recipients of maritime security-related communications, including Recognized Security Organizations.
Port facilities	- creating new port facilities associated to existing ports, or updating/removing existing ones, including updating of any associated information related to port facility security plans, alternative and/or equivalent security arrangements and maritime security point(s) of contact.
Security arrangements	- adding, updating or removing specific security agreements and arrangements

Conditions of use

6 Updates of information through the present electronic data transfer mechanism may be initiated not necessarily by those who have been designated as national points of contact for security-related matters. The Organization has no means to authenticate the identity of individuals operating a remote information system, thus any SOLAS Contracting Government willing to implement the electronic transfer of information into the Maritime Security module of GISIS should take responsibility for ensuring that only the appropriately authorized individuals are permitted to initiate such transfers to GISIS from within their information system.

7 The information to be transferred into the Maritime Security module of GISIS as part of the electronic data transfer mechanism is the responsibility of SOLAS Contracting Government. Any update of information conducted through the electronic data transfer mechanism will be considered as information communicated officially by the SOLAS Contracting Government that has implemented the mechanism.

8 Special attention should be paid to the establishment of processes related to the deletion or update of information as the Organization has no processes in place for the recovery of data that might be deleted or updated in error. In particular, it should be noted that due to technical limitations of the system, IMO Port facility numbers cannot be reused once an existing Port Facility is deleted from the system.

9 The Secretariat remains available to assist with any issues related to the technical implementation of the electronic data transfer mechanism. Any requests for assistance should be addressed to marsec@imo.org.

Technical implementation specifications

Application layer

10 The application layer should be based upon version 1.2 of the SOAP (Simple Object Access Protocol) as defined by the World Wide Web consortium (W3C). SOAP is an application layer protocol that allows communications between nodes without requiring any specific communications network, operating system or programming language. SOAP Version 1.2 specification is available at http://www.w3.org/TR/soap12.

Web services

11 The web services messages are described through WSDL and XSD schema.

Dev/Test	https://gisis-devtest.imo.org/webservices/isps/ispsdata.asmx
Production	

Authentication Header

12 Web service methods must be called with the Authentication Header providing Authority Code, Username, and Password. If there are any issues with authentication or authorisation, a SOAP Exception is thrown.

Web service security

13 Each SOLAS Contracting Government can request a service account for maritime security data exchange. The service accounts are managed by the Secretariat. This special account will be created under a Contracting Government's authority but hidden from the web account administrator's view.

14 A SOLAS Contracting Government can add/modify/delete its own records created by web services. Records created manually cannot be modified or deleted by web services. If records were created by web services they can be edited manually or by web services, and they can be deleted manually or by web services.

Data validation

15 All web services methods will only commit changes if there is no error in the entire process. If there is an error with any part of the input, no record will be committed. The issue must then be resolved and all the data must be submitted again.

16 Web service call results including details of data errors are available under the Data Import tab of the Maritime Security module. This tab is only visible to SOLAS Contracting Governments with a Maritime Security module web service account.

17 Data administrators of SOLAS Contracting Governments can only access logs of web service calls initiated by the same authority.

Submit Method Calls

18 The Submit Methods Calls can be used to submit new or update records in a batch. XML should be UTF8-encoded, and passed as ZIP in binary format. XML will be unzipped and validated by the system for processing.

Delete Method Calls

19 The Delete Methods Calls can be used to delete a single record.

Retrieval Method Calls

20 Retrieval methods are open to any Web Accounts user, including public account and service account. Fair use measurement will be enforced for non-service account users. Public accounts and authorities without a data manager account will not have access to the service call log. If the web service produces any error, the details of the error will be returned to the user account. Returned data will be in XML format, matching the same schema as the XML supplied in the data submission.

Reference code

21 A SOLAS Contracting Government should establish a reference code unique to their authority (up to 12 digits) to identify each record made. The code can be a combination of digits, letters (case sensitive), hyphen and underscore. It must be supplied by the Contracting Government every time when adding/editing/deleting records.

Web service calls histories

22 The history of web service calls is available at the Data Import tab of the Maritime Security module. The purpose of the Data Import page is to give access to the historic web service usage and see details of any errors. The history of all web service calls to submit and delete from the service account will be shown.

APPENDIX

WEB METHODS

SubmitOrganizationalContacts
Header: AuthorityCode, Username, Password
Body: OrganizationalContacts
Return: True – success; False – fail

XML Element/Attribute	Supply in XML	Non-Empty Content Required	Remarks
referenceCode	Y	Y	Reference Code attribute must be provided by the Contracting Government to uniquely identify organizational contact in the same authority
ContactType	Y	Y	Type of contact. Refer to schema for valid numbers and mappings
CountryCode	Y	Y	ISO 3166-1 alpha-3 code. Must be same as web service account authority code. Upper case.
OrganizationName	Y	Y	Name of the organization
NameTitle	Y	Y	
NameFirst	Y	Y	
NameLast	Y	Y	
ContactPost	Y	Y	
SpecificResponsibilities	N	N	Optional, only for RSO contact type. Leave blank or don't supply if not required
AuthorityCondition	N	N	Optional, only for RSO contact type. Leave blank or don't supply if not required
AddressLine1	Y	Y	Must be supplied and cannot be empty
AddressLine2	N	N	
AddressLine3	N	N	
AddressPostCode	Y	Y	
Tel	Y	Y	
Fax	Y	Y	
Mobile	Y	N	
Telex	Y	N	
Email	Y	N	
Website	Y	N	

SubmitPortFacilities
Header: AuthorityCode, Username, Password
Body: PortFacilities,
Return: True – success; False – fail

XML Element/Attribute	Supply in XML	Non-Empty Content Required	Remarks
referenceCode	Y	Y	Reference Code attribute must be provided by the Contracting Government to uniquely identify organizational contact in the same authority
PortLOCODE	Y	Y	UN/LOCODE must be provided and exist in GISIS. This field cannot be updated

FacilityNumber	N	N	This number will be generated in GISIS and cannot be updated
Name	Y	Y	Port facility name
Alias	N	N	Alternative name(s) for this port facility, if applicable
Description	Y	Y	Port facility description
Longitude	Y	Y	ISO 6709 standard
Latitude	Y	Y	ISO 6709 standard
Contacts	Y	Y	
Contact	Y	Y	At least one must be provided
ContactName	Y	Y	
ContactAddress	Y	N	
ContactPostcode	Y	N	
ContactTelephone	Y	Y	
ContactFax	Y	Y	
ContactEmail	Y	N	
ContactTelex	Y	N	
HasApprovedPFSP	Y	Y	Port facility has approved port facility security plan (PFSP)
PFSPApprovalDate	N	Y	Date of port facility security plan (PFSP) approval
PFSPRecentReviewDate	N	N	Date of most recent review or approval of the port facility security plan (PFSP)
SOCRecentIssueDate	N	N	Date of most recently issued Statement of Compliance, if applicable
PFSPWithdrawn	Y	Y	Has this port facility security plan (PFSP) been withdrawn
PFSPWithdrawnDate	N	Y	Port facility security plan (PFSP) withdrawal date

SubmitAlternativeSecurityAgreements
Header: AuthorityCode, Username, Password
Body: AlternativeSecurityAgreements,
Return: True – success; False – fail

XML Element/Attribute	**Supply in XML**	**Non-Empty Content Required**	**Remarks**
referenceCode	Y	Y	Reference Code attribute must be provided by the Contracting Government to uniquely identify organizational contact in the same authority
Facilities	Y	Y	
FacilityNumber	Y	Y	Facility covered by this agreement
Name	Y	Y	Name of the arrangement
FixedRoute	Y	N	Fixed route covered by the arrangement
Information	Y	N	Information on consultation with other governments
EntryIntoForceDate	Y	Y	Date of entry into force of arrangement
PeriodicityReviewDate	Y	N	Periodicity of review of arrangement
HasWidthdrawn	Y	Y	Has security arrangement been withdrawn?
WithdrawnDate	N	Y	If withdrawn, then supply the date

SubmitShipEquivalentSecurityArrangements
Header: AuthorityCode, Username, Password
Body: ShipEquivalentSecurityArrangements,
Return: True – success; False – fail

XML Element/Attribute	Supply in XML	Non-Empty Content Required	Remarks
referenceCode	Y	Y	Reference Code attribute must be provided by the Contracting Government to uniquely identify organizational contact in the same authority
ShipName	Y	Y	Must be supplied
IMONumber	Y	Y	Must be supplied
ArrangementName	Y	Y	Security Arrangement Name
ArrangementDescription	Y	N	Description

SubmitPortFacilityEquivalentSecurityArrangements
Header: AuthorityCode, Username, Password
Body: PortFacilityEquivalentSecurityArrangements,
Return: True – success; False – fail

XML Element/Attribute	Supply in XML	Non-Empty Content Required	Remarks
referenceCode	Y	Y	Reference Code attribute must be provided by the Contracting Government to uniquely identify organizational contact in the same authority
FacilityNumber	Y	Y	From the same authority
ArrangementName	Y	Y	Name of the arrangement
ArrangementDescription	Y	N	Optional

DeleteOrganizationalContact
Header: AuthorityCode, Username, Password
Body: ExternalReference
Return: True – success; False – fail

DeletePortFacility
Header: AuthorityCode, Username, Password
Body: ExternalReference
Return: True – success; False – fail

DeleteAlternativeSecurityAgreement
Header: AuthorityCode, Username, Password
Body: ExternalReference
Return: True – success; False – fail

DeleteShipEquivalentSecurityArrangements
Header: AuthorityCode, Username, Password
Body: ExternalReference
Return: True – success; False – fail

DeletePortFacilityEquivalentSecurityArrangement
Header: AuthorityCode, Username, Password
Body: ExternalReference
Return: True – success; False – fail

GetOrganizationalContacts
Header: AuthorityCode, Username, Password
Parameters: referenceCode (optional), countryCode (optional)
Return: XML – success; Error details – fail

Notes: Either referenceCode or countryCode can be supplied. All records will be returned if no parameter is supplied. referenceCode can only be supplied by the service account of the same authority under which the referenceCode is valid. This code will only be visible in the XML if supplied.

GetPortFacilities
Header: AuthorityCode, Username, Password
Parameters: referenceCode (optional), countryCode (optional), facilityNumber (optional), updatedBefore (optional), updatedAfter (optional)
Return: XML – success; Error details – fail

Notes: All records will be returned if no parameter is supplied. Either referenceCode or facilityNumber can be supplied to return a single record; countryCode and updatedBefore, updatedAfter are additional search conditions and will return port facilities matching all conditions. updatedBefore and updatedAfter must be in UTC. referenceCode can only be supplied by the service account of the same authority under which the referenceCode is valid. This code will only be visible in the XML if supplied.

GetAlternativeSecurityAgreements
Header: AuthorityCode, Username, Password
Parameters: referenceCode (optional), countryCode (optional)
Return: XML – success; Error details – fail

Notes: Either referenceCode or countryCode can be supplied. All records will be returned if no parameter is supplied. referenceCode can only be supplied by the service account of the same authority under which the referenceCode is valid. This code will only be visible in the XML if supplied.

GetShipEquivalentSecurityArrangements
Header: AuthorityCode, Username, Password
Parameters: referenceCode (optional), countryCode (optional)
Return: XML – success; Error details – fail

Notes: Either referenceCode or countryCode can be supplied. All records will be returned if no parameter is supplied. referenceCode can only be supplied by the service account of the same authority under which the referenceCode is valid. This code will only be visible in the XML if supplied.

GetPortFacilityEquivalentSecurityArrangements
Header: AuthorityCode, Username, Password
Parameters: referenceCode (optional), countryCode (optional)
Return: XML – success; Error details – fail

Notes: Either referenceCode or countryCode can be supplied. All records will be returned if no parameter is supplied. referenceCode can only be supplied by the service account of the same authority under which the referenceCode is valid. This code will only be visible in the XML if supplied.

___