

Extraordinary



Federal Republic of Nigeria

Official Gazette

No. 109

Lagos - 7th March, 2014

Vol. 101

Government Notice No. 93

The following is published as supplement to this *Gazette* :

<i>S.I. No.</i>	<i>Short Title</i>	<i>Page</i>
36	Requirement for Registration with the Financial Reporting Council of Nigeria	B459

Printed and Published by The Federal Government Printer, Lagos, Nigeria
FGP150/122014/3,200

Annual Subscription from 1st January, 2014 is Local : ₦25,000.00 Overseas : ₦37,500.00 [Surface Mail]
₦49,500.00 [Second Class Air Mail]. Present issue ₦500.00 per copy. Subscribers who wish to obtain *Gazette* after 1st
January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

S. I. No. 36 of 2014

FINANCIAL REPORTING COUNCIL OF NIGERIA
REQUIREMENT FOR REGISTRATION WITH THE FINANCIAL
REPORTING COUNCIL OF NIGERIA

[5th Day of March, 2014]

Commence-
ment.

In exercise of the powers conferred on me by Section 73 of the Financial Reporting Council of Nigeria Act No. 6 of 2011, and all other powers enabling me in that behalf, I, OLUSEGUN O. AGANGA, CON, Minister of Industry, Trade and Investment, hereby grant approval for the enforcement of the following Orders :

1. From the commencement of this Order, the Financial Reporting Council of Nigeria shall comply with the provisions of Section 8(1)(f) and Section 41(2) of the Financial Reporting Council of Nigeria Act No.6, 2011, as follows—

Comply
with the
Provision.

2. Maintain a register of professional Accountants and other professionals engaged in the financial reporting process.

Maintain a
Register of
Professional
Accountants.

3. No person shall hold any appointment or offer any service for remuneration as a professional for public interest entities, unless he is registered under this Act.

Public
Interest
Entities.

4. In this Order—

Interpretation.

“Act” means the Financial Reporting Council of Nigeria, Act No. 6, 2011.

“Professionals” means professional Accountants and other professionals engaged in the financial reporting process.

5. This Order may be cited as the Financial Reporting Council of Nigeria (Order No. 1, 2014).

Citation.

MADE at Abuja this 5th day of March, 2014.

OLUSEGUN O. AGANGA, CON
Honourable Minister
Federal Ministry of Industry,
Trade and Investment



Federal Republic of Nigeria

Official Gazette

No. 90

Lagos - 6th October, 2014

Vol. 101

Government Notice No. 94

The following is published as supplement to this *Gazette* :

<i>S.I. No.</i>	<i>Short Title</i>	<i>Page</i>
37	Financial Reporting Council of Nigeria—Guidelines/Regulations for Inspection and Monitoring of Reporting Entities	B461-473

Printed and Published by The Federal Government Printer, Lagos, Nigeria
FGP152/122014/3,200

Annual Subscription from 1st January, 2014 is Local : ₦25,000.00 Overseas : ₦37,500.00 [Surface Mail]
₦49,500.00 [Second Class Air Mail]. Present issue ₦1,000.00 per copy. Subscribers who wish to obtain *Gazette* after
1st January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

FINANCIAL REPORTING COUNCIL OF NIGERIA**REVISED GUIDELINES/REGULATIONS 2014****GUIDELINES/REGULATIONS FOR INSPECTIONS AND
MONITORING OF REPORTING ENTITIES**

This is to bring to the notice of all entities, users and preparers of Financial Statements and the General Public that the Guidelines/Regulations aimed at the effective implementation of Nigeria's Accounting, Auditing, Actuarial and Valuation Standards and Code of Corporate Governance, have been issued by the Financial Reporting Council of Nigeria (FRC), an Agency of the Federal Government of Nigeria charged with the responsibility for, amongst other things, developing and publishing accounting and financial reporting standards to be observed in the preparation of financial statements of reporting entities in Nigeria and for related matters vide the FRC Act No. 6 of 2011.

2. Kindly find below the guidelines/regulations for information and due compliance.

FINANCIAL REPORTING COUNCIL OF NIGERIA
ACT NO. 6, 2011

DIRECTORATE OF INSPECTIONS AND MONITORING
GUIDELINES/REGULATIONS, 2014



ARRANGEMENT OF REGULATIONS

Regulation :

1. Enforcement of Compliance.
2. Authority of the Directorate of Inspections and Monitoring.
3. Matters for the attention of the Council.
4. Act on matters by the Council.
5. Details of Analysis on Matters.
6. Complainant duly informed.
7. Conduct of Investigation and Constitution of Panel of Inspectors.
8. Extension of Time of Investigation.
9. Holding of Meeting.
10. Purpose of Meeting.
11. Entity's Representation.
12. Document Verification.
13. Failure to attend Meeting.
14. Seek and receive information from Third Parties
15. Review of Issue(s).
16. Sanctions/ Penalties as prescribed by these Guidelines/Regulations.
17. Penalty.
18. Categories of Non-compliance.
19. Confirmation of decision of the External Auditors and Approval of the Council.
20. Management Time Charge.
21. Revision and Restatement of Accounts.
22. Monitoring of defective Accounts by entity's.
23. Alternative Corrective Action.
24. Informing the Entity's of Imposed Penalty.
25. Appeal.
26. Decision of Technical and Oversight Committee on Appeals.
27. Institution of Legal Action against the Entity.
28. Announcement of Pending Action.

29. Advance Clearance of Financial Statements.
30. Consultation with Council.
31. Management Time Charge for Consulting.
32. Presence of Engagement Partner at Consulting Meetings.

S. I. No. 37 of 2014

**FINANCIAL REPORTING COUNCIL OF NIGERIA
ACT NO. 6, 2011**

**DIRECTORATE OF INSPECTIONS AND MONITORING
GUIDELINES/REGULATIONS, 2014**

[3rd Day of October, 2014]

Commence-
ment.

In exercise of the powers conferred by Section 73 of the Financial Reporting Council of Nigeria Act, No. 6, 2011 (hereinafter referred to as the FRC Act) and of all other enabling powers in that regard, the Honourable Minister of Industry, Trade and Investment, hereby makes the following Regulations—

1. In accordance with Section 7, the Council is empowered to do all things necessary for or in connection with the performance of its functions. The Council is empowered to enforce and approve enforcement of compliance with accounting, auditing, corporate governance and Financial Reporting Standards in Nigeria.

Enforcement
of
Compliance.

2. The powers of the Directorate of Inspections and Monitoring in this regard are derived from Sections 23 and 28 of the FRC Act. The Act is available in pdf format on the Council's website, www.financialreportingcouncil.gov.ng. Legally, the authority of the Directorate of Inspections and Monitoring extends to the accounts, financial reports, returns and other documents of all entities pursuant to the various laws and/or regulations in existence in Nigeria in accordance with Section 11 of the FRC Act. This means that all entities that apply any financial reporting standards in the preparation and presentation of its financial statements, accounts, financial reports, returns and other documents are within the ambit of the authority of the Directorate of Inspections and Monitoring.

Authority of
the
Directorate
of
Inspections
and
Monitoring.

3. Matters may be brought to the attention of the Council due to any of the following—

Matters for
the attention
of the
Council.

(i) a review of financial statements, accounts, financial reports, returns and other documents selected for that purpose by the Inspectors, an officer or agent of the Council ;

(ii) a complaint from individual, entity, regulator, or otherwise ; any breach of the code of conduct and ethics by a registered professional ;

(iii) any material irregularity notified to it ;

(iv) a qualified report ;

(v) public comments (such as press commentary) ; and

(vi) any other matter on financial reporting and corporate governance that may come to the attention of the Council.

Act on
matters by
the Council.

4. When any such matter as in 3 above comes to the attention of the Council, the Secretariat shall acknowledge receipt and refer same to the Directorate of Inspections and Monitoring. The Directorate shall determine whether or not there is ample evidence available to conduct an investigation. Thereafter, the Directorate shall consider the matter(s) drawn to its attention, but may also inquire into other issues relating to financial reporting standards, code of corporate governance and the requirements of the Act.

Details of
Analysis on
Matters.

5. The Inspectors shall provide a preliminary analysis of each matter brought to the Council's attention. This analysis will detail all areas where there appears to be non-compliance with financial reporting standards, code of corporate governance and the requirements of the Act. The analysis will also include a recommendation as to a course of action.

Complainant
duly
informed.

6. Where the Council determines whether or not the issues raised warrant an investigation, the complainant shall be duly informed. Where additional information is required to decide whether an investigation should be opened, the Secretariat may request from the Chief Executive Officer of the relevant entity, such information. The additional information provided by the entity shall be analysed by the Directorate and such other persons with whom the Directorate chooses to consult. The complainant may also be advised of the final outcome of the case.

Conduct of
Investigation
and
Constitution
of Panel of
Inspectors.

7. Where the Council decides to conduct an investigation, a Panel of Inspectors shall be constituted and an Inspector, officer or agent of the Council shall inform in writing the Chief Executive Officer of the entity concerned, copying its auditors. This letter shall identify the relevant reports and indicate whether or not there is a question requiring compliance with the Act. The letter shall indicate the date, time and venue of a meeting with the panel, officer or agent of the Council.

Extension of
Time of
Investigation

8. The Panel, officer or agent of the Council may, in the course of its inspection extend or vary the ambit of the investigation. When such a decision is made, it shall inform the entity as soon as possible.

Holding of
Meeting.

9. A number of meetings may be held with the entity during an investigation. The Panel, Officer or Agent of the Council shall identify the purpose of each meeting and notify the entity of any specific points to be covered. Where practicable, at the end of every meeting, it may indicate any step which the entity may be required to take.

Purpose of
Meeting.

10. The meeting may be held for anyone or more of the following reasons—

(i) explain the preliminary view of the Panel, officer or agent of the Council ;

- (ii) hear further explanation on the matter(s) ;
- (iii) discuss the inappropriateness of an accounting treatment ;
- (iv) explain the requirement to effect remedial action ;
- (v) impose sanctions as deemed fit ; and
- (vi) hear final explanation prior to issuing a letter of warning/penalty, modality for correcting an error, order to withdraw and amend reports, accounts, financial reports or returns and other documents; restatement or notice of intention to prosecute.

11. The entity's representation must include one or more members of its management who have requisite authority to commit it to a required course of action. It should also include the Engagement Partner(s) of the entity's external auditors.

Entity's
Representation.

12. Inspectors may require an entity to produce documents or other evidential material that may shed light on the appropriateness of an accounting treatment.

Document
Verification.

13. Failure to attend or honour an invitation to a meeting, or a request to furnish information, amounts to willful obstruction or delay of an Inspector, in accordance with Section 63 of the Act.

Failure to
attend
Meeting.

14. Where necessary, subject to considerations of confidentiality, the Panel may seek and receive representations from third parties and/or a complainant where it appears that they may have useful information.

Seek and
receive
information
from Third
Parties

15. Where an issue of non-compliance cannot be resolved in a meeting or the Council is of the opinion that an issue requires an in-depth inspection or inquiry, an on-site inspection may be required. Inspectors may be sent to the entity to review the issue(s). The Chief Executive Officer of the entity shall be notified of the date for the on-site inspection. Within ten (10) working days of the notice, the entity must inform the Council of its readiness to receive the Inspectors on the scheduled date.

Review of
Issue(s).

16. The Directorate of Inspections and Monitoring shall impose sanctions/penalties as prescribed by these guidelines/regulations. The appropriate sanctions/penalties are arrived at after due consideration of the nature and materiality of the contravention of the applicable financial reporting standards, code of corporate governance or requirements of the Act.

Sanctions/
Penalties as
prescribed
by these
Guidelines/
Regulations

17. When the Panel decides that any matter is material but not misleading, the entity, the external auditor/audit firm and other relevant professionals/professional firms shall be penalised and the materiality shall determine the penalty.

Penalty.

Categories of
Non
Compliance.

18. There are five categories of non-compliance situations that may be material without rendering the 'financial statements' totally misleading as specified in the schedule attached hereto. In such situations, the Council shall impose sanctions as follows :

- (a) Type 1 non-compliance (N5m) ;
- (b) Type 2 non-compliance (N15m) ;
- (c) Type 3 non-compliance (N25m) ;
- (d) Type 4 non-compliance (N50m) ; and
- (e) Type 5 non-compliance (N100m).

Type 6 : Withdrawal of financial statements leading to restatement - Not less than N500 Million but not more than N5 Billion for each year requiring such restatement. The range is based on Market Capitalization/Turnover as distinguished by Section 33 of the Act and in multiples of N500m.

(b) Entities that are not within the categorization will be penalised based on such factors that may be so determined by the Directorate of Inspections and Monitoring in so far as the amounts are not more than the rates stated here above and not too distinct from the rates altogether. These amounts are subject to review from time to time by the Council.

Confirmation
of decision
of the
External
Auditors and
Approval of
the Council.

19. Where the established contravention or non-compliance is material but not misleading, the error(s) may be corrected in the following year's financial statements. The external auditors shall write to the Council confirming their understanding of the decisions reached at an Inspection meeting. Thereafter, the Council shall communicate its approval to the entity.

Management
Time Charge.

20. The time spent in discovering the errors on non-compliance will be charged to the entity by way of management time at N250,000 (Two Hundred and Fifty Thousand Naira) only per hour. The hours are calculated at the Inspection meeting. However, if the Inspectors have to carry out on-site inspection, the entity shall pay Inspection fee of N1,000,000 (One Million Naira) only per day.

Revision and
Restatement
of Accounts.

21. Where the Panel and the entity agree that accounts are to be rectified by way of revision or restatement, the directors shall effect a full revision of the accounts and not by way of supplementary notes. The procedure for the restatement of financial statements is as stated hereunder :

- (i) The entity shall publish, within seven (7) working days from the date of the Council's final notice, in at least two national newspapers (full page), that the affected reports, accounts, financial reports or returns and other documents have been withdrawn for non-compliance with Financial Reporting Standards and Code of Corporate Governance.

(ii) The Council shall immediately post the information on its website and inform other regulatory agencies that the defective reports, accounts, financial reports or returns and other documents have been withdrawn for restatement, giving reasons.

(iii) The entity shall thereafter republish the reports, accounts, financial reports or returns and other documents, as amended in the same form as the earlier prints, and circulate same to the stakeholders, regulatory agencies and other persons, to whom the defective financial statements had been earlier circulated, drawing their attention to any matters of emphasis.

(iv) The entity shall enclose, to all recipients of the reports, accounts, financial reports or returns and other documents, a reconciliation of the amendments made to the withdrawn financial statements.

22. The Engagement Partner(s) and Panel shall monitor the entity's restatement of the defective accounts. If the entity fails to carry out the restatement in the manner agreed as acceptable to the Panel within 60 days, the Council may institute administrative, civil or criminal proceedings in accordance with Sections 64 and 65 of the Act and also report to other agencies in accordance with Section 67 of the Act.

Monitoring
of defective
Accounts by
entity's.

23. In some cases, the Panel may decide on alternative corrective action, such as issuing a corrective statement published by the entity either separately or, in the next interim report, together with a corrective statement in the following year's annual accounts and adjustment of the relevant comparative figures.

Alternative
Corrective
Action.

The following, among other factors, will be taken into consideration :

- (i) nature and effect of the defect ;
- (ii) the need to protect users of accounts ;
- (iii) the need to correct/prevent a false impression ; and
- (iv) the timing of the entity's reporting cycle.

24. In all circumstances, the Panel shall communicate to the entity the imposed penalty, which must be paid within fourteen (14) days, failing which an additional penalty of 0.1 % of the imposed penalty shall accrue for each day of default.

Informing
the Entity's
of Imposed
Penalty.

25. An entity may appeal against the Panel's decision to the Technical and Oversight Committee (TOC) of the Council within fourteen (14) days with a non-refundable application fee of ₦1m.

Appeal.

26. The decision of the TOC on all appeals shall be communicated to the entity and shall be complied with as follows :

- (a) In the case of a penalty, within seven (7) working days ;
- (b) In the case of restatement, within sixty (60) days.

Decision of
Technical
and
Oversight
Committee
on Appeals.

Institution of
Legal Action
against the
Entity.

27. If at the end of the notice period, the entity still fails to accept the Council's position, the Council shall institute a legal action against the entity. The Council shall notify all relevant regulatory agencies of the pending action, and subsequently, of the outcome of the case.

Announcement
of Pending
Action.

28. The Council shall also make a public announcement on its website and such other media, as it may deem necessary, of the pending action.

Advance
Clearance of
Financial
Statements.

29. The Council or its Directorate of Inspections and Monitoring does not operate a system of advance clearance and would, therefore, not be able to give advice to any entity or its auditors as to whether, in the opinion of the Council, a particular accounting treatment would or would not meet the requirements of the Act or any of the financial reporting standards and code of corporate governance.

Consultation
with
Council.

30. In limited circumstances, the Council may grant audience to an entity or its auditors to give clarification on paragraph(s) of financial reporting standards, code of corporate governance or requirements of the Act or explain a concession provision contained in a financial reporting standard or code of corporate governance.

Management
Time Charge
for
Consulting.

31. The Council may grant such appointment for clarification on the payment of a non-refundable fee of ₦100,000 (One Hundred Thousand Naira) only. The management time spent by the Council during such meetings also attracts ₦500,000 (Five Hundred Thousand Naira) only per hour. This amount is subject to review, from time to time by the Council.

Presence of
Engagement
Partner at
Consulting
Meeting.

32. The Council may request that the Engagement Partner(s) in charge of the audit be present at such clarification meetings.

APPENDIX

SOME ACCOUNTING AND DISCLOSURE ANOMALIES DISTINGUISHED BY TYPE

1.1. No classification of expenses e.g. staff costs, auditor's remuneration, interest on loan, depreciation, directors' remuneration, etc.

1.2. Off-setting of interest received and paid or dividend paid and received in a Statement of Cash Flows.

1.3. Failure to disclose analysis of expenses by nature.

1.4. Failure to provide a split between current and non-current assets and liabilities.

1.5. Failure to classify financial instruments into the appropriate categories e.g. Fair Value Through Profit or Loss, Held to Maturity, Loans and Receivables, Available for Sale and Ammortized Cost.

1.6. No proper reconciliation of the tax charge or deferred taxes, appearing in the income statements.

1.7. No disclosure of accounting policies for accounting for certain significant transactions. This includes :

(i) manner of measurement or valuation of financial assets ;

(ii) manner in which assets and liabilities in foreign currencies are accounted for (conversions and translations) ;

(iii) accounting policies for deferred taxes, taxation, off balance sheet engagements, valuation methods adopted in arriving at the values of inventory, depreciation, leases, employee benefits, etc.

(iv) No accounting policy with respect to funding of employee benefits.

2.1. Wrong or inappropriate treatment of items in the financial statements rectified by disclosure of the accounting policies adopted or by notes or explanatory materials in the same financial statements.

2.2. Crediting of accumulated depreciation associated with the revaluation of property, plant and equipment, to income or retained profit.

2.3. Failure to show an analysis of the portfolio of investments where the main business of the enterprise is the holding of investments.

2.4. Failure to state the accounting policy for accounting for costs incurred and the manner of disposing of capitalized costs in respect of activities involving oil and gas exploration, development and production.

2.5. Failure to show the required highlights in a Statement of Cash Flows and to show, by way of note, a reconciliation of the amounts in a Statement of Cash Flows with equivalent items reported in the Statement of Comprehensive Income or the Statement of Financial Position.

2.6. Non-disclosure of the make-up of "other assets" and "other liabilities" when either of them consists of a significant balance or item in proportion to the total.

3.1. Non-disclosure of the treatment of foreign currency conversions and translations, the treatment given to foreign exchange gains or losses, restriction on repatriation of investments or returns thereon to Nigeria, the amount of gains or losses on foreign currency conversions and translations deferred.

3.2. Failure to provide or make full provision for deferred tax. Failure to compute deferred taxes using the Balance Sheet Liability method or to present deferred tax balance in the appropriate section of the Statement of Financial Position.

3.3. For a Lessor in a finance lease transaction, failure to disclose the gross investment in leases under proper classification, the breakdown of the net investment in leases, the basis used to allocate the income thereon. For a Lessee, failure to disclose assets under finance lease, the amount of assets under each category and accumulated depreciation at the reporting date.

3.4. Non-disclosure of diluted and adjusted EPS where and when necessary.

3.5. Non-disclosure in the notes to the financial statements of the existence, accounting and provisions relating to employee benefits.

4.1. Amortization of past service costs associated with employee benefits.

4.2. Failure to separately disclose the operating results of non-core businesses owned by an entity.

5.1. Departure from a requirement of Statement of Recommended Practice with inadequate, incomplete and misleading disclosure.

5.2. Various errors and anomalies in the Statement of Cash Flows, e.g, the inclusion of non-cash flow items in the statement.

5.3. Misleading disclosure in accounting for leases.

5.4. Comparatives changed without the required disclosures (*i.e.* when a presentation or classification is amended, the comparative amounts is supposed to be reclassified to ensure comparability disclosing the nature, amount and reason for the reclassification).

5.5. Presentation of interim financial statements based on estimates of annual performance rather than actual results.

WITHDRAWAL OF FINANCIAL STATEMENTS UNDER MANAGEABLE RISKS

6.1. The publication of financial statements by an entity where such financial statements are qualified by its external auditors without resolving the qualification issues with the Council.

6.2. Failure to comply with the provisions of the FRC Act.

6.3. Omission of a principal statement in the set of financial statements such as the omission of the Statement of Financial Position, Statement of Comprehensive Income, Statement of Cash Flows, Statement of Changes in Equity or Notes to the financial statements.

6.4. Omission of the Auditors' reports in the financial statements or the inclusion of a corrupted copy in the financial statements or other similar variant of auditors' reports.

6.5. Preparation of financial statements, or part thereof, in line with foreign financial reporting standards where relevant IFRS exists.

These guidelines/regulations may be cited as Financial Reporting Council of Nigeria, Directorate of Inspections and Monitoring Guidelines/Regulations 2014.

MADE at Abuja this 3rd October, 2014.

OLUSEGUN O. AGANGA, CON
Honourable Minister
Federal Ministry of Commerce

EXPLANATORY NOTE

(This note does not form part of the above Regulations but is intended to explain its purport)

These Guidelines/Regulations provide for the Directorate of Inspections and Monitoring of the Financial Reporting Council to enforce compliance with the developed standards, impose sanctions and perform other functions for the Council.

Extraordinary



Federal Republic of Nigeria

Official Gazette

No. 111

Lagos - 21st December, 2014

Vol. 101

Government Notice No. 224

The following is published as supplement to this *Gazette* :

<i>S.I. No.</i>	<i>Short Title</i>	<i>Page</i>
38	Nigerian Maritime Administration and Safety Agency (International Ship and Port Facility Security Code Implementation) Regulations, 2014	B475-514

Printed and Published by The Federal Government Printer, Lagos, Nigeria
FGP 163/122014/1,200

Annual Subscription from 1st January, 2015 is Local : ₦25,000.00 Overseas : ₦37,500.00 [Surface Mail] ₦49,500.00 [Second Class Air Mail]. Present issue ₦1,500 per copy. Subscribers who wish to obtain *Gazette* after 1st January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

NIGERIAN MARITIME ADMINISTRATION AND SAFETY AGENCY
ACT (CAP. N161 LFN)

AND

INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT
SEA (ENFORCEMENT AND RATIFICATION) ACT (CAP. I26 LFN)

NIGERIAN MARITIME ADMINISTRATION AND SAFETY AGENCY
(INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE
IMPLEMENTATION) REGULATIONS, 2014



ARRANGEMENT OF REGULATIONS

Regulation :

PART I—PURPOSES AND APPLICATION

1. Purpose.
2. Application.

PART II—STRATEGY AND RESPONSIBILITY FOR SHIP
AND PORT FACILITY SECURITY

3. ISPS Code Implementation Strategy.
4. The Ministerial Implementation Committee on the ISPS Code (MIC-
ISPS).
5. The ISPS Code Implementation Committee (ICIC).
6. Duties of the ICIC.
7. The ISPS Code Unit.
8. Head and Membership of the ISPS Code Unit.
9. The Lead Recognised Security Organisation (LRSO).
10. Tenure of a Lead RSO.
11. Remuneration of a Lead RSO.
12. Engagement of RSOs.
13. Accreditation of RSOs.
14. Removal of a Lead RSO.
15. The Zonal Security Committee.
16. The General Conference on Maritime Security.
17. Duties of the Designated Authority.
18. Powers of the Designated Authority.
19. Delegation of Powers.
20. Alternative Security Arrangements.
21. Equivalent Security Arrangements.
22. Administrative Enforcement Powers.
23. Recognised Security Organisations (RSOs).

PART III—DOCUMENTATION

24. Security Assessments.
25. Security Plans.
26. Statement of Compliance (SOC) and International Ship Security Certificate (ISSC).
27. Declarations of Security (DOS).
28. Records.
29. Audit Requirements.
30. Restrictions.

PART IV—SECURITY LEVELS

31. General.
32. Security Level 1.
33. Security Level 2.
34. Security Level 3.

PART V—SHIP SECURITY

35. Company Security Officer (CSO).
36. Qualifications of a CSO.
37. Duties of a CSO.
38. Powers of the CSO.
39. Revocation of the CSO's Appointment.
40. Ship Security Officer (SSO).
41. Qualifications of an SSO.
42. Duties of an SSO.
43. Powers of an SSO.
44. Security Personnel.
45. Training, Drills and Exercises.
46. Physical Security.
47. Ship Security Alert System (SSAS).
48. Automatic Identification System (AIS).
49. Long-Range Identification and Tracking (LRIT).
50. Operational Security.
51. Security Obligations.
52. Incident Response.

PART VI—PORT FACILITY SECURITY

53. Port Facility Security Officer (PFSO).
54. Qualifications of a PFSO.
55. Duties of a PFSO.
56. Powers of a PFSO.
57. Revocation of a PFSO's Appointment.
58. Port Facility Security Personnel.
59. Basic Port Security Knowledge.

- 60. Security Guards.
- 61. Training, Security Awareness, Drills and Exercises.
- 62. Physical Security.
- 63. Operational Security.
- 64. Regular Users.
- 65. Service Providers.
- 66. Ship's Crew.
- 67. Visitors.
- 68. Vehicles.
- 69. Law Enforcement or Emergency Responders.
- 70. Unauthorised Access Procedures.
- 71. Cargo Operations.
- 72. Ship's Stores.
- 73. Passenger Procedures.
- 74. Primary Ship and Port Interface Security Information.
- 75. Incident Response.

PART VII—ENFORCEMENT

- 76. Authorities.
- 77. Control Measures.

PART VIII—OFFENCES AND PENALTIES

- 78. General.
- 79. Administrative Violations.

PART IX—MISCELLANEOUS

- 80. Interpretation.
- 81. Citation.

PREAMBLE

WHEREAS the International Ship and Port Facility Security (ISPS) Code was adopted by the International Maritime Organization (IMO) on December, 2002 as an amendment to the International Convention for the Safety of Life at Sea (SOLAS), 1974 ;

AND WHEREAS, Nigeria ratified the International Ship and Port Facility Security (ISPS) Code as an amendment to the International Convention for the Safety of Life at Sea (SOLAS) 1974, by the enactment of the International Convention for the Safety of Life at Sea (Ratification and Enforcement) Act, 2004 ;

AND WHEREAS, it is expedient to establish the administrative and legal framework for the implementation of the International Convention for the Safety of Life at Sea (Ratification and Enforcement) Act 2004.

S. I. 38 of 2014

**NIGERIAN MARITIME ADMINISTRATION AND SAFETY AGENCY
ACT (CAP. N161 LFN)**

AND

**INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT
SEA (ENFORCEMENT AND RATIFICATION) ACT (CAP. I26 LFN)**

**NIGERIAN MARITIME ADMINISTRATION AND SAFETY AGENCY
(INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE
IMPLEMENTATION) REGULATIONS, 2014**

[18th Day of November, 2014]

Commence-
ment.

In exercise of the powers conferred on the Government of the Federal Republic of Nigeria by Article 4, Part I of the Annex to the International Convention for the Safety of Life at Sea (Enforcement and Ratification) Act, 2004, Cap. I26 LFN ; and the powers conferred on the Nigerian Maritime Administration and Safety Agency by Section 51(3) of the Nigerian Maritime Administration and Safety Agency Act, Cap. N161, LFN ; and all other powers enabling it in that behalf, the Nigerian Maritime Administration and Safety Agency makes the following Regulations—

PART I—PURPOSE AND APPLICATION

1. The purpose of these Regulations is to—

Purpose.

(a) establish a legal framework for the implementation of the International Ship and Port Facility Security (ISPS) Code in the Federal Republic of Nigeria ;

(b) implement and enforce the provisions of the International Ship and Port Facility Security (ISPS) Code, as adopted by the International Maritime Organization (IMO) on 12th December, 2002 ; and

(c) appoint the Nigerian Maritime Administration and Safety Agency (NIMASA), as the Designated Authority to oversee the implementation, application, administration and management of these Regulations with respect to Ships and Port facilities.

2.—(1) These Regulations shall apply to—

Application.

(a) the following types of ships engaged on international voyages—

(i) passenger ships, including high speed passenger crafts,

(ii) cargo ships, including high speed crafts of 500 gross tonnage and upwards, and

(iii) self-propelled mobile offshore drilling units capable of making international voyages unassisted and unescorted when underway and not on location ;

- (b) port facilities which service ships defined under these Regulations ;
- (c) the following types of ships engaged in domestic voyages—
 - (i) passenger ships of 500 gross tonnage and upwards,
 - (ii) cargo ships of 500 gross tonnage and upwards, and
 - (iii) fishing vessels ancillaries not involved in catching living resources of the sea of 500 gross tonnage and upwards ; and
- (d) such other ships and port facilities as may be so defined by the Designated Authority.

(2) These Regulations do not apply to—

- (a) warships, naval auxiliaries or other ships owned or operated by a Government and used only on Government non-commercial service ; or
- (b) a ship while the ship is laid up, dismantled or otherwise out of commission.

PART II—STRATEGY AND RESPONSIBILITY FOR SHIP AND PORT FACILITY SECURITY

ISPS Code
Implementation
Strategy.

3. The Designated Authority shall be assisted in the discharge of its maritime security objectives by the—

- (a) Ministerial Implementation Committee on the ISPS Code (MIC-ISPS) ;
- (b) ISPS Code Implementation Committee (ICIC) ;
- (c) ISPS Code Unit ;
- (d) Lead Recognized Security Organization (LRSO) ;
- (e) General Conference on Maritime Security ; and
- (f) Zonal Security Committee.

The
Ministerial
Implementation
Committee
on the ISPS
Code (MIC-
ISPS).

4.—(1) The Minister shall convene the MIC-ISPS, which shall meet quarterly to review the Designated Authority's performance of its ISPS Code implementation functions and advise the Minister accordingly.

(2) The membership of the MIC-ISPS shall comprise of representatives of each of the following Organisations who shall be persons not below the rank of Assistant Director—

- (a) NIMASA ;
- (b) Federal Ministry of Transport (FMOT) ; and
- (c) Nigeria Port Authority (NPA).

5.—(1) The Designated Authority shall convene the ICIC which shall meet quarterly.

The ISPS
Code
Implementa-
tion
Committee
(ICIC).

(2) The membership of the ICIC shall comprise of representatives of each of the following organisations who shall be persons not below the rank of Assistant Director—

- (a) Nigerian Maritime Administration and Safety Agency (NIMASA) ;
- (b) Federal Ministry of Transport (FMOT) ;
- (c) Nigerian Ports Authority (NPA) ;
- (d) Nigerian Navy (NN) ;
- (e) Nigerian Inland Waterways Agency (NIWA) ;
- (f) Nigerian National Petroleum Corporation (NNPC) ;
- (g) Department of Petroleum Resources (DPR) ;
- (h) Nigeria Police Force (NPF) ;
- (i) Nigeria Customs Service (NCS) ;
- (j) Nigeria Immigration Service (NIS) ; and
- (k) Department of State Services (DSS).

(3) The Designated Authority shall appoint a qualified member of its ISPS Code Unit to serve as the Secretary to the ICIC and the Unit shall serve as the ICIC's Secretariat.

6. The ICIC shall—

Duties of
the ICIC.

(a) assist the Designated Authority in determining ISPS Code implementation expectations, goals and objectives ;

(b) assist the Designated Authority in formulating policies to achieve established ISPS Code implementation expectations, goals and objectives ;

(c) review the Designated Authority's achievement of the ISPS Code implementation expectations, goals and objectives ;

(d) mobilize support for the Designated Authority's programs for ISPS Code implementation ;

(e) review overall schedules and plans for advancing and improving ISPS Code implementation performance ;

(f) recommend budget, membership personnel, organizational lines of communication, responsibility, accountability and authority to execute the plans designed to meet ISPS Code implementation goals and objectives ;

(g) ensure implementation of the ISPS Code through recommendations and action items from internal and external reviews, lessons learnt and continuous improvement initiatives ;

(h) recommend modalities for the recognition and reward of outstanding performance in ISPS Code Implementation ;

(i) avail Agencies represented in the ICIC with periodic reports on ISPS Code implementation status and performance ; and

(j) carry out any other duty as may be assigned to it by the Designated Authority, considered necessary for the attainment of the ISPS Code implementation strategy.

The ISPS
Code Unit.

7. The Designated Authority shall establish an ISPS Code Unit, which shall be responsible for the routine and administrative components of ISPS Code implementation and enforcement.

Head and
Membership
of the ISPS
Code Unit.

8.—(1) The Designated Authority shall appoint a qualified member of its staff with proven expertise and experience in ISPS Code implementation to head the ISPS Code Unit.

(2) The Unit in sub-regulation (1) of this regulation shall be made up of administrative, operations and enforcement officers, who shall be ISPS Code certified officers drawn from the ranks of the Designated Authority.

The Lead
Recognised
Security
Organisation
(LRSO).

9.—(1) The Designated Authority may appoint from the ranks of the accredited Recognized Security Organizations (RSOs), a person of proven experience, integrity and leadership quality to be the Lead RSO.

(2) A person appointed under sub-regulation (1) of this regulation shall serve as a liaison between the Designated Authority and the RSOs and advise the Designated Authority on such matters as Ship and Port Facility Security Assessments or Plans, Verification Inspection Exercise (VIE), training and certification of relevant professionals as well as other ISPS Code related matters that the Designated Authority may require technical assistance on.

Tenure of a
Lead RSO.

10. An RSO appointed as a Lead RSO shall hold the position for a period of two years, which may be renewed for a further period of two years after which another RSO from the pool of RSOs may be appointed to the position.

Remuneration
of a Lead
RSO.

11. A Lead RSO shall receive payment for his services as may be determined by the terms of his engagement by the Designated Authority.

Engagement
of RSOs.

12. A Lead RSO shall assist the Designated Authority in the accreditation and engagement of the services of RSOs to carry out field operational activities, such as Port Facility Security Survey, Inspections, Assessments and such other technical activities as may be required by the Designated Authority on grounds of inadequate capacity.

13.—(1) RSOs shall be accredited by the Designated Authority after due evaluation through a selection process established by the Designated Authority.

Accreditation
of RSOs.

(2) The accreditation in sub-regulation (1) of this regulation shall be for a period of one year, renewable at the expiration of the approved period.

(3) An accredited RSO may be blacklisted and sanctioned by the Designated Authority on grounds of non-performance or unsatisfactory performance of his functions.

14.—(1) Nothing in the provisions of regulation 13 of these Regulations shall preclude the powers of the Designated Authority to terminate the appointment of a Lead RSO, on grounds of non-performance or unsatisfactory performance of his functions.

Removal of
a Lead RSO.

(2) In the event of there being a termination under sub-regulation (1) of this regulation, a former Lead RSO shall continue his duties as an RSO, provided he was not removed on grounds of fraud, dishonesty, abuse of privilege or activities considered tantamount to a breach of security of ships and port facilities under the administration of the Designated Authority.

15. The Port Security Officer shall periodically and when necessary, convene the Zonal Security Committee comprising of the Designated Authority, Port Facility Security Officers (PFSOs), RSOs and representatives of relevant government Agencies, where review of contemporary matters affecting the security of port facilities and ships utilizing their services shall be conducted in addition to any ISPS Code related matter.

The Zonal
Security
Committee.

16. The Designated Authority shall convene a bi-annual General Conference on Maritime Security where all stakeholders shall be updated on the status of ISPS Code implementation and shall thereafter suggest recommended improvement opportunities for the consideration of the Designated Authority.

The General
Conference
on Maritime
Security.

17. The Designated Authority shall—

(a) be responsible for ensuring full implementation of the ISPS Code in Nigeria ;

(b) evaluate and distribute port facility security information to subordinate port facility officials and responsible Recognised Security Organisations ;

(c) develop plans and policies to counter port security threats ;

(d) review, test and audit security plans ;

(e) issue Statements of Compliance as warranted ;

Duties of
the
Designated
Authority.

- (f) inspect, maintain, and test security facilities equipment and systems ;
- (g) oversee the implementation and adequacy of port facility security ;
- (h) set the applicable security level ;
- (i) identify security regulated port facilities and certify Port Facility Security Officers ;
- (j) ensure the completion and approval of port facility security assessments, plans and subsequent amendments ;
- (k) exercise control, compliance measures and enforce the implementation of the ISPS Code ;
- (l) supervise and coordinate all law enforcement agencies and government or private security organizations performing port security services ;
- (m) report existing national port security legislation to the International Maritime Organization (IMO) ;
- (n) refer infringements of the ISPS Code with criminal elements to the appropriate Agencies for investigation and prosecution ;
- (o) provide necessary technical and professional guidance on ISPS Code ;
- (p) train and retrain the Designated Authority's ISPS Code implementation personnel to keep pace with global trends, technical updates and innovations ;
- (q) advise the Federal Government of Nigeria on ISPS Code related issues ;
- (r) articulate and present the position of the Federal Republic of Nigeria on ISPS Code related matters at local and international seminars, workshops and conferences ; and
- (s) carry out such other ISPS Code implementation functions as may be directed by the appropriate authorities.

Powers of
the
Designated
Authority.

18.—(1) *Security Level and Governance Powers* : The Designated Authority shall have the power to—

- (a) implement a system to collect, collate, integrate and analyze threats to ports, port facilities, shipping and cargo ;
- (b) set security levels and provide security guidance to ports, port facilities, shipping and cargo ;
- (c) direct the implementation of additional security measures as necessary to prevent probable or imminent unlawful interference with ships and port facilities regulated under these Regulations; and

(d) have unlimited and full access, whether scheduled or unscheduled, to any port facility or ship within Nigeria to carry out ISPS Code implementation functions.

(2) *Regulatory Powers* : The Designated Authority shall—

(a) issue guidelines, directives and notices implementing these Regulations ; and

(b) provide such general directions as may be required to implement guidelines, directives and notices.

(3) *Investigative Powers* : The Designated Authority shall have the power to—

(a) enter and inspect any security regulated ship or port facility to ensure compliance with these Regulations ;

(b) make inquiries, examinations, inspections, searches, seizures, and arrests upon any security regulated ships or port facilities or those adjacent thereto, to ensure compliance with these Regulations ;

(c) disseminate such information and documentation as is required under these Regulations ; and

(d) investigate and refer any violation of these Regulations for prosecution.

(4) *Enforcement Powers* : The Designated Authority shall have the power to enforce all laws and regulations pertaining to ship and port facility security in Nigeria and in so doing, it may enlist the assistance of law enforcement agencies or other appropriate authorities, or appoint relevant personnel to carry out its mandate.

19. The Designated Authority may delegate its powers and functions under these Regulations to qualified personnel or Recognized Security Organizations, subject to restrictions set forth by these Regulations.

Delegation
of Powers.

20. Where port facilities interface with regulated ships operating on short, fixed international routes, the Designated Authority may enter into alternative security agreements with other participating governments to ensure that the ships undertake all steps necessary to maintain the security of the ship to port interface.

Alternative
Security
Arrangements.

21.—(1) Port facilities with infrequent or special operations may be designated as occasional port facilities.

Equivalent
Security
Arrangements.

(2) The Designated Authority may authorize occasional port facilities to adopt security measures equivalent to those prescribed by these Regulations.

Administrative
Enforcement
Powers.

Recognised
Security
Organisations
(RSOs).

22. The administrative inquiry of offences under these Regulations may be initiated and performed by the Designated Authority, who shall collaborate with the Port Security Officers in the exercise.

23.—(1) *General* : The Designated Authority may authorize a Recognized Security Organization to—

- (a) conduct security assessments on behalf of the Designated Authority ;
- (b) assist in the development and preparation of security plans for Port Facilities ;
- (c) inspect and audit port facilities ; or
- (d) perform other ISPS Code implementation related duties.

(2) *Qualifications* : The Designated Authority shall ensure that Recognized Security Organizations are qualified to perform delegated duties and the appointment of a Recognized Security Organization shall be revoked where it fails to meet the conditions and qualifications set forth in these Regulations as well as the terms of reference of its engagement.

(3) *Restrictions* : Recognized Security Organizations shall not—

- (a) set applicable security levels ;
- (b) approve port facility security assessments or plans, or amendments to an approved assessment or plan ;
- (c) determine which port facilities will be required to designate a Port Facility Security Officer ;
- (d) exercise control and compliance measures ;
- (e) establish requirements for Declaration of Security ; or
- (f) review or approve ship security assessments or plans where the Recognized Security Organization has participated in the preparation of the ship security assessment or plan under review.

PART III—DOCUMENTATION

Security
Assessments.

24.—(1) The Designated Authority shall ensure that a completed security assessment is submitted with all pending security plans prior to approval.

(2) A security assessment shall address the following—

- (a) physical security ;
- (b) security equipment ;
- (c) security procedures ;
- (d) communications ;
- (e) transportation infrastructure ;
- (f) utilities infrastructure ; and

(g) any other area that may, where damaged or used for unauthorized observation, pose a risk to persons, property, or operations within the port, port facility or aboard ships adjacent thereto.

(3) The Designated Authority shall review security assessments periodically, at intervals not exceeding three years.

25.—(1) Ships shall maintain a security plan approved by the Designated Authority, Classification Society or Organization, or Recognized Security Organization.

Security
Plans.

(2) Port facilities shall maintain a security plan approved by the Designated Authority.

(3) A submitted ship or port facility security plan or an amendment thereto, shall be examined for compliance with these Regulations by the Designated Authority or the Recognized Security Organization, as may be applicable in line with sub-regulations (1) and (2) of this regulation.

(4) A security plan shall address the following—

- (a) security incident duties and comprehensive response procedures ;
- (b) weapon and dangerous substance interdiction ;
- (c) access control procedures ;
- (d) evacuation procedures ;
- (e) security personnel duties ;
- (f) periodic security plan review, audit and update procedures ;
- (g) emergency response and public safety contact information ;
- (h) security plan protection measures ;
- (i) cargo security procedures ;
- (j) security level compliance and establishment procedures ;
- (k) ship security communication procedures ;
- (l) public threat announcement procedures ;
- (m) operational interface security procedures ;
- (n) identification of a Company Security Officer and Port Facility Security Officer, including twenty-four hour contact details ;
- (o) training and drills ;
- (p) equipment testing, calibration and maintenance procedures ;
- (q) monitoring security procedures ; and
- (r) incident management and corrective actions tracking.

(5) A Port Facility Security Officer shall review port facility security plans periodically, at intervals not exceeding one year, and notify the Designated Authority of such review.

Statement of
Compliance
(SOC) and
International
Ship
Security
Certificate
(ISSC).

Declarations
of Security
(DOS).

Records.

Audit
Requirements.

(6) The security plan shall be protected from unauthorized access or disclosure.

26.—(1) The Designated Authority shall issue a Statement of Compliance (SOC) or International Ship Security Certificate (ISSC) to compliant port facilities and ships respectively, indicating the security plan compliance with the provisions of these Regulations.

(2) The period of validity of the certificates under sub-regulation (1) of this regulation shall not exceed—

(a) one year for Statement of Compliance ; and

(b) five years for International Ship Security Certificate.

27.—(1) A regulated port facility shall require a Declaration of Security with arriving ships detailing the security responsibilities of each ship when the—

(a) port facility is operating at a higher security level than the ship ;

(b) port facility or ship is operating at Security Level 3 ;

(c) ship to port interface poses a specific risk to local facilities or residents ;

(d) ship has undertaken a ship to ship activity with a non-SOLAS or high risk ship ;

(e) ship is a non-SOLAS ship ;

(f) Port Security Officer deems a Declaration of Security necessary to maintain port security ; or

(g) ship does not possess a valid International Ship Security Certificate.

(2) A ship shall request for a Declaration of Security when—

(a) the ship is operating at a higher security level than the port facility or another ship it is interfacing with ;

(b) another ship it is interfacing with is not required to implement a security plan ; or

(c) warranted by circumstances.

28.—(1) The responsible security officer shall maintain all security records for a period of not less than ten years.

(2) Records of ships security activities, including Declarations of Security and the record of the ship security level, shall be maintained onboard for a period covering at least the previous ten calls at port facilities.

29. Security plans shall be audited by internal or external auditors at intervals not exceeding—

(a) one year for port facilities ; and

(b) five years for ships.

30. Security plans shall not be audited by the organizations which developed the plan.

Restrictions.

PART IV—SECURITY LEVELS

31.—(1) The Designated Authority shall set and communicate security levels to alert Port Security Officers, Port Facility Security Officers and Ship Security Officers of the perceived risk of a terrorist attack or security threat.

General.

(2) In setting the security levels under sub-regulation (1) of this regulation, the Designated Authority shall take account of general and specific threat information including the—

- (a) degree that the threat information is credible ;
- (b) degree that the threat information is corroborated ;
- (c) degree that the threat information is specific or imminent ; and
- (d) potential consequences of such a security incident.

(3) The Designated Authority shall set security levels applying to ships or port facilities at one of the following three levels—

- (a) security level 1 – normal – being the level at which the ship or port facility normally operates ;
- (b) security level 2 – heightened – being the level applying for as long as there is a heightened risk of a security incident ; and
- (c) security level 3 – exceptional – being the level applying for the period of time when there is the probable or imminent risk of a security incident based on credible information.

(4) The Designated Authority shall communicate any changes in security levels to ships and port facilities that may be affected, as soon as possible.

(5) A ship or port facility shall acknowledge receipt of the Designated Authority's communication under sub-regulation (4) of this regulation, on a change in the security.

32.—(1) Security level 1 means the level at which minimum appropriate protective security measures shall be maintained at all times.

Security
Level 1.

(2) At security level 1, the following security measures shall be implemented—

- (a) enforce access controls ;
- (b) screen or search persons and vehicles ;
- (c) conspicuous post signs identifying restricted areas and security measures in effect ;
- (d) inspect cargo and ship stores prior to loading ;

(e) screen accompanied and unaccompanied baggage prior to loading ; and

(f) monitor access points, land and waterside perimeter, restricted areas and ship to port interface.

Security
Level 2.

33.—(1) Security Level 2 means the level at which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

(2) At Security Level 2, the following security measures shall be implemented—

- (a) increase landside, waterside and shipboard security patrols ;
- (b) reduce the number of access points to restricted areas ;
- (c) increase the coverage and intensity of lighting and surveillance equipment ;
- (d) intensify checking of cargo, seals, ship stores, cargo transport units and cargo storage areas ;
- (e) intensify cargo documentation review ;
- (f) intensify delivery vehicles searches ;
- (g) subject all unaccompanied bag-gages to x-ray screening from at least two different angles ; and
- (h) escort all delivery vehicles.

Security
Level 3.

34.—(1) Security Level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent.

(2) At Security Level 3, the following security measures shall be implemented—

- (a) suspend access to all, or part of, the ship or port facility ;
- (b) grant access only to those responding to the security incident or threat thereof ;
- (c) suspend personnel or vehicular movement within all, or part, of the ship or port facility ;
- (d) increase security patrols aboard ship or within the port facility ;
- (e) suspend operations within all, or part, of the ship or port facility ;
- (f) direct ship movements relating to all, or part, of the port facility ;
- (g) evacuate all, or part of, the ship or port facility ;
- (h) activate all lighting within, or adjacent to the ship or port facility ;
- (i) activate all surveillance equipment aboard ships or, in and adjacent to the port facility ; and
- (j) restrict or suspend of handling of unaccompanied bag-gages.

PART V—SHIP SECURITY

35. A shipping company shall appoint a Company Security Officer who has been duly certified by the Designated Authority to implement and administer these Regulations.

Company
Security
Officer
(CSO).

36.—(1) A shipping company shall ensure that the Company Security Officer is qualified to perform his duties.

Qualifications
of a
Company
Security
Officer
(CSO).

(2) The minimum qualification for appointment as a Company Security Officer shall be as follows—

(a) a University degree in marine related subjects, a Certificate Of Competence (COC) in line with provisions of the Standard of Training Certification and Watch-keeping, 1995 (STCW '95) or its equivalent ;

(b) five years cognate experience in a security related position ; and

(c) ISPS Code certification by the Designated Authority or its accredited training institutions.

37. The Company Security Officer shall—

Duties of a
Company
Security
Officer
(CSO).

(a) ensure the completion and timely audit of required security assessments ;

(b) ensure the development, submission, implementation and timely audit of required security plans ;

(c) ensure the conduct of ship security drills and exercises ;

(d) conduct ship security inspections ;

(e) ensure adequate company security personnel training ;

(f) maintain records as required by these Regulations ;

(g) notify law enforcement personnel and other emergency responders of applicable ship security incidents ; and

(h) ensure that all security measures and protocols set forth in these Regulations are implemented and enforced.

38. The Company Security Officer shall be empowered to—

Powers of
the
Company
Security
Officer
(CSO).

(a) enter ships belonging to or under the control of his Company to make inquiries, examinations, inspections and searches in accordance with these Regulations ; and

(b) implement all security measures and protocols as required by these Regulations.

39. The Company Security Officer's appointment shall be revoked where his ISPS Code certificate is withdrawn by the Designated Authority or is not renewed within three months of the stated expiry period.

Revocation
of the
Company
Security
Officer's
Appointment.

Ship
Security
Officer
(SSO).

Qualifications
of a Ship
Security
Officer
(SSO).

Duties of a
Ship
Security
Officer
(SSO).

Powers of a
Ship
Security
Officer
(SSO).

Security
Personnel.

40. Shipping companies shall appoint, aboard each security regulated ship, a Ship Security Officer who has been duly certified by the Designated Authority to implement and administer these Regulations.

41.—(1) The shipping company shall ensure that the Ship Security Officer (SSO) is qualified to perform his other duties.

(2) The minimum qualification for appointment as an SSO shall be as follows—

(a) Certificate of Competence (COC) in line with the provisions of the Standard of Training Certification and Watch-Keeping, 1995 (STCW '95) or its equivalent ;

(b) five years cognate experience in a security related position ; and

(c) ISPS Code certification by the Designated Authority or its accredited training institutions.

(3) A Ship Security Officer's appointment shall be revoked where he fails to meet the conditions and qualifications set forth in these Regulations or the terms of the contract of his appointment.

42. A Ship Security Officer shall—

(a) co-ordinate security measures with interfacing security regulated ports and port facilities ;

(b) ensure the development, submission and implementation of required security plans ;

(c) conduct ships security drills and exercises ;

(d) conduct ship security inspections ;

(e) ensure adequate ship security personnel training ;

(f) maintain records as required by these Regulations ;

(g) ensure the execution of any required Declarations of Security ;

(h) notify law enforcement personnel, emergency responders and relevant port security authorities of applicable ship security incidents ; and

(i) ensure that all security measures and protocols set forth in these Regulations are implemented and enforced.

43. A Ship Security Officer shall—

(a) exercise security controls aboard assigned ships ; and

(b) implement security measures and protocols as required by these Regulations.

44.—(1) *Qualification* : Shipping Companies shall ensure that security personnel are qualified to perform delegated duties.

(2) *Revocation of Appointment* : The appointment a of security personnel shall be revoked where he fails to meet the conditions and qualifications set forth in these Regulations or the terms of his contract of appointment.

(3) *Background Checks* : All ship security personnel shall be subjected to background record checks in accordance with the shipping company's administrative procedures.

(4) *Expertise* : All security personnel under these Regulations shall have relevant knowledge in the following areas of ship and port facility security—

- (a) basic security organization ;
- (b) ship and port facility security measures ;
- (c) emergency preparedness and response ;
- (d) basic security equipment and systems ;
- (e) inspections, patrol, and monitoring techniques ;
- (f) law enforcement responsibilities ;
- (g) basic security related communications ;
- (h) current security level ;
- (i) recognizing and detecting potentially dangerous substances and devices ;
- (j) recognizing behavioural patterns of persons who are likely to threaten security ;
- (k) basic techniques used to circumvent security measures ;
- (l) conducting physical searches and non-intrusive inspections ; and
- (m) basic security drills and exercises.

45.—(1) The Designated Authority shall review and approve the curricula for all ISPS Code training.

Training.
Drills and
Exercises.

(2) The Designated Authority shall provide the training under sub-regulation (1) of this regulation where necessary.

(3) A Ship Security Officer shall ensure that security awareness is maintained on board ships at all times.

(4) Security drills shall be conducted at least once every three months to test the scenarios developed from the contents of the security plan.

(5) Security exercises shall be conducted once every year to test the effectiveness of the security plan.

(6) Security exercises may be either full scale or tabletop simulation.

46.—(1) *Security Zones* : Ships may designate shipboard restricted areas and security zones to restrict access and address specific security requirements.

(2) *Restricted Access* : A person shall not enter a shipboard restricted area or security zone except by permission of the CSO, SSO, or their authorized delegates.

(3) *Access Points* : Ship Security Officers shall secure and control all shipboard access points, including—

- (a) access ladders ;
- (b) access gangways ;
- (c) access ramps ;
- (d) access doors, side scuttles, windows and ports ;
- (e) mooring lines and anchor chains ; and
- (f) cranes and hoisting gear.

(4) *Signage* : A ship shall install signage clearly identifying all security zones and restricted areas.

(5) *Lighting* : A ship's deck, access points and areas immediately around the ship shall be illuminated during hours of darkness and periods of low visibility while conducting ship to ship and ship to port interface activities and at anchorage.

(6) *Lighting* : While underway, ships shall use the maximum lighting available consistent with safe navigation.

(7) *Surveillance* : A Ship Security Officer shall ensure the continued monitoring of—

- (a) access points ;
- (b) weather decks ;
- (c) restricted areas on board the ship ; and
- (d) area surrounding the ship.

(8) *Key Control* : Where access points into restricted areas are key-controlled, a restricted key system shall be implemented to monitor, track, and control subject keys.

(9) *Communications* : A Ship Security Officer shall have the means to effectively communicate with the ship and port facility security personnel, law enforcement authorities and emergency response authorities and notify facility personnel of changes in shipboard security conditions.

47. In accordance with the International Convention for the Safety of Life at Sea (SOLAS) Chapter XI-2, a security regulated ship shall maintain a Ship Security Alert System which shall—

(a) be capable of being activated from the navigation bridge and in at least one other location ;

(b) conform to the International Maritime Organization (IMO) standards ;

(c) be designed so as to prevent the inadvertent initiation of the ship security alert ;

(d) initiate and transmit a ship to shore security alert to the Designated Authority, which shall include the following information—

(i) vessel name,

(ii) IMO ship identification number,

(iii) date and time,

(iv) position,

(v) course and speed,

(vi) CSO and phone number, and

(vii) a message stating that the Ship Security Alert System (SSAS) has been activated and indicating the ship is under threat or has been compromised ;

(e) not send the ship security alert to any other ship ;

(f) not raise any alarm onboard the ship ; and

(g) continue the ship security alert until deactivated or reset.

48. A regulated ship shall employ, maintain and operate an Automatic Identification System in accordance with the Designated Authority's specifications.

Automatic
Identification
System
(AIS).

49. A regulated ship shall employ, maintain and operate Long Range Identification and Tracking systems in accordance with the Designated Authority's specifications.

Long-Range
Identification
and Tracking
(LRIT).

50.—(1) Master's Discretion : Where in the professional judgment of a Master, a conflict between any safety and security requirement applicable to the ship arises during its operations, the Master may give precedence to measures intended to maintain the safety of the ship, and take such temporary security measures as seem best under all circumstances.

Operational
Security.

(2) Port Control Compliance : A security regulated ship shall comply with port control directives issued by authorized Port Security Officers and Port Facility Security Officers.

(3) Manning Requirements : A security regulated ship shall maintain sufficient crew to operate and navigate the ship in case of emergency onboard.

(4) Security Sweeps : At all security levels, a Master shall ensure security sweeps are performed prior to getting underway and after any period the ship was unattended.

(5) *Access Control* : A ship shall implement access control procedures as specified in the ship security plan for—

- (a) ship's crew ;
- (b) service providers ;
- (c) passengers ;
- (d) visitors ;
- (e) cargo and stores ; and
- (f) law enforcement officers and emergency providers.

(6) *Cargo Operations* : Cargo security and control measures shall be implemented to—

- (a) prevent cargo tampering ; and
- (b) track cargo for loading, and discharge.

(7) *Cargo Operations* : Security personnel shall ensure that containers are shut and sealed and check the container numbers against ship's manifest before the containers are loaded aboard.

(8) *Cargo Operations* : Signs of tampering or damage shall be referred to the Ship Security Officer, Master and Port Security Officer for investigation and co-ordination with the appropriate law enforcement authorities.

(9) *Ship's Stores* : Ship's stores shall be—

- (a) documented in advance ;
- (b) coordinated with ship ;
- (c) inspected upon arrival at the ship ; and
- (d) accepted or received by a member of ship's crew.

(10) *Passenger Procedures* : Security regulated passenger ships shall designate passenger access areas and passengers shall—

- (a) present valid ticket and travel authorizations ;
- (b) present valid identifications ; and
- (c) submit all bag-gages for screening.

Security
Obligations.

51.—(1) *International Ship Security Certificate (ISSC)* : A security regulated ship shall maintain a valid International Ship Security Certificate in accordance with SOLAS Chapter XI-2 and the Designated Authority shall verify and issue initial International Ship Security Certificates as allowed by law, and shall review International Ship Security Certificates periodically, at an interval not exceeding five years.

(2) *Communications and Reporting Procedures* : Prior to entering a port facility, an arriving ship shall provide the following information within the period specified by the Designated Authority—

- (a) International Ship Security Certificate (ISSC) status ;

- (b) current security level of the ship ;
- (c) details of last ten ships to port and ship to ship interface activities ;
- (d) ship location and estimated time of arrival ;
- (e) crew list ;
- (f) cargo description or manifest ; and
- (g) passenger list.

52.—(1) *Security Incidents* : A ship security incident shall be responded to, reported and managed in accordance with the ship security plan.

Incident
Response.

(2) *Unauthorized Access and Breach Procedures* : The following unauthorized access and breach procedures shall be upheld—

(a) in the event of a breach of security in a restricted area, a Ship Security Officer or his authorized delegate shall investigate and conduct a security sweep of the affected area ; and

(b) an individual gaining unauthorized access to the port facility from landside, waterside, or shipboard shall be apprehended and referred for administrative or criminal prosecution in accordance with these Regulations.

(3) *Stowaway Procedures* : A regulated ship shall employ the following stowaway prevention and detection measures as applicable—

(a) securely fasten and lock doors, hatchways, storerooms, equipment lockers, cargo hatches, engine rooms and crew or passenger accommodations ;

(b) fit plates over anchor hawse pipes ;

(c) ensure that accommodation doors are secured and locked, leaving only one open entrance and in the interest of safety, keys to the locked doors are placed in convenient positions so that doors can be opened in the event of emergencies ;

(d) ensure that store rooms, equipment lockers on deck, the engine room and the accommodations remain locked throughout a port call ;

(e) establish a gangway watch ;

(f) inspect areas that cannot be locked on a regular basis ; and

(g) ensure that a detected stowaway is immediately reported to the appropriate authorities but where a stowaway is be violent, direct engagement is discouraged so that the safety and security of the ship and its crew may not be compromised.

(4) *Best Management Practices* : Pursuant to the ISPS Code, a ship security plan shall include security measures to protect against incidents of piracy, armed attacks, including armed robbery, hijacking or terrorism that meet internationally accepted Best Management Practices (BMP) at a minimum, and the Designated Authority's specifications and requirements.

PART VI—PORT FACILITY SECURITY

Port Facility
Security
Officer
(PFSO).

53. Subject to these Regulations, operators of port facilities shall appoint a Port Facility Security Officer to implement and administer these Regulations, subject to the approval of the Designated Authority.

Qualifications
of a Port
Facility
Security
Officer
(PFSO).

54.—(1) A port facility operator shall ensure that the Port Facility Security Officer is qualified to perform delegated duties.

(2) The minimum qualification for appointment as a PFSO shall be as follows—

- (a) a University degree or its equivalent ;
- (b) five years cognate experience in a security related position ; and
- (c) an ISPS Code certification by the Designated Authority or its accredited training institution.

Duties of a
Port Facility
Security
Officer
(PFSO).

55. A Port Facility Security Officer shall—

- (a) co-ordinate security measures with interfacing security regulated ships ;
- (b) ensure the development, submission and implementation of required security plans ;
- (c) conduct port facility security drills and exercises ;
- (d) conduct port facility security inspections ;
- (e) ensure adequate port facility security personnel training ;
- (f) maintain records as required by these Regulations ;
- (g) ensure the execution of any required Declarations of Security ;
- (h) notify law enforcement personnel and other emergency responders of applicable port facility security incidents ; and
- (i) ensure that all security measures and protocols set forth in these Regulations are implemented and enforced.

Powers of a
Port Facility
Security
Officer
(PFSO).

56. A Port Facility Security Officer shall have the power to—

- (a) enter any area of the port facility or board a ship to make inquiries, examinations, inspections, confiscations and detentions in accordance with these Regulations ;
- (b) request Declarations of Security of ships on the instructions of the Port Security Officer ; and
- (c) implement any security measure or protocol as may be required by these Regulations.

57. The appointment of a Port Facility Security Officer shall be revoked where he fails to meet the requirements of these Regulations or the terms of the contract of his appointment.

Revocation
of a Port
Facility
Security
Officer's
(PFSO's)
Appointment.

58. *Screening Requirements* : A Port Facility security personnel shall be subjected to a background records check in accordance with the Port Facility's administrative procedures.

Port Facility
Security
Personnel.

59. A security personnel or organization governed by these Regulations shall demonstrate expertise in the following areas of ship and port security—

Basic Port
Security
Knowledge.

- (a) basic security organization ;
- (b) ship and port facility security measures ;
- (c) emergency preparedness and response ;
- (d) basic security equipment and systems ;
- (e) inspections, patrol, and monitoring techniques ;
- (f) law enforcement responsibilities ;
- (g) basic security related communications ;
- (h) current security level ;
- (i) recognizing and detecting potentially dangerous substances and devices ;
- (j) recognizing behavioural patterns of persons who are likely to threaten security ;
- (k) basic techniques used to circumvent security measures ;
- (l) conducting physical searches and non-intrusive inspections ; and
- (m) basic security drills and exercises.

60.—(1) A security guard shall be a person who is—

Security
Guards.

(a) employed by the port or port facility or a guard force company to perform security duties ; and

(b) not a law enforcement officer.

(2) A security guard shall possess the following qualifications—

- (a) complete the training as required by the Designated Authority ; and
- (b) basic port security skills and knowledge as set forth in these Regulations.

(3) While on duty, a security guard shall dress in accordance with safety and security standards and possess valid identification as specified by the Designated Authority.

(4) Security guards shall—

- (a) enter a regulated security area, or any building, vehicle, or place in any part of a regulated security area, for the purpose of exercising or

executing his powers, functions, and duties under these Regulations ;

(b) enter any ship for the purpose of exercising or executing his powers, functions, and duties under these Regulations, where they have been specifically designated as onboard security by the Port Security Officer ;

(c) visually and physically search persons, vehicles, vessels, cargo, stores and bag-gages on or entering into a restricted zone ;

(d) require any person found in a restricted zone to produce an identification and state his reasons for being there ;

(e) compel unauthorized persons, vehicles and vessels to be removed from a restricted zone ;

(f) detain and frisk a person where a security guard reasonably suspects that the person is committing, or has committed an offence ;

(g) upon detaining a person under paragraph (f) of this sub-regulation, the detained person shall be handed over to the Nigeria Police within reasonable time ;

(h) seize any item for the purpose of determining whether the item may lawfully be taken on board a ship or into a restricted zone ;

(i) cause to destroy or dispose of items which pose an imminent safety or security risk ; and

(j) use minimum force necessary to carry out assigned duties.

Training,
Security
Awareness,
Drills and
Exercises.

61.—(1) The following procedure shall regulate training—

(a) the Designated Authority shall be responsible for reviewing and approving curricula for all ISPS Code training ;

(b) the Designated Authority shall provide the training under paragraph (a) of this sub-regulation where necessary ; and

(c) the Port Facility Security Officer shall be responsible for ensuring that security awareness is maintained in the facility at all times.

(2) *Drills* : Security drills shall be conducted at least once every three months to test the scenarios developed from the contents of the port facility security plan.

(3) *Exercises* : Security exercises shall be conducted once every year to test the effectiveness of the port facility security plan and security exercises may either be full scale or tabletop simulation.

Physical
Security.

62.—(1) *Restricted Area Designation* : Port Facilities shall designate restricted areas to control access to—

(a) the ship to port interface ;

(b) cargo facilities ;

(c) passenger facilities ;

- (d) critical infrastructure ; and
- (e) security administration facilities.

(2) *Fixed and Moving Security Zones* : The Port Facility may designate fixed and moving security zones to address specific security requirements in and adjacent to the port facility and its approaches.

(3) *Restricted Area Access* : A person shall not enter a port facility restricted area or security zone except by permission of the Port Facility Security Officer, the port facility operator or his authorized delegate.

(4) *Perimeter* : A port facility shall establish a controlled perimeter around restricted areas and control measures may include fencing and natural barriers and shall—

- (a) define the restricted area ;
- (b) deter unauthorized entry ;
- (c) delay unauthorized entry ; and
- (d) identify access control points.

(5) Perimeter integrity shall be verified at least once per security shift.

(6) *Signage* : The port facility shall install signage clearly identifying all restricted areas, current security level and other relevant security related instructions to interfacing ships, passengers, crew and visitors to the facility and a signage shall be visible from the landside perimeter and waterside approaches at all times.

(7) *Access Points* : Port facility security shall control all port facility access points when in use and secure access points when not in use against access by unauthorized persons and vehicles.

(8) *Communications* : A Port Facility Security Officer shall have the means to effectively communicate with ship and port facility security personnel, law enforcement authorities and emergency response authorities, and provide notification of changes in security conditions at the facility.

(9) *Surveillance* : A Port Facility Security Officer shall ensure continued monitoring of—

- (a) the port facility and its approaches ;
- (b) restricted areas within the port facility ; and
- (c) ships at the port facility and areas surrounding the ships.

63.—(1) *Access Control* : A port facility shall implement access control procedures as specified in the Port Facility Security Plan for—

Operational
Security.

- (a) regular users ;
- (b) service providers ;
- (c) ship's crew ;

- (d) passengers ;
- (e) visitors ;
- (f) vehicles ;
- (g) cargo and ship's stores ; and
- (h) law enforcement officers and emergency responders.

(2) *Identification Requirements* : The following identification requirements shall be adhered to—

(a) all persons gaining entry to a port facility shall hold an identification card as required by these Regulations and be authorized to be in the area ;

(b) a Port Security Officer may issue an identification card to a regular user only upon a successful completion of a background records check ;

(c) a port facility identification card shall be denied or revoked where a —

(i) person has been convicted of a felony,

(ii) Port Security Officer reasonably believes a person to be a terrorism security risk, or

(iii) person has caused a port facility security incident ;

(d) that a port facility identification card shall at a minimum, meet the following requirements—

(i) be laminated or otherwise secure against tampering ;

(ii) contain the individual's full name - full first and last names, middle initial is acceptable ;

(iii) contain a photograph that accurately depicts the individual's current appearance or other suitable biometric ; and

(iv) bear the name of the issuing authority ;

Regular
Users.

64. Regular users gaining entry to the port facility shall—

(a) present valid port facility identification to access control personnel ;

(b) be authorized to be in the area which access is gained ;

(c) be in the course and scope of his duties ; and

(d) be screened and searched.

Service
Providers.

65. Service providers gaining entry to the port facility shall—

(a) be pre-approved ;

(b) be verified by the requesting port, ship or organization ;

(c) present valid identification ;

(d) be screened and searched ; and

(e) be escorted at all times within the port facility by the requesting port, ship or organization.

66. A ship's crew gaining entry to a port facility shall—

Ship's Crew.

- (a) be pre-approved ;
- (b) present valid identification ;
- (c) be screened by the Customs and Immigration ;
- (d) be screened and searched ; and
- (e) be escorted at all times within the port facility.

67. Visitors gaining entry to the port facility shall—

Visitors.

- (a) be pre-approved ;
- (b) present valid identification ;
- (c) be screened and searched ;
- (d) be issued a visitor's pass ; and
- (e) be escorted at all times within the port facility.

68. The following guidelines shall be observed by vehicles—

Vehicles.

- (a) a vehicle entering a port facility shall be searched and screened ;
- (b) drivers and passengers of vehicles shall produce valid identification as required by the port facility security plan ; and
- (c) a port facility security shall immediately notify security agencies of the presence of any unauthorized vehicle left unattended within or around the port facility.

69.—(1) To enter a security regulated port facility, a Law Enforcement Officer or emergency responder shall—

Law
Enforcement
or Emer-
gency
Responders.

- (a) be in the course and scope of his duties ;
- (b) identify himself as a Law Enforcement Officer ; and
- (c) notify Security Personnel as to the reason for access.

(2) A Law Enforcement Officer or responder shall present identification issued by his Agency for access, when not responding to an emergency.

70. A person gaining unauthorised access to a port facility from a landside, waterside, or shipboard shall be apprehended and referred for administrative sanction or criminal prosecution in accordance with these Regulations.

Unauthorised
Access
Procedures.

71.—(1) Cargo security and control measures shall be implemented to—

Cargo
Operations.

- (a) prevent cargo tampering ; and
- (b) track cargo for storage, stacking, loading, and discharge.

(2) A port security personnel shall ensure that containers are shut and sealed and check the container numbers against ship's manifest before containers are moved to the loading area.

(3) Signs of tampering or damage shall be referred to the Port Security Officer or Port Facility Security Officer for investigation and co-ordination with the appropriate law enforcement authority.

Ship's
Stores.

72. Ship's stores shall be—

- (a) documented in advance ;
- (b) co-ordinated with ship ;
- (c) inspected upon arrival at the port facility by relevant security officials ;
- (d) escorted to and from ship ; and
- (e) accepted or received by a member of ship's crew.

Passenger
Procedures.

73. A passenger shall—

- (a) present valid ticket and travel authorizations ;
- (b) present valid identification ;
- (c) be screened by Customs and Immigration officials ;
- (d) escort, label, and submit all bag-gages for screening ;
- (e) be segregated from all other port facility activities ; and
- (f) be further segregated by embarkation or debarkation class.

Primary
Ship and
Port
Interface
Security
Information.

74. Prior to entering a port facility, the Port Facility Security Officer or his authorized delegate shall notify arriving ships of—

- (a) the current port security level ; and
- (b) Port Security Officer and Port Facility Security Officer's contact information.

Incident
Response.

75.—(1) Port Security Incidents shall be regulated by the following guidelines—

(a) a port security incident is any occurrence resulting in the violation of any port security regulation within the geographical boundaries of the port security authority ;

(b) a major port security incident is any occurrence resulting or likely to result in the—

(i) introduction of weapons, explosives or security prohibited items into a port facility or aboard a ship adjacent to a port facility,

(ii) infiltration of terrorists or hostile persons into the port facility or aboard a ship adjacent to a port facility,

(iii) destruction of, damage to, or tampering with port facility property or ships or cargo within or adjacent to the port facility,

(iv) non-accidental death or personal injury within a port facility or aboard a ship adjacent to a port facility ; or

(v) unauthorized breach of the ship to port interface ; and

(c) a minor port security incident is any violation other than a major port security incident.

(2) *Security Threats* : Threats of major security incidents shall be deemed major security incidents and threats shall be classified as either 'GENUINE', in which case appropriate response procedures are to be implemented; or 'HOAX', in which case no further action other than to report the incident to the Designated Authority is necessary.

(3) *Incident Reporting Requirements* : An authorized user of a port facility is obligated to immediately report known or suspected violations of port security regulations and activities of a suspicious nature to a port security authority.

(4) *Major Incident Response* : Upon notification of a major security incident, the Port Security Officer and Port Facility Security Officer shall notify the Designated Authority and security agencies and co-ordinate incident response measures in accordance with incident response procedures set forth in the Port Security Plan and Port Facility Security Plan respectively.

(5) *Minor Incident Response* : Upon notification of a minor security incident, the Port Security Officer and Port Facility Security Officer shall respond in accordance with the procedures set forth in the Port Security Plan and Port Facility Security Plan respectively.

(6) *Weapons of Mass Destruction Response* : Upon notification of the threat or existence of chemical, biological, or radiological (CBR) weapons of mass destructions within a port facility or in, on or aboard a cargo or ship in or adjacent to a port facility, a Port Security Officer or Port Facility Security Officer shall notify the Designated Authority and initiate emergency procedures in accordance with the procedures set forth in the Port Security Plan and Port Facility Security Plan respectively.

PART VII—ENFORCEMENT

76.—(1) *Law Enforcement Officers* : For the purpose of these Regulations, a law enforcement officer means an officer of the Nigeria Police Force and a law enforcement officer shall enforce criminal laws and make arrests for violations of these Regulations within security regulated port facilities and aboard security regulated ships and may exercise general law enforcement authority. Authorities.

(2) *Authority of Law Enforcement Officers* : Where a law enforcement officer reasonably believes that it is necessary to do so for the purposes of safeguarding against unlawful interference with maritime transport or offshore facilities, he may exercise a lawful authority provided for in statutes, including, but not limited to—

- (a) investigate a suspected offence under these Regulations ;
- (b) enter a regulated security area, or any building, vehicle, or place in any part of a regulated security area, or any ship, for the purpose of exercising and executing his powers, functions, and duties under these Regulations ;
- (c) stop and conduct a search of a person within a restricted zone ;
- (d) stop and search a vehicle within a restricted zone ;
- (e) make inquiries, examinations, inspections, searches, seizures, and arrests ;
- (f) arrest a person suspected of committing an offence subject to any other lawful appropriate action ;
- (g) remove a person, vehicle or vessel which has entered the restricted zone without authority ;
- (h) prevent a person, vehicle or vessel that has entered a restricted zone without authority, from leaving the zone ;
- (i) seize an item for the purpose of determining whether the item may lawfully be taken on board that ship or into a restricted zone ;
- (j) destroy or dispose of any item which poses an imminent safety or security risk ;
- (k) enforce moving or fixed safety or security zones established pursuant to law ;
- (l) conduct high speed intercepts ; and
- (m) carry out such other security mission on a port facility as may be required by the Designated Authority considered necessary for the attainment of the purpose of these Regulations.

(3) *Guard Force Company* : A Guard Force Company shall, subject to the provisions of regulation 60 of these Regulations, exercise the necessary authority for the implementation of these Regulations.

(4) *Master's Power to Detain* : A Master of a ship may detain a person onboard the ship, within a reasonable time, in the interest of security.

Control
Measures.

77.—(1) *Fixed and Moving Security Zones* : A port facility may designate fixed and moving security zones to address specific security requirements in and adjacent to the port facility and its approaches.

(2) *Ship Control Measures* : The following ship control measures shall be adhered to—

- (a) a Port Security Officer or Port Facility Security Officer shall implement ship control measures where a—
 - (i) ship fails to comply with the requirements of these Regulations,
 - (ii) ship presents a serious security risk, or

(iii) ship has failed to provide all the requested security-related information ;

(b) in the event of any of the above listed in paragraph (a) of this sub-regulation occurring, a Port Security Officer or Port Facility Security Officer shall implement the following control measures—

- (i) inspect the ship,
- (ii) request the ship to rectify the non-compliance,
- (iii) delay the ship,
- (iv) detain the ship,
- (v) restrict the operations of the ship, including its movement within the port,
- (vi) expel the ship from the port,
- (vii) deny the ship entry into the port, or
- (viii) execute an administrative sanction ; and

(c) any ship control measure implemented shall be reported to the Designated Authority, Flag State and the International Maritime Organization.

(3) *Conditions of Entry* : A Port Security Officer or Port Facility Security Officer may where necessary, impose any of the following conditions of entry on ships entering the port facility—

- (a) movement restrictions ;
- (b) increased security measures ;
- (c) execution of a Declaration of Security ; or
- (d) such other condition of entry as may be applicable in the circumstance.

(4) *Administrative Remedies for Ships* : Where an owner, agent, master, officer, or person in charge of a ship is liable for a penalty under these Regulations, the Designated Authority may—

- (a) revoke any license or certificate issued in respect to the ship, with or without prejudice to the issuance of a subsequent license ;
- (b) suspend a license issued in respect to the ship for a period of time considered appropriate by the Designated Authority ;
- (c) deny a license issued in respect to the ship ;
- (d) impose additional conditions and restrictions on any license issued in respect to the ship ; or
- (e) refuse or revoke the clearance issued in respect to the ship, required for entry into a port facility.

(5) *Administrative Remedies for Port Facilities* : Where a port facility owner or operator is liable for a penalty under these Regulations, the Designated Authority may—

(a) revoke any license or certificate issued in respect to the facility, with or without prejudice to the issuance of a subsequent license or certificate ;

(b) suspend a license or certificate issued in respect to the facility for a period of time considered appropriate by the Designated Authority ;

(c) deny a license or certificate issued in respect to the facility ;

(d) impose additional conditions and restrictions on any license or certificate issued to such a facility ; or

(e) suspend or withdraw the approved security plan and statement of compliance, issued in respect of such a facility.

(6) *Administrative Remedies for Persons* : Where a person is liable for a penalty under these Regulations, the Designated Authority may—

(a) revoke any license issued in respect to the person, with or without prejudice to the issuance of a subsequent license ;

(b) suspend a license issued in respect to the person, for a period of time considered appropriate by the Designated Authority ;

(c) deny any license issued in respect to the person ;

(d) impose additional conditions and restrictions on any license issued in respect to the person ; or

(e) impose a fine on the person.

PART VIII—OFFENCES AND PENALTIES

General.

78. The violation of a provision of these Regulations, the commission of an activity proscribed by these Regulations or the failure to perform a positive action required by these Regulations shall be an offence punishable under these Regulations.

Administrative
Violations.

79.—(1) *Failure to implement and maintain a security plan* : A regulated entity which operates without a valid security plan as required by these Regulations commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of one million naira per day for a ship ;

(b) a fine not exceeding the sum of two million, five hundred thousand Naira per day for a port facility ;

(c) withdrawal of maritime services ;

(d) ship seizure and detention ;

(e) revocation of operating license, International Ship Security Certificate, or Statement of Compliance, as may be applicable ; and

(f) facility closure where the violation persists for more than three calendar months despite written warnings from the Designated Authority.

(2) *Failure to Conduct Training, Drills and Exercises* : A regulated entity which fails to conduct training, drills and exercises as required by these Regulations, commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of five hundred thousand naira per day for a ship ;

(b) a fine not exceeding the sum of one million naira per day for a port facility ;

(c) withdrawal of maritime services ;

(d) ship seizure and detention ;

(e) revocation of operating license, International Ship Security Certificate or Statement of Compliance, as may be applicable ; and

(f) facility closure where the violation persists for more than three calendar months despite written warnings from the Designated Authority.

(3) *Failure to implement and maintain physical security measures* : A regulated entity which fails to implement and maintain all physical security measures as required by these Regulations, commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of five hundred thousand naira per day for a ship ;

(b) a fine not exceeding the sum of one million naira per day for a port facility ;

(c) withdrawal of maritime services ;

(d) ship seizure and detention ;

(e) revocation of operating license, International Ship Security Certificate or Statement of Compliance, as may be applicable ; and

(f) facility closure where the violation persists for more than three calendar months despite written warnings from the Designated Authority.

(4) *Failure to implement and maintain operational security measures* : A regulated entity which fails to implement and maintain all operational security measures as required by these Regulations, commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of five hundred thousand naira per day for a ship ;

(b) a fine not exceeding the sum of one million naira per day for a port facility ;

(c) withdrawal of maritime services ;

(d) ship seizure and detention ;

(e) revocation of operating license, International Ship Security Certificate or Statement of Compliance, as may be applicable ; and

(f) facility closure where the violation persists for more than three calendar months despite written warnings from the Designated Authority.

(5) *Failure to maintain Security Records* : A regulated entity which fails to maintain security records as required by these Regulations, commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of five hundred thousand naira per day for a ship ;

(b) a fine not exceeding the sum of one million naira per day for a port facility ;

(c) withdrawal of maritime services ;

(d) ship seizure and detention ;

(e) revocation of operating license, International Ship Security Certificate or Statement of Compliance, as may be applicable ; and

(f) facility closure where the violation persists for more than three calendar months despite written warnings from the Designated Authority.

(6) *Failure to Meet Audit Requirements* : A regulated entity which fails to meet audit requirements as required by these Regulations, commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of five hundred thousand naira per day for a ship ;

(b) a fine not exceeding the sum of one million naira per day for a port facility ;

(c) withdrawal of maritime services ;

(d) ship seizure and detention ;

(e) revocation of operating license, International Ship Security Certificate or Statement of Compliance, as may be applicable ; and

(f) facility closure where the violation persists for more than three calendar months despite written warnings from the Designated Authority.

(7) *Operating Ships without Valid International Ship Security Certificates* : A regulated entity which fails to operate a regulated ship that does not possess a valid International Ship Security Certificate (ISSC), commits an administrative violation, punishable by—

(a) a fine not exceeding the sum of five million naira ; and

(b) ship seizure and detention.

(8) *Failure of a Ship to comply with Security Directions* : A ship, commercial or recreational boat which fails to comply with security directions issued by the Designated Authority, commits an administrative violation, punishable by—

- (a) a fine not exceeding three hundred thousand naira ;
- (b) ship or boat seizure and detention ; and
- (c) revocation of international ship security certificate or statement of compliance.

(9) *Failure to Maintain SSAS, AIS or LRIT* : A regulated ship which fails to maintain its ship's Security Alert System (SSAS), Automatic Identification System (AIS) or Long Range Identification and Tracking (LRIT), as required by these Regulations, commits an administrative violation, punishable by—

- (a) a fine not exceeding the sum of one million naira per violation ;
- (b) ship seizure and detention ; and
- (c) revocation of international ship security certificate or statement of compliance.

(10) *Violations by recognized security organizations* : A Recognized Security Organization (RSO) which sets security levels, approves ship or port facility security assessments, approves ship or port facility security plans, or exercises ship control and compliance measures or any other action in violation of the terms of its engagement as an RSO, commits an administrative violation, punishable by—

- (a) a fine not exceeding the sum of three million naira per violation ; and
- (b) revocation of an RSO certification.

PART IX—MISCELLANEOUS

80. In these Regulations, terminologies conform to definitions set forth in the International Ship and Port Facility Security (ISPS) Code and the relevant Laws of the Federal Republic of Nigeria as applicable. Interpretation.

81. These Regulations may be cited as the Nigerian Maritime Administration and Safety Agency (International Ship and Port Facility Security Code Implementation) Regulations, 2014. Citation.

MADE at Abuja this 18th day of November, 2014.

SENATOR IDRIS AUDU UMAR
Honourable Minister of Transport

EXPLANATORY NOTE

*(This note does not form part of these Regulations but
is intended to explain its purport)*

These Regulations establish a legal guideline for the implementation of the International Ship and Port Facility Security (ISPS) Code in the Federal Republic of Nigeria ; implement and enforce the provisions the ISPS Code as adopted by the International Maritime Organization (IMO) and appoint the Nigerian Maritime Administration and Safety Agency (NIMASA), as the Designated Authority to oversee the implementation, application, administration and management of these Regulations with respect to ships and port facilities.