Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 697 28 July / Julie 2023 No. 49045

ISSN 1682-5845

9 771682 584003 49045

Contents

No.		Gazette No.	Page No.
GOVERNMENT NOTICES • GOEWERMENTSKENNISGEWINGS			
Civilian Secretariat for the Police Service / Burgerlike Sekretariaat vir die Polisiediens			
3732	Critical Infrastructure Protection Act (8/2019): Critical Infrastructure Protection Regulations, 2023	49045	3

CIVILIAN SECRETARIAT FOR THE POLICE SERVICE

NO. 3732 **28 July 2023**

INVITATION FOR PUBLIC COMMENTS:

CRITICAL INFRASTRUCTURE PROTECTION REGULATIONS, 2023

1. Notice is hereby given that the attached Critical Infrastructure Protection Regulations, 2023 ("draft Regulations") are published for public comments.

2. Interested persons can also visit the website of the Civilian Secretariat for Police Service at http://www.policesecretariat.gov.za for –

   (i) A Copy of the draft Regulations; and
   (ii) Application Forms I, II, III, IV, V, VI.

3. All interested persons and organisations are invited to submit written comments no later than 1 September 2023 by -

   (i) email to: Jacob.Setouto@csp.gov.za

   (ii) posting comments to:
   Acting Secretary for Police Service
   for attention of Mr M. Ntwana at:
   Civilian Secretariat for Police Service
   Private Bag x 922
   PRETORIA
   0001

   (iii) Hand delivery at the Civilian Secretariat for Police Service at Fedsure Forum Building, 2nd Floor, Corner of Pretorius and Lilian Ngoyi Street, Pretoria.

4. Kindly provide the name, postal and email address, telephone and fax number of the person or organization submitting the comments.
5. Enquiries regarding access to a copy of the draft Regulations may be made to Mr Jacob Setouto via the following email address: Jacob.Setouto@csp.gov.za

SCHEDULE

ARRANGEMENT OF REGULATIONS

CHAPTER 1

INTERPRETATION AND APPLICATION OF REGULATIONS

1. Definitions

CHAPTER 2

FUNCTIONING AND MEETING PROCEDURE OF CRITICAL INFRASTRUCTURE COUNCIL

2. Establishment and functions of Critical Infrastructure Council
3. Ordinary meetings of Critical Infrastructure Council
4. Special meeting of the Critical Infrastructure Council
5. Resolutions of the Critical Infrastructure Council in respect of application for declaration of infrastructure as critical infrastructure
6. Resolutions of the Critical Infrastructure Council to dispense with publication
7. Resolutions of the Critical Infrastructure Council in respect of policies, protocols and standards
8. Assignment of functions by Minister
9. *Ad hoc* committees
10. Standing committees

CHAPTER 3

ORGANISATIONAL STRUCTURES TO SUPPORT THE NATIONAL COMMISSIONER

11. Establishment of Critical Infrastructure Protection Regulator
12. Functions of the Critical Infrastructure Protection Regulator

13. Identification of infrastructure for possible declaration as Critical Infrastructure
14. Assistance to person in control

CHAPTER 4

APPLICATION FOR DECLARATION AS CRITICAL INFRASTRUCTURE

15. Manner and format of application
16. Documents to accompany the application
17. Request for departure from provisions of section 17(4)*(a)* of Act
18. Application for declaration of government infrastructure by National Commissioner

CHAPTER 5

SYSTEM OF CATEGORISATING CRITICAL INFRASTRUCTURE IN LOW-RISK, MEDIUM RISK OR HIGH-RISK CATEGORY

19. System of categorising infrastructure in low-risk, medium-risk or high-risk category
20. Functions of the National Commissioner in respect of risk categorisation
21. Consideration of risk categorisation proposed by National Commissioner

CHAPTER 6

DECLARATION OF INFRASTRUCTURE AS CRITICAL INFRASTRUCTURE

22. Certificate of declaration as critical infrastructure
23. Critical Infrastructure register
24. Conditions that may be imposed by Minister in respect of physical security measures
25. Steps to be taken by the person in control after declaration as critical infrastructure
26. Failure to take steps after declaration as critical infrastructure

CHAPTER 7

ESTABLISHMENT, FUNCTIONS, FUNCTIONING, MEETING AND REPORTING PROCEDURE OF COMMITTEES AND FORUMS

27. Establishment of Joint Planning Committee
28. Functions of Joint Planning Committee
29. Chairperson of Joint Planning Committee
30. Inaugural meeting of Joint Planning Committee
31. Ordinary meetings of Joint Planning Committee
32. Special meeting of the Joint Planning Committee
33. Specific matters to be attended to by the Joint Planning Committee
34. Reporting by the Joint Planning Committee
35. Standing committees
36. *Ad hoc* committees
37. Critical Infrastructure Liaison Forum

CHAPTER 8

SECURITY POLICY AND PLAN

38. Definitions
39. Responsibility for security policy and plan
40. Security policy
41. Security plan
42. Access and egress control
43. Security awareness and preparation
44. Quality assurance
45. Incident response
46. Incident response simulation exercises

CHAPTER 9

INSPECTIONS

47. Designation of inspectors
48. Inspections
49. Physical Security Assessment
50. Physical Security Audit
51. Physical Security Evaluation
52. Compliance notices
53. Written notices

CHAPTER 10

SECURITY PERSONNEL

54. Definitions
55. Security manager
56. Control security officer
57. Security personnel and security service providers
58. Application for certificate of competence to render security services at critical infrastructure
59. Qualifications and requirements
60. Disqualifications
61. Security equipment
62. Security Operations Centre
63. Occurrence Book and registers
64. Powers of arrest
65. Directive in respect of search of persons body
66. Refusal for examination or search
67. Dangerous objects
68. Prohibited objects
69. Search of arrested person

CHAPTER 11

GENERAL PROVISIONS

70. Offences and Penalties
71. Manner of service of notice
72. Repeal
73. Commencement

CHAPTER 1

INTERPRETATION AND APPLICATION OF REGULATIONS

1. Definitions

In these regulations, unless the context indicates otherwise—

"applicant" means:

(a) a person in control of infrastructure who submits an application for declaration of that infrastructure as critical infrastructure in terms of section 17(1) of the Act; or

(b) the National Commissioner when he or she submits an application for declaration of that infrastructure as critical infrastructure in terms of section 18(1) of the Act;

"application" means an application contemplated in section 17 or 18 of the Act to have infrastructure declared as critical infrastructure by the Minister in terms of section 20 of the act;

"application form" means the form referred to in regulation 15(1);

"compliance notice" means a compliance notice contemplated in section 11(3) of the Act;

"Council" means the Critical Infrastructure Council established in section 4(1) of the Act;

''Critical Infrastructure Council'' means the Critical Infrastructure Council established in terms of section 4 of the Act, and **''Council''** has a corresponding meaning;

"Critical Infrastructure Protection Regulator" means the Critical Infrastructure Protection Regulator that must be established in terms of regulation 11, and **"Regulator"** has a corresponding meaning;

"dangerous object" means any object that represents a threat to the safety or security of critical infrastructure or any person present at such critical infrastructure and includes an object which resembles such dangerous object;

"incident" means any threat that realises where such an event may prejudicially affect the security of that critical infrastructure;

"official regulatory authority" means any regulatory authority or entity established by an Act of Parliament or in terms of an obligation of the Republic under any international instrument;

"preliminary physical security assessment" means a preliminary physical security assessment contemplated in regulation 14(2);

"process-based security management system" means a security management system that views security management as a collection of key activities managed to achieve an acceptable level of assurance that critical infrastructure is secure;

"prohibited object" means any prohibited object in respect of which a direction has been issued in terms of subsection 25(1)(b) of the Act and includes an object which resembles such dangerous object;

"risk categorisation" means a process in terms of which critical infrastructure is categorised in a low-risk, medium-risk, or high-risk category in accordance with Chapter 5 ;

"Security Operations Centre" means a centralised facility from where security measures of critical infrastructure are monitored to detect and analyse incidents and to initiate and coordinate a response thereto, and **"SOC"** has a corresponding meaning;

"security policy" means a framework for the development of organizational physical security standards; and

"the Act" means the Critical Infrastructure Protection Act, 2019 (Act No. 8 of 2019);

"threat" bears the same meaning as in the Act;

"written notice" means a written notice contemplated in section 11(4) of the Act.

CHAPTER 2

FUNCTIONING AND MEETING PROCEDURE OF CRITICAL INFRASTRUCTURE COUNCIL

2. Establishment and functions of Critical Infrastructure Council

(1) The Critical Infrastructure Council is established in terms of section 4(1) of the Act and must advise the Minister in an independent and impartial manner in the exercise of his or her functions in terms of the Act.

(2) The Council must have regard to its primary functions as set out more fully in section 7(1) of the Act.

3. Ordinary meetings of Critical Infrastructure Council

(1) The Chairperson of the Critical Infrastructure Council must, in order to comply with section 8(1) of the Act, ensure that the Council meets quarterly by notifying each member appointed in terms of section 4 of the Act in writing no less than 30 days before the date of such meeting.

(2) The notification referred to in subregulation (1) must include the venue, date and time of such meeting and must be accompanied by the minutes of the previous preceding meeting of the Council, as well as an agenda of the business to be considered at such meeting.

(3) At each meeting of the Council the venue, date and time for the subsequent meeting may be determined by consent, failing which the Chairperson may determine such a venue, date and time after consultation with the members.

(4) A copy of any—

(a) application for declaration of infrastructure as critical infrastructure referred to in section 7(1)*(a)* of the Act;

(b) request referred to in section 17(5) of the Act to dispense with publication in terms of section 17(4)*(a)* of the Act;

(c) proposed policies, protocols or standards referred to in section 7(1)*(b)* of the Act; or

(d) assignment of functions by the Minister referred to in section 7(1)*(c)* of the Act,

that will be discussed during an ordinary meeting of the Council, must accompany the notification referred to in subregulation (1).

(5) The Chairperson must ensure that the documents referred to in subregulation (4) are adequately sealed or, in the case of electronic documents, protected by means of a unique password in order to protect the confidentiality thereof.

(6) The Council determines its own rules of debate subject to subregulations (8) to (17).

(7) Seven members of the Council, which must include the chairperson or deputy chairperson, will constitute a quorum at any meeting of the Council as provided for in section 8(5) of the Act.

(8) The first act of an ordinary meeting, after being constituted, is to read and confirm by the signature of the Chairperson the minutes of the last preceding ordinary meeting and of any special meeting subsequently held. The meeting may consider the minutes as read, provided that objections or proposed amendments to the minutes of the last preceding ordinary or special meeting are raised and decided upon before confirmation of the minutes.

(9) The meeting must deal with the business of which notice has been given and any other business which a majority of the total membership of the Council agrees to consider.

(10) Every motion must be seconded and must, if the chairperson requires this, be in writing and a motion that is not seconded falls away.

(11) Except where the Act requires a different procedure, and where consensus cannot be reached, each question must be decided by the majority of votes of the members present and voting and unless the meeting decides otherwise, voting must be by show of hands.

(12) Should the majority of members present abstain from voting, the matter to be decided on must be deferred to the next meeting.

(13) The Chairperson may, in the case of any procedural matter or any matter not contemplated in section 7(1) of the Act, refer such matter by letter or electronic means for consideration by members of the Council.

(14) When a majority of the members of the Council reaches agreement on a matter referred to in subregulation (13) without convening a meeting, such resolution is equivalent to a resolution of the Council and must be recorded in the minutes of the subsequent ordinary meeting.

(15) The views of a member of the Council who is unable to attend a meeting may be submitted to the meeting in writing for consideration but may not count as a vote of such member.

(16) The number of members voting for or against a motion, as well as the number of members abstaining from voting, must be recorded in the minutes, and at the request of any member the Chairperson must direct that the vote of such member be likewise recorded.

(17) The ruling of the Chairperson on any question of order or procedure is binding unless immediately challenged by a member, in which event such ruling must be submitted for discussion to the meeting whose decision is final.

(18) The Council may, on an *ad hoc* basis, invite persons or entities who are not members but with a direct interest in a matter before the Council, to attend meetings and allow them to take part in discussions on the matters in which such a person has an interest, provided that they are not allowed to vote.

(19) The Chairperson may direct that an ordinary meeting of the Council be conducted on an electronic virtual platform.

4. Special meeting of the Critical Infrastructure Council

(1) The Chairperson of the Council—

(a) must convene a special meeting of the Council in terms of regulation 5(6) where any matter referred to in regulation 5(6), 6(7) or 8(1) must be considered; or

(b) must convene a special meeting of the Council in terms of section 8(3) of the Act at the written request of the Minister;

(c) may convene a special meeting of the Council in terms of section 8(3) or 8(4) of the Act where a matter that is to be discussed is of such an urgent nature that it should not be delayed until the next ordinary meeting.

(2) In the event that a special meeting of the Critical Infrastructure Council is required as contemplated in subregulation (1), the Chairperson must, in writing,

notify the members of the Council of the date, time, venue and purpose of such special meeting no less than 7 days, or within such reasonable period as the Chairperson may deem fit, prior to the date of such special meeting.

(3) The notification referred to in subregulation (1) must include the venue, date and time of such special meeting and must be accompanied by an agenda of the business to be considered at such special meeting.

(4) Any matter on the agenda of a special meeting must contain sufficient information to enable the members of the Council to adequately prepare for the special meeting.

(5) A member of the Council who is of the opinion that the agenda does not describe the matter in question sufficiently, may request further particulars from the Chairperson at least 3 days before the special meeting.

(6) The Chairperson may direct that a special meeting of the Council be conducted on an electronic virtual platform.

(7) A copy of any—

(a) application for declaration of infrastructure as critical infrastructure referred to in section 7(1)*(a)* of the Act;

(b) request for a departure from the provisions of section 17(4)*(a)* of the Act;

(c) proposed policies, protocols or standards referred to in section 7(1)*(b)* of the Act; or

(d) assignment of functions by the Minister referred to in section 7(1)*(c)* of the Act,

that will be discussed during a special meeting of the Council, must accompany the notification referred to in subregulation (2).

(8) The provisions of regulation 3(5) to 3(18) apply to special meetings with the changes required by the context.

5. Resolutions of the Critical Infrastructure Council in respect of application for declaration of infrastructure as critical infrastructure

(1) After consideration of an application for declaration of infrastructure as critical infrastructure referred to in section 7(1)*(a)* of the Act, the Council must adopt a resolution whether or not it intends to—

(a) recommend declaration of such infrastructure as critical infrastructure; and

(b) recommend an appropriate risk category for the infrastructure in question.

(2) The Council must record the intended recommendation that it is considering to adopt regarding the matter before the Council, subject to the following:

(a) where all the members of the Council move to adopt a resolution to recommend such matter, the Council must record the reasons for such recommendation;

(b) where the majority of the members of the Council move to adopt a resolution to recommend such matter, the Council must record reasons for such majority recommendation and allow each of the dissenting members to state his or her reasons for dissenting, which must likewise be recorded;

(c) where the majority of the members of the Council move to adopt a resolution not to recommend such matter, the Council must record reasons for such majority recommendation and allow each of the dissenting members to state his or her reasons for dissenting, which must likewise be recorded; or

(d) where all the members of the Council move to adopt a resolution not to recommend such matter, the Council must record reasons for such recommendation.

(3) The Council must, within 14 days of the meeting of the Council, notify the applicant of the intended recommendation of the Council referred to in subregulation (2).

(4) An applicant may, upon receiving a notification referred to in subregulation (3), make representations to the Council regarding the intended recommendation in respect of his or her application for declaration of infrastructure as critical infrastructure.

(5) The representations referred to in subregulation (4) must be lodged with the Chairperson of the Council within 30 days of receipt of the notification referred to in subregulation (3).

(6) The Council must, at a special meeting convened within 30 days after receipt of the representations, consider the representations of the applicant and adopt a final resolution whether or not to—

(a) recommend declaration of such infrastructure as critical infrastructure; and

(b) recommend the appropriate risk category for the infrastructure in question, and notify the applicant accordingly.

(7) The Chairperson must record any final resolution that the Council may adopt regarding a matter before the Council, subject to the following:

(a) where all the members of the Council move to adopt a final resolution to recommend such matter, the Council must record the reasons for such recommendation;

(b) where the majority of the members of the Council move to adopt a final resolution to recommend such matter, the Council must record reasons for such majority recommendation and allow each of the dissenting members to state his or her reasons for dissenting, which must be recorded;

(c) where the majority of the members of the Council move to adopt a final resolution not to recommend such matter, the Council must record reasons for such majority recommendation and allow each of the dissenting members to state his or her reasons for dissenting, which must be recorded; or

(d) where all the members of the Council move to adopt a final resolution not to recommend such matter, the Council must record reasons for such final resolution.

(8) The Chairperson must submit the application to the Minister for consideration accompanied by—

(a) the recommendation based on the final resolution of the Council referred to in subregulation (6)*(a),(b)* and where applicable *(c)*, together with the reasons referred to in subregulation (7) which must include the reasons recorded for any dissenting vote;

(b) any written comments made by interested persons in terms of section 17(4)*(a)*(ii) of the Act;

(c) the assessment of the National Commissioner in terms of section 17(4)*(b)* of the Act;

(d) any submissions made by the applicant regarding the risk category referred to in section 17(4)*(b)*(iv) of the Act;

(e) any submissions by the Head of a Government Department in terms of section 18(3)(b) of the Act; and

(f) any other representations made by the applicant or any other person in terms of section 19(3)*(b)* of the Act.

6. Resolutions of the Critical Infrastructure Council to dispense with publication

(1) Where an applicant requests the Council for approval to depart from the procedure of publication of the notice referred to in section 17(4)*(a)* of the Act, the Council must consider the request to determine whether the applicant showed good cause as contemplated in section 17(5) of the Act and adopt a resolution whether or not to approve such request.

(2) The Council must record the resolution adopted, subject to the following:

(a) where all the members of the Council move to approve that the procedure in section 17(4)*(a)* of the Act may be departed from, the Council must record the reasons for such resolution;

(b) where the majority of the members of the Council move to approve that the procedure in section 17(4)(a) of the Act may be departed from, the Council must record reasons for such majority resolution and allow each of the dissenting members to state his or her reasons for dissenting, which must likewise be recorded;

(c) where the majority of the members of the Council move that the procedure in section 17(4)*(a)* of the Act may not be departed from, the Council must record reasons for such intended majority resolution and allow each of the dissenting members to state his or her reasons for dissenting, which must likewise be recorded; or

(d) where all the members of the Council move that the procedure in section 17(4)*(a)* of the Act may not be departed from, the Council must record reasons for such intended resolution.

(3) Where the Council adopts a resolution in terms of subregulation (2)*(a)* or (2)*(b)* it must, within 14 days of the meeting of the Council—

(a) direct the National Commissioner to depart from the provisions of section 17(4)(a) of the Act; and

(b) notify the person in control accordingly.

(4) Where the Council intends adopting a resolution in terms of subregulation (2)*(c)* or (2)*(d)*, it must notify the applicant within 14 days of the meeting of the Council of its intention to deny the request.

(5) An applicant may, upon receiving a notification referred to in subregulation (4), make representations to the Council regarding his or her request to depart from the procedure referred to in section 17(4)*(a)* of the Act.

(6) The representations referred to in subregulation (4) must be lodged with the Chairperson of the Council within 30 days of receipt of the notification referred to in subregulation (3).

(7) The Council must, at a special meeting convened within 30 days after receipt of the representations, consider the representations of the applicant and adopt a final resolution whether or not to approve a departure from the procedure of publication of the notice referred to in section 17(4)*(a)* of the Act.

(8) The Chairperson must record any final resolution that the Council may adopt regarding a matter before the Council, subject to the following:

(a) where all the members of the Council move to adopt a final resolution to approve the request, the Council must record the reasons for such recommendation;

(b) where the majority of the members of the Council move to adopt a final resolution to approve the request, the Council must record reasons for such majority recommendation and allow each of the dissenting members to state his or her reasons for dissenting, which must be recorded;

(c) where the majority of the members of the Council move to adopt a final resolution not approve the request, the Council must record reasons for such majority recommendation and allow each of the dissenting members to state his or her reasons for dissenting, which must be recorded; or

(d) where all the members of the Council move to adopt a final resolution not to approve the request, the Council must record reasons for such final resolution.

(9) Where the Council adopts a resolution in terms of subregulation (7), it must, within 14 days of the meeting of the Council —

(a) direct the National Commissioner to either depart from or follow the provisions of section 17(4)(a) of the Act; and

(b) notify the applicant accordingly.

7. Resolutions of the Critical Infrastructure Council in respect of policies, protocols and standards

(1) Where the National Commissioner submits draft uniform standards, guidelines or protocols in terms of section 9(2) of the Act for approval by the Council in terms of section 7(1)*(b)* of the Act, the Council may consult any person or entity who, in the opinion of the Council, is sufficiently qualified and experienced to assist the Council.

(2) Any guideline in respect of a uniform standard, guideline or protocol approved by the Council in terms of section 7(1)*(b)* of the Act must be available on the website of the Civilian Secretariat for the Police Service within 14 days of the resolution, unless publication thereof may prejudice national security.

(3) Where the Council considers guidelines in respect of any policy affecting the functioning of the South African Police Service, the Civilian Secretariat for the Police Service must be consulted.

8. Assignment of functions by Minister

(1) Where the Minister has assigned any function on the Council in terms of section 7(1)*(c)* of the Act, the Chairperson may, within 14 days of receipt of the assignment, call a special meeting of the Council if he or she is of the opinion that the matter is urgent.

(2) In the event that the Council takes a resolution that the matter cannot be dealt with at such special meeting of the Council, the Council—

(a) may resolve to consult any person within 14 days of the resolution referred to in subregulation (1) who, in the opinion of the Council, is sufficiently qualified and experienced to assist the Council to perform such function;

(b) must inform the Minister of such resolution within 14 days after adopting such resolution; and

(c) report on such matter in the bi-annual report to the Minister contemplated in section 7(6) of the Act.

9. *Ad hoc* committees

(1) In order to function effectively and efficiently, the Council may, from time to time, adopt a resolution to designate suitably qualified and experienced members of the Council to form an *ad hoc* committee with a specific task to assist the Council in the performance of its functions.

(2) A resolution referred to in subregulation (1) must be in writing and clearly state—

(a) the terms of reference and task of the *ad hoc* committee;

(b) the name of the convener of the *ad hoc* committee;

(c) the names of members designated to serve on the *ad hoc* committee; and

(d) the expected timeframe within which the *ad hoc* committee is expected to complete the task assigned to it.

(3) An *ad hoc* committee need not reflect the composition of the Council as contemplated in sections 4(2)(b) and 4(2)(c) of the Act.

(4) The object of an *ad hoc* committee is to research a specific matter or collate information thereon and advise the Council on such matter for consideration at a meeting of the Council.

(5) An *ad hoc* committee must consider all relevant facts and factors pertaining to the matter and may, for this purpose, collate information, research any matter referred to it or consider any research that had previously been done on the subject matter, engage with any person or entity, or take any other reasonable action in the performance of the task assigned to it.

(6) After finalising a task assigned to it, an *ad hoc* committee must compile a report on the matter for submission to the Council for consideration within the timeframe referred to in subregulation (1)*(d)*.

(7) An *ad hoc* committee dissolves after completion of the task outlined in the terms of reference, unless the Council by resolution extends the timeframe referred to in subregulation (1)*(d)*.

(8) The Council is not bound by the report of an *ad hoc* committee.

10. Standing committees

(1) In order to function effectively and efficiently, the Council may, from time to time, adopt a resolution to designate suitably qualified and experienced members of the Council to form a standing committee to assist the Council in the performance of its functions.

(2) A resolution referred to in subregulation (1) must be in writing and clearly state—

(a) the terms of reference of the standing committee;

(b) the name of the convener of the standing committee; and

(c) the names of members designated to serve on the standing committee.

(3) A standing committee need not reflect the composition of the Council as contemplated in sections 4(2)*(b)* and 4(2)*(c)* of the Act.

(4) The object of a standing committee is to research or investigate matters of an ongoing nature or to collate information on standing matters related to its terms of reference and advise the Council on such matters for consideration at meetings of the Council.

(5) A standing committee must consider every matter and all relevant facts and factors pertaining to the matter and may, for this purpose, collate information, research any matter referred to it or consider any research that had previously been done on the subject matter, engage with any person or entity, or take any other reasonable action in the performance of the task assigned to it.

(6) A standing committee must, at each meeting of the Council, submit a report on its activities since the preceding meeting to the Council for consideration.

(7) A standing committee dissolves by resolution of the Council.

CHAPTER 3

ORGANISATIONAL STRUCTURES TO SUPPORT THE NATIONAL COMMISSIONER

11. Establishment of Critical Infrastructure Protection Regulator

(1) The National Commissioner must establish a Critical Infrastructure Protection Regulator as a component within the structures of the South African Police Service to ensure the maintenance of the administrative systems and procedures necessary for the implementation and enforcement of the Act as contemplated in section 9 of the Act.

(2) The National Commissioner must designate a police official of a rank not less than that of level 14 as the Head of the Regulator.

(3) Where the National Commissioner delegates any function to a police official in the Regulator in terms of section 14(5) of the Act, such police official must perform his or her functions strictly in accordance with any—

(a) limitations and conditions contained in the delegation; and

(b) National Instruction that the National Commissioner may issue from time to time.

12. Functions of the Critical Infrastructure Protection Regulator

(1) The Critical Infrastructure Protection Regulator is responsible for support to the National Commissioner in the performance of functions assigned to him or her in terms of the Act, and more specifically to:

(a) maintain the administrative systems and procedures necessary for the implementation and enforcement of the Act;

(b) support the National Commissioner in the administration of the Act; and

(c) effect cooperation between the South African Police Service, other organs of state and the private sector insofar as it relates to the protection of critical infrastructure.

(2) Unless otherwise provided for in these regulations, the Regulator must develop uniform standards, guidelines and protocols for submission to the National Commissioner.

(3) The uniform standards, guidelines and protocols referred to in subregulation (2) must include—

(a) the manner in which—

(i) infrastructure may be identified, categorised and declared critical infrastructure to supplement any regulations made in terms of the Act;

(ii) any physical security assessment of critical infrastructure and potential critical infrastructure is conducted and coordinated between officials of the Regulator and officials from any other government department, including the State Security Agency and the National Disaster Management Centre;

(iii) information which may be relevant to critical infrastructure protection is shared between the relevant stakeholders; or

(iv) any committee or forum referred to in the Act or these regulations must function and report; and

(b) structures and mechanisms to facilitate coordination in, and management of, the protection of critical infrastructure.

(4) Subject to subregulation (5) and (6), the Regulator must develop uniform standards, guidelines and protocols referred to in subregulation (3)*(a)*(i) to (iv), after consultation with government departments in the Justice, Crime Prevention and Security Cluster, other relevant government departments, the National Intelligence Co-ordinating Committee or any other person or entity who has an interest in the protection of critical infrastructure.

(5) Where any uniform standard, guideline or protocol is of a purely internal administrative nature, the Regulator may dispense with the consultation process.

(6) Where any uniform standard, guideline or protocol requires to be classified in accordance with the Minimum Information Security Standards, the National Commissioner may restrict the consultation to persons or officials in other departments who has the relevant security clearance.

(7) The Regulator must specifically support the National Commissioner in the performance of the functions assigned to him or her in terms of section 9(3) of the Act and—

(a) assist any person who wishes to apply for declaration of infrastructure as critical infrastructure as contemplated in section 17 of the Act, to complete

an application for declaration in terms of that section and these regulations;

(b) receive and process applications referred to in section 17 of the Act for declaration as critical infrastructure;

(c) process applications referred to in section 18 of the Act;

(d) conduct or facilitate physical security assessments referred to in sections 9(3)*(b)* and 17(4)*(b)* of the Act;

(e) submit a report on any application and accompanying documents to the National Commissioner for approval of the report and submission to the Council;

(f) evaluate, monitor and review the application and operational effectiveness of directives, policy, guidelines or legislation related to the protection of critical infrastructure, to enable the National Commissioner to advise the Council accordingly;

(g) ensure that all Joint Planning Committees are aware of directives, policy, guidelines or legislation related to the protection of critical infrastructure;

(h) evaluate and review physical security assessments, resilience reports and any designation as critical infrastructure, to enable the National Commissioner to advise the Council accordingly;

(i) monitor and evaluate the standard of—

(i) security at critical infrastructures;

(ii) security service providers at critical infrastructure;

(iii) critical infrastructure related training at registered security training providers;

(iv) competency in firearms proficiency of security personnel at critical infrastructure;

(v) application of working animals at critical infrastructure; and

(vi) critical infrastructure related security technology governed in terms of other national legislation,

to address any identified inadequacies;

(j) implement mechanisms to assign responsibility within the South African Police Service regarding—

(i) protection of critical infrastructure in a province, district or other geographical location;

(ii) allocation and deployment of resources of the South African Police Service to protect critical infrastructure; and

(iii) determination of reporting procedures regarding incidents or occurrences;

(k) consider any draft of a security policy or plan submitted to the National Commissioner and advise the National Commissioner accordingly;

(l) submit directives to the National Commissioner for consideration regarding the procedures to be followed at the meetings of any committee or forum where such procedures are not prescribed in terms of these regulations;

(m) keep a database of—

(i) security personnel at critical infrastructure;

(ii) security service providers at critical infrastructure;

(iii) critical infrastructure related security training providers;

(iv) registered working animals at critical infrastructure; and

(v) registered trainers and assessors appointed to provide a security service or training at critical infrastructure;

(n) compile and submit quarterly reports referred to in section 9(3)*(h)* of the Act to the National Commissioner for submission to the Council; and

(o) perform any related tasks as directed by the National Commissioner.

(8) The reports referred to in subregulation (7)*(n)* must include particulars of the—

(a) related activities of the South African Police Service during the preceding quarter, including all physical security assessments and inspections;

(b) number of applications for declaration of infrastructure as critical infrastructure;

(c) level and extent of Government department participation in the functioning of a committee or forum, including all Joint Planning Committees and liaison forums; and

(d) level and extent of public-private sector cooperation in the functioning of a committee or forum, including all Joint Planning Committees and liaison forums.

13. Identification of infrastructure for possible declaration as Critical Infrastructure

(1) The Regulator must, in cooperation with an applicable standing committee referred to in regulation 35, identify sectors in the Republic which may contain infrastructure that qualifies for declaration as critical infrastructure as contemplated in section 16(1) of the Act.

(2) The Regulator must analyse the services rendered by the sectors referred to in subregulation (1) in order to define all critical services within each sector.

(3) After defining the critical services referred to in subregulation (2), the Regulator must identify infrastructure involved with the rendering of such critical service and determine whether the infrastructure in question qualifies for possible declaration as critical infrastructure as contemplated in section 16(1) of the Act.

(4) Where the Regulator identifies for possible declaration as critical infrastructure any infrastructure under the control of or occupied by a person or institution other than a Government department, the Regulator must request the person in control of such infrastructure to complete a questionnaire to determine whether the person in control should lodge an application in terms of section 17 of the Act.

(5) The Regulator must consider the response to the questionnaire referred to in subregulation (4) and, where applicable, advise the person in control to lodge an application for declaration as critical infrastructure in terms of section 17 of the Act.

(6) The advice of the Regulator does not assign any legal duty on the person in control of that infrastructure to apply for declaration of the infrastructure as critical infrastructure.

(7) Identification of infrastructure for possible declaration of that infrastructure as critical infrastructure must be done with regard to any other guidelines that may be approved by the Critical Infrastructure Protection Council from time to time.

14. Assistance to person in control

(1) The Head of the Critical Infrastructure Protection Regulator or any police official under his or her command must render assistance to a person in control who wishes to apply for declaration of infrastructure as critical infrastructure.

(2) For purposes of the assistance referred to in subregulation (1), a police official placed within the Regulator may—

(a) assist the person in control with a questionnaire before such person lodges an application for declaration as critical infrastructure;

(b) conduct a preliminary physical security assessment; and

(c) render such assistance to the person in control as may be necessary to complete the application form.

CHAPTER 4

APPLICATION FOR DECLARATION AS CRITICAL INFRASTRUCTURE

15. Manner and format of application

(1) A person in control of infrastructure who intends to apply for declaration of that infrastructure as critical infrastructure as contemplated in section 17 of the Act, must obtain the application form from the office of the Head of the Critical Infrastructure Protection Regulator or the official Internet website of the South African Police Service at www.saps.gov.za and complete and sign the application form.

(2) The application must be in a form that corresponds with Form 1 of Annexure A to these regulations.

(3) Where a person in control is of the opinion that he or she may need assistance with the completion of the application form, he or she may, before lodging such application, request the Head of the Regulator to assign a police official in the Regulator to assist him or her as provided for in regulation 14.

(4) The Head of the Regulator may not impose any fee or tariff for any assistance rendered in terms of this regulation.

(5) A police official designated to assist an applicant to complete the application form, may conduct a preliminary physical security assessment in order to

provide sufficient information to the person in control to complete and lodge the application.

(6) The application form, together with supporting documents, must be lodged with the Head of the Regulator at the address indicated on the application form.

(7) Any application form and supporting documents that are lodged electronically, must be encrypted with a password which must be provided to the police official receiving the application.

16. Documents to accompany the application

An application form for declaration as critical infrastructure must be accompanied by—

(a) a statement which confirms that—

(i) the person in control knows and understands the duties of a person in control of critical infrastructure as provided for in Chapter 4 of the Act; and

(ii) the person in control undertakes to ensure compliance with the requirements of other legislation regulating that business or industry.

(b) a certified copy of the identity document of the person in control and every person responsible for the management or day-to-day control of the infrastructure in question;

(c) a recent utility account or a lease agreement verifying the address of the premises to which the application relates;

(d) written proof of the applicant's bank account;

(e) a copy of the person in control's fingerprints, or where more than one person are involved in the day to day management of the infrastructure, a copy of the fingerprints of each person so involved;

(f) documents which verify applicant's founding as a company or any other business form which establishes the applicant as a juristic person;

(g) a plan of the layout of the premises to which the application relates;

(h) submissions to depart from the procedure set out in section 17(4)*(a)* of the Act;

(i) any other documentation requested by the National Commissioner; and

(j) any other documentation that applicant wishes to submit in support of the application, including a copy of any certificate or permit relating to other legislation regulating that industry.

17. Request for departure from provisions of section 17(4)*(a)* of Act

(1) A person in control of infrastructure who applies for declaration of that infrastructure as critical infrastructure, may, in terms of section 17(5) of the Act, show good cause why the provisions of section 17(4)*(a)* should not be followed and lodge such request with the National Commissioner.

(2) The applicant must obtain the applicable form from the office of the Head of the Critical Infrastructure Protection Regulator or the official Internet website of the South African Police Service at www.saps.gov.za and complete and sign the form.

(3) The request must, besides the factors set out in section 17(6) of the Act, contain sufficient information to support the submission.

(4) The Head of the Regulator may require the person in control to provide further information necessary to process the request.

(5) The Head of the Regulator must, within 30 days of the request, consult with the State Security Agency, and compile a report for the National Commissioner.

(6) The National Commissioner must, within 30 days of the receiving the report, submit the request with his or her recommendation indicating whether the request is reasonable and justifiable in the circumstances to enable the Critical Infrastructure Council to take a decision on the matter.

(7) The Council must consider the request as contemplated in regulation 6.

18. Application for declaration of government infrastructure by National Commissioner

(1) An application by the National Commissioner for declaration of government infrastructure as critical infrastructure must be in a form that substantially corresponds with Form 1 of Annexure A to these regulations.

(2) Any application referred to in subregulation (1) that is submitted to the Critical Infrastructure Protection Council, must be accompanied by—

(a) written reasons why the National Commissioner applies for declaration of the government infrastructure;

(b) the written representations of the head of the Government department in question referred to in section 18(3)*(b)* of the Act;

(c) where applicable, the written response of the National Commissioner to the representations by the Head of the Government department in question where the National Commissioner is of the opinion that the written representations of the head of the Government department in question should not be considered favourably.

(3) A notice referred to in section 18(3)*(a)* of the Act must be served on the Head of the Government department in question or, if the Head of the Government department cannot be found, a person in the Senior Management Service in the employ of the Government department concerned.

CHAPTER 5

SYSTEM OF CATEGORISATING CRITICAL INFRASTRUCTURE IN LOW-RISK, MEDIUM RISK OR HIGH-RISK CATEGORY

19. System of categorising infrastructure in low-risk, medium-risk or high-risk category

(1) The system of categorising infrastructure in a low-risk, medium-risk or high-risk category is based on the national societal risk to the Republic in the event of failure, disruption or destruction of critical infrastructure.

(2) The national societal risk describes the risk of failure, disruption or destruction of infrastructure where that infrastructure forms part of a national or global network of interdependent infrastructure, whether the infrastructure is declared as critical infrastructure or not.

(3) To determine the risk inherent to specific infrastructure, the Minister must have regard to the effect or impact of failure, disruption or destruction of that infrastructure in relation to the probability of such failure, disruption or destruction to determine whether the infrastructure must be categorised in a low-risk, medium-risk or high-risk category.

(4) The Minister may, from time to time, issue a directive with guidelines in respect of the application of the system of categorising infrastructure in a low-risk, medium-risk or high-risk category.

20. Functions of the National Commissioner in respect of risk categorisation

(1) In order to assess the risk categorisation in respect of infrastructure where an applicant applies for declaration of that infrastructure as critical infrastructure, the National Commissioner must—

(a) assess the application referred to in section 17(1) of the Act;

(b) assess the physical security assessment referred to in section 17(4)*(b)* of the Act and, where applicable, have regard to any written submissions in terms of section 17(4)*(b)*(iv) of the Act;

(c) consider any other facts submitted by the applicant; and

(d) apply the system of categorising infrastructure in a low-risk, medium-risk or high-risk category contemplated in regulation 19.

(2) After evaluating the application, physical security assessment and other facts outlined in subregulation (1), the National Commissioner must determine the national societal risk to the Republic in the event of failure, disruption or destruction of the infrastructure in question.

(3) When determining the national societal risk to the Republic as contemplated in subregulation (2), the National Commissioner may have regard to—

(a) the significance of the infrastructure in respect of economic, public, social or strategic importance;

(b) the effect on the Republic's ability to function, deliver basic public services; maintain law and order or comply with international obligations if a service rendered by the infrastructure is interrupted, or if the infrastructure is destroyed, disrupted, degraded or caused to fail;

(c) the effect of interruption of a service rendered by the infrastructure, or whether the destruction, disruption, degradation, or failure of such infrastructure will have a significant effect on the environment, the health or safety of the public or any segment of the public, or any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question;

(d) the probability of destruction, disruption, degradation, or failure of such infrastructure; and

(e) any other relevant factor or criteria that may assist in the determination of the national societal risk to the Republic.

(4) For purposes of the determination contemplated in subregulation (3), the consequences and probability of destruction, disruption, degradation, or failure of such infrastructure must be measured incrementally.

(5) The National Commissioner may, where circumstances require, take any other relevant facts into consideration in assessing the appropriate risk category pertaining to the infrastructure in question, including consultation with—

(a) the person in control of the infrastructure in question;

(b) the security manager of the infrastructure in question;

(c) any other government organ; or

(d) any other entity,

before completing the risk categorisation process in terms of this regulation.

(6) After completion of the risk categorisation process contemplated in this regulation, the National Commissioner must submit a motivated recommendation on the categorisation of the infrastructure in question in a low-risk, medium-risk or high-risk category to the Critical Infrastructure Council.

21. Consideration of risk categorisation proposed by National Commissioner

(1) In order to advise the Minister on the risk category of infrastructure that is the subject of an application for declaration as critical infrastructure, the Critical Infrastructure Council must consider the recommendation submitted by the National Commissioner and any other facts pertaining to the matter.

(2) The Critical Infrastructure Council may, in order to satisfy itself that the system of categorising the infrastructure in a low-risk, medium-risk or high-risk

category, was applied correctly, follow the process set out in this Chapter to determine the risk category of the infrastructure.

(3) The Critical Infrastructure Council must, after consideration of the risk categorisation as contemplated in section 19(1)*(b)* of the Act, submit its recommendation on the appropriate risk categorisation together with all applicable documents, to the Minister for consideration.

(4) The Minister may, after satisfying him- or herself that the system of categorising the infrastructure in a low-risk, medium-risk or high-risk category, was applied correctly, categorise the infrastructure in an appropriate risk category.

(5) The Minister is not bound by the recommendations of the Critical Infrastructure Council and may consult with any other person or entity in order to apply his or her mind.

CHAPTER 6

DECLARATION OF INFRASTRUCTURE AS CRITICAL INFRASTRUCTURE

22. Certificate of declaration as critical infrastructure

(1) Upon declaring infrastructure as critical infrastructure, the Minister must issue a certificate of declaration as critical infrastructure in a form that corresponds with Form 2 of Annexure A to these regulations.

(2) The certificate of declaration must contain—

(a) a description of the critical infrastructure concerned, together with any applicable critical infrastructure complex;

(b) in the event that different parts of the critical infrastructure are categorised in different risk categories, a detailed plan of the critical infrastructure setting out the risk category must be appended to the certificate; and

(c) a comprehensive list of conditions imposed, together with the time frames within which the conditions must be fulfilled as contemplated in regulation 24.

(3) The National Commissioner must deliver a certificate of declaration to the person in control by hand within seven days of its issue.

(4) The publication in the Gazette contemplated in section 21(6) of the Act must contain the name of the critical infrastructure, the sector in which it operates together with the name of the province in which the critical infrastructure is situated.

23. Critical Infrastructure register

(1) The National Commissioner must keep and maintain a register of all critical infrastructure in a form that corresponds with Form 3 of Annexure A to these regulations.

(2) The critical infrastructure register referred to in subregulation (1) must be made accessible to the public by placing an electronic copy of the register, as updated from time to time, on the website of the South African Police Service at www.saps.gov.za.

24. Conditions that may be imposed by Minister in respect of physical security measures

(1) The Minister may, when declaring infrastructure as critical infrastructure, impose any of the following conditions on the person in control of the critical infrastructure to ensure sufficient security at such critical infrastructure:

(a) zoning of different infrastructure, areas, facilities, buildings or elements of the critical infrastructure concerned into applicable security zones;

(b) installation of adequate physical security measures in general or in the specified security zones contemplated in paragraph *(a)*;

(c) where critical infrastructure is categorised as medium- or high-risk critical infrastructure, the installation of a physical Security Operations Centre at that critical infrastructure;

(d) deployment of security personnel and equipment;

(e) the activation of a Joint Planning Committee; or

(f) any other measure set out in a directive issued by the Minister from time to time.

(2) Installation of any or all of the physical security measures referred to in subregulation (1) may be deferred over a period not exceeding 60 months on condition

that the person in control submits a satisfactory implementation plan for the incremental installation of such measures.

(3) Any decision to allow installation of physical security measures over a period referred to in subregulation (2), may be reviewed from time to time depending on the exposure of the critical infrastructure to any threat or any physical security assessment or audit conducted within that period.

(4) Different conditions may be imposed on critical infrastructure categorised as low-risk, medium-risk, or high-risk.

(5) Different conditions may be imposed on infrastructure, areas, facilities, buildings, assets or elements of the critical infrastructure concerned where such infrastructure, areas, facilities, buildings, assets or elements of the critical infrastructure concerned are categorised in different low-risk, medium-risk, or high-risk categories or security zones.

(6) Any physical security measure referred to in this regulation must, where applicable, conform to the relevant South African National Standard as determined by the South African Bureau of Standards or any applicable standard of the International Standards Organisation.

(7) Where critical infrastructure must conform to minimum physical security standards of an official regulatory authority, such minimum standards may be considered in the event that it conforms to or exceeds the standards imposed in terms of these regulations.

25. Steps to be taken by the person in control after declaration as critical infrastructure

A person in control of critical infrastructure must ensure that the following steps are taken upon declaration as critical infrastructure referred to in section 20(1) of the Act:

(a) compliance with the conditions of declaration as critical infrastructure;

(b) subject to paragraph *(c)*, appointment of a security manager where such person has not been appointed;

(c) vetting of such security manager as contemplated in section 24(7) of the Act;

(d) in the case of critical infrastructure categorised as medium-risk or high-risk critical infrastructure, the appointment of a control security officer;

(e) establishment of a Joint Planning Committee;

(f) nomination of a chairperson for the Joint Planning Committee for approval by the National Commissioner;

(g) establishment of a Security Operations Centre; and`

(h) appointment or sourcing of security personnel or security service providers in accordance with Chapter 10 of these regulations.

26. Failure to take steps after declaration as critical infrastructure

(1) In the event that a person in control of a critical infrastructure fails to take the steps referred to in regulation 25, the Minister may, in terms of section 24(5) of the Act and by written notice in a form that substantially corresponds with Form 4 of Annexure A to these regulations, order him or her to take such steps in respect of the security of the critical infrastructure as may be specified in the notice.

(2) The notice referred to in subregulation (1) must set out the period within which the person in control of the critical infrastructure concerned, must take the steps in respect of the security of the critical infrastructure—

(a) set out in the certificate of declaration as a condition; or

(b) referred to in regulation 25(1).

(3) The period under subregulation (2)*(b)* within which the person in control must take the steps set out in regulation 25(1), may not be longer than three months.

(4) The notice referred to in subregulation (1) must be delivered to the person in control of the critical infrastructure in question by hand, registered mail, electronically by email.

(5) In the event that a dispute arises whether the person in control received a notice electronically by email, it will be sufficient proof of such delivery if the notice was delivered to the email address supplied by the person in control when applying for the infrastructure to be declared critical infrastructure.

CHAPTER 7

ESTABLISHMENT, FUNCTIONS, FUNCTIONING, MEETING AND REPORTING PROCEDURE OF COMMITTEES AND FORUMS

27. Establishment of Joint Planning Committee

(1) Every person in control of critical infrastructure must, upon declaration of that infrastructure as critical infrastructure, establish and maintain a Joint Planning Committee for that critical infrastructure.

(2) Subject to regulation 30(1), the Committee must comprise the following role players:

(a) the person in control of the critical infrastructure concerned, or a person referred to in *(b)* designated by him or her;

(b) a person involved in the day-to-day management of the critical infrastructure concerned;

(c) the security manager of the critical infrastructure concerned;

(d) the following environments from the South African Police Service:

(i) the local police station in whose precinct the critical infrastructure is situated;

(ii) the Critical Infrastructure Protection Regulator; and

(e) the State Security Agency.

(3) The Committee may from time to time co-opt persons or entities who may have an interest in the physical security of the critical infrastructure concerned, including but not limited to:

(a) a person involved with the financial environment of the critical infrastructure;

(b) a legal adviser for the critical infrastructure;

(c) the following environments from the South African Police Service where applicable:

(i) Division Crime Intelligence;

(ii) Division Visible Policing and Operations;

(iii) Division Legal Services;

(d) the Disaster Management Centre and the Emergency Response Services of the local authority in whose jurisdiction the critical infrastructure is situated, including any municipal or traffic police of the local authority;

(e) the South African National Defence Force, where applicable; and

(f) other critical infrastructure in a critical infrastructure complex, or critical infrastructure that may affect or be affected by the physical security of the critical infrastructure in question.

(4) Each role player to be represented in the Committee in terms of subregulations (2) and (3) must designate in writing a specific official or officials to represent that entity or body on a continuous basis.

(5) A designated representative other than from the South African Police Service must be vetted by the State Security Agency.

(6) In the case of—

(a) a critical infrastructure complex;

(b) critical infrastructure facilities in close geographical proximity to each other; or

(c) critical infrastructure facilities that have an interdependence,

the persons in control may in consultation with the Regulator agree to establish a single Committee where all the critical infrastructure facilities are represented.

(7) The person in control must ensure that secretarial services are rendered by personnel of the critical infrastructure concerned.

28. Functions of Joint Planning Committee

The functions of the Joint Planning Committee are to—

(a) plan and co-ordinate all activities of the members of the Committee related to the protection and security of the critical infrastructure concerned;

(b) compile an action plan to set out the steps to implement any condition of declaration as critical infrastructure or any recommendation of the National Commissioner in respect of the security at that critical infrastructure;

(c) ensure that a security policy and plan is developed for the critical infrastructure concerned;

(d) allocate responsibilities to designated members of the Committee to co-ordinate, align and implement all security policies and plans of the members of the Committee;

(e) allocate responsibilities to designated members of the Committee insofar it relates to the physical security of the critical infrastructure concerned;

(f) monitor and evaluate the efficiency of the security plan and policy from time to time;

(g) promote integration and collaboration between members of the Committee, including other stakeholders;

(h) provide oversight, advice and assurance on all aspects of risk identification and mitigation, security measures and protection of the critical infrastructure concerned; and

(i) foster awareness and training on the security policy and plan, including any response plans and mitigation measures, for the critical infrastructure concerned.

29. Chairperson of Joint Planning Committee

(1) The person in control of a critical infrastructure must, upon declaration of the infrastructure as critical infrastructure, in writing designate a person in the employ of the critical infrastructure to serve as the—

(a) convener and chairperson of the Joint Planning Committee for that critical infrastructure; and

(b) deputy chairperson.

(2) The letter of designation of the proposed chairperson and deputy chairperson must be submitted to the Head of the Critical Infrastructure Regulator for screening in terms of subregulation (3), consideration and approval by the National Commissioner.

(3) The Head of the Regulator must, where the proposed chairperson and deputy chairperson have not been screened, submit the names to the State Security Agency for screening.

(4) After successful screening, the Head of the Regulator must, in writing, inform the person in control of such approval where after the chairperson must convene an inaugural meeting of the Joint Planning Committee as contemplated in regulation 30.

(5) In the event that the proposed chairperson or deputy chairperson referred to in subregulation (1) are not successfully screened by the State Security

Agency, the Head of the Regulator must inform the person in control accordingly and request the person in control to propose other persons to serve as such, where after the procedure in subregulation (2) must be followed.

(6) In the event that the second proposed chairperson or deputy chairperson are not screened successfully, the Head of the Regulator may designate a police official to act as chairperson or deputy chairperson until a suitable candidate is approved.

30. Inaugural meeting of Joint Planning Committee

(1) The chairperson of a Joint Planning Committee must, upon his or her approved designation, consult with the National Commissioner to determine the composition of the Joint Planning Committee role players as referred to in regulation 27(2) and (3) with due regard to the risk categorisation of that critical infrastructure.

(2) After determination of the composition of the Committee, the chairperson must convene an inaugural meeting of the Committee following the procedure set out in regulation 31.

31. Ordinary meetings of Joint Planning Committee

(1) The chairperson of the Joint Planning Committee must ensure that the Committee meets quarterly by notifying each member designated in terms of regulation 27(3) in writing at least 30 days before the date of such meeting.

(2) A Committee must meet at least—

(a) once per quarter in the case of critical infrastructure categorised as high- or medium risk; or

(b) once per semester in the case of critical infrastructure categorised as low-risk.

(3) The notification referred to in subregulation (1) must contain the venue, date and time of such meeting and must be accompanied by the minutes of the previous preceding meeting of the Committee, as well as an agenda of the business to be considered at such meeting.

(4) At each meeting of the Committee the venue, date and time for the succeeding meeting may be determined by consent, failing which the chairperson may determine such a venue, date and time.

(5) A copy of any document to be discussed at the meeting must accompany the notification referred to in subregulation (1).

(6) The chairperson must ensure that the documents referred to in subregulation (4) are adequately sealed or, in the case of electronic documents, protected by means of a unique password in order to protect the confidentiality thereof.

(7) The Committee decides its own rules of debate subject to subregulations (9) to (17) or any practice directive issued by the Minister under section 27(4) of the Act.

(8) The first act of an ordinary meeting, after being constituted, is to read and confirm by the signature of the chairperson the minutes of the last preceding ordinary meeting and of any special meeting subsequently held. The meeting may consider the minutes as read, provided that objections or proposed amendments to the minutes of the last preceding ordinary or special meeting are raised and decided upon before confirmation of the minutes.

(9) Attendance by the following members of the Committee will constitute a quorum:

(a) the chairperson or deputy chairperson;

(b) the security manager;

(c) the environments of the South African Police Service referred to in regulation 27(2)*(c)*;

(d) the State Security Agency.

(10) The meeting must deal with the business of which notice has been given and any other business which a majority of the total membership of the Committee agrees to consider.

(11) Every motion must be seconded and must, if the chairperson requires this, be in writing and a motion that is not seconded falls away.

(12) Each question must be decided by the majority of votes of the members present and voting, and unless the meeting decides otherwise voting must be by show of hands.

(13) Should the majority of members present abstain from voting, the matter to be decided on must be deferred.

(14) The chairperson may, in the case of any strictly procedural matter, refer such matter by letter or electronic means for consideration by members of the Committee.

(15) When a majority of the members of the Committee reaches agreement on a matter referred to in subregulation (13) without convening a meeting, such resolution is equivalent to a resolution of the Committee and must be recorded in the minutes of the next succeeding ordinary meeting.

(16) The views of a member of the Committee who is unable to attend a meeting may be submitted to the meeting in writing but may not count as a vote of such member.

(17) If so decided by the meeting, the number of members voting for or against, or abstaining from, any motion must be recorded in the minutes, and at the request of any member the chairperson must direct that the vote of such member be likewise recorded.

(18) The ruling of the chairperson on any question of order or procedure is binding unless immediately challenged by a member, in which event such ruling must be submitted without discussion to the meeting whose decision is final.

(19) The Committee may invite persons who are not members to attend meetings and allow them to take part in discussions, provided that they are not allowed to vote.

(20) Meetings of the Committee must take place at the critical infrastructure concerned, unless special arrangements are agreed upon by the members of the Committee: Provided that the chairperson may direct that a meeting of the Committee be conducted on an electronic virtual platform when required by exigent circumstances.

(21) An attendance list shall be kept and must accompany any report of the committee.

32. Special meeting of the Joint Planning Committee

(1) In the event that a special meeting of the Joint Planning Committee is required, the chairperson must notify the members of the Committee of the date, time

and venue of such special meeting in writing at least 14 days before the date of such special meeting.

(2) The notification referred to in subregulation (1) must contain the venue, date and time of such special meeting and must be accompanied by an agenda of the business to be considered at such special meeting.

(3) Attendance by the members of the Committee referred to in regulation 31(9) will constitute a quorum.

(4) Any matter on the agenda of a special meeting must contain sufficient information to enable the members of the Committee to sufficiently prepare for the special meeting.

(5) A member of the Committee who is of the opinion that the agenda does not describe the matter in question sufficiently, must request further particulars from the chairperson at least 10 days before the special meeting.

(6) Special meetings of the Committee must take place at the critical infrastructure concerned, unless special arrangements are agreed upon by the members of the Committee: Provided that the chairperson may direct that a special meeting of the Committee be conducted on an electronic virtual platform when required by exigent circumstances.

(7) An attendance list shall be kept and must accompany any report of the committee.

33. Specific matters to be attended to by the Joint Planning Committee

(1) The Joint Planning Committee must, in order to fulfil its functions referred to in regulation 28, specifically deal with the following matters:

(a) establishment and maintenance of institutional arrangements that enable the implementation of and compliance with the Act;

(b) determination of the effectiveness of physical security measures, emergency response measures and contingency plans for the critical infrastructure;

(c) consideration of any amendment of the risk categorisation of the critical infrastructure, including termination of the declaration of the critical infrastructure concerned;

(d) conducting of quality assurance assessments;

(e) compilation, approval and implementation of a detailed security policy and plan in support of the security manager;

(f) noting any written report of an inspector;

(g) discussion where the person in control fails or refuses to implement or maintain the required physical security measures;

(h) advising on the type of firearm required for the protection of the critical infrastructure concerned;

(i) establishment of a Security Operations Centre from where all activities must be coordinated in an emergency situation;

(j) considering the activation of a Security Operations Centre when an incident affecting the physical security of the critical infrastructure security is reported;

(k) schedule incident response simulation exercises for the protection of critical infrastructure that involves all role players;

(l) establish a system for communication and reporting for the purposes of incident command and the management of joint operations;

(m) establish a process and appropriate system for disseminating early warnings, intelligence or information to take risk avoidance measure for the critical infrastructure;

(n) approve and review the local police response plan for the critical infrastructure concerned;

(o) analyse the threat intelligence briefings and threat risk assessments issued by the State Security Agency;

(p) monitor compliance and key performance indicators outlined in the security plan and make recommendations for improvement or compliance;

(q) assess the budgetary and funding plan for the implementation of physical security measures for the critical infrastructure;

(r) measure performance and evaluate effectiveness of the Committee and submit copies of the evaluation report to the relevant structures of the critical infrastructure and the Critical Infrastructure Regulator; and

(s) liaise with persons representing any other infrastructure, critical infrastructure, entity or sphere of government, including representatives

from international infrastructure where such infrastructure has a direct link with the critical infrastructure in question.

(2) A Joint Standing Committee may, in order to fulfil its purpose, establish a standing committee or an *ad hoc* committee consistent with the provisions of regulation 35(3) to (8) and regulation 36(3) to (7) respectively, which apply with the necessary changes required by the context.

34. Reporting by the Joint Planning Committee

(1) The chairperson of the Joint Planning Committee must draft a report after each meeting of the Committee or after an incident response simulation exercise referred to in regulation 46 to advise the person in control of the critical infrastructure concerned of any matter dealt with by the Committee, more particularly any shortcomings or deficiencies in the security policy and plan and the physical security measures at the critical infrastructure.

(2) The report must be classified in accordance with the Minimum Information Security Standards approved by Cabinet from time to time.

(3) The report referred to in subregulation (1) must make suitable recommendations regarding the physical security of the critical infrastructure, the security policy and plan and the implementation thereof to ensure compliance with the Act and these regulations.

(4) A person in control of infrastructure must consider any report referred to in subregulation (1) and must take the necessary steps to ensure that the critical infrastructure concerned complies with the conditions of declaration referred to in section 20(1)(d) of the Act regarding any steps and measures he or she must implement to safeguard the critical infrastructure in question.

(5) The person in control of critical infrastructure must ensure that he or she implements the necessary steps and measures to safeguard the critical infrastructure in question where the report referred to in subregulation (1) shows that physical security measures at the critical infrastructure concerned—

(a) do not comply with the conditions of declaration referred to in section 20(1)(d) of the Act; or

(b) are inadequate.

(6) The report referred to in subregulation (1) must be submitted by the chairperson to the person in control of that infrastructure.

(7) A copy of the report referred to in subregulation (1) must be submitted to the National Commissioner as well as the State Security Agency.

35. Standing committees

(1) The National Commissioner may establish any standing committee which in his or her opinion is necessary or expedient to obtain advice or assistance in order to perform any function contemplated in sections 9(2) and (3) of the Act.

(2) The purpose of a standing committee is primarily to advise the National Commissioner on any of the following matters:

(a) identification of infrastructure for possible declaration as critical infrastructure;

(b) applications for declaration of infrastructure as critical infrastructure;

(c) physical security assessments, physical security re-assessments and physical security evaluations;

(d) risk categorisation; and

(e) any other matter relevant to the protection of critical infrastructure that may arise from time to time.

(3) A standing committee must comprise of representatives of the Critical Infrastructure Protection Regulator, other Divisions or components of the South African Police Service and, where applicable, the State Security Agency.

(4) A standing committee may co-opt any other person to attend a meeting of the standing committee as and when required.

(5) The National Commissioner or his representative must act as chairperson of a standing committee to convene and chair meetings and to ensure that the necessary secretarial services are provided to the committee.

(6) The disqualifications from appointment as a member of Critical Infrastructure Council set out in section 5*(a)* and *(c)* to *(g)* of the Act shall apply *mutatis mutandis* to members of a standing committee.

(7) A standing committee must adopt terms of reference for that committee that may set out any or all of the following:

(a) the purpose and objectives of the committee;

(b) membership of the committee;

(c) meeting frequency;

(d) meeting quorums;

(e) reporting responsibilities;

(f) reporting procedures;

(g) guiding principles;

(h) meeting procedures;

(i) administrative duties and secretarial services;

(j) performance evaluation;

(k) review procedures for the terms of reference;

(l) duties of the chairperson;

(m) decision making procedures;

(n) disqualification of persons; and

(o) removal of members.

(8) An attendance list shall be kept and must accompany any report of the standing committee.

36. *Ad hoc* committees

(1) The National Commissioner may establish any *ad hoc* committee which in his or her opinion is necessary or expedient to obtain advice or assistance regarding a specific matter related to any function contemplated in sections 9(2) and (3) of the Act.

(2) The purpose of an *ad hoc* committee is primarily to advise the National Commissioner on matters that are not dealt with by a standing committee.

(3) An *ad hoc* committee may comprise of representatives of the Critical Infrastructure Protection Regulator and any other person who may be knowledgeable or experienced in the matter referred to the *ad hoc* committee.

(4) The National Commissioner or his or her representative must act as chairperson of an *ad hoc* committee to convene and chair meetings and to ensure that the necessary secretarial services are provided to the committee.

(5) The disqualifications from appointment as a member of Critical Infrastructure Council set out in section 5*(a)* and *(c)* to *(g)* of the Act shall apply *mutatis mutandis* to members of an *ad hoc* committee.

(6) The meeting procedures and other relevant matters must be determined by the Head of the Regulator.

(7) An attendance list shall be kept and must accompany any report of the *ad hoc* committee.

37. Critical Infrastructure Liaison Forum

(1) In order to promote cooperation and a culture of shared responsibility between various role-players in order to provide for an appropriate multi-disciplinary approach to deal with critical infrastructure protection, the National Commissioner may establish a Critical Infrastructure Liaison Forum on a national level as well as on a provincial level where applicable.

(2) A Forum should consist of persons involved with physical security at critical infrastructure and may include—

(a) chairpersons of Joint Planning Committees;

(b) security managers;

(c) relevant police officials, including the Critical Infrastructure Protection Regulator;

(d) representatives of the State Security Agency;

(e) representatives of the relevant level of a Disaster Management Centre; and

(f) any other person with an interest in critical infrastructure protection.

(3) The objective of a Forum is to liaise with the members thereof to—

(a) share information pertinent to physical security of critical infrastructure;

(b) share best practices; and

(c) consult Joint Planning Committees and security managers of critical infrastructure regarding any function of the Minister, the Critical Infrastructure Council, the National Commissioner or the Regulator.

(4) A Forum must meet at least once per quarter.

(5) The meeting procedures and other relevant matters must be determined by the National Commissioner.

(6) An attendance list shall be kept and must accompany any report of the Forum.

CHAPTER 8

SECURITY POLICY AND PLAN

38. Definitions

In this Chapter, unless the context indicates otherwise—

"graded approach" means application of incremental security measures to limit access or egress to and from the critical infrastructure or restricted areas, facilities, buildings, assets, elements or security zones of the critical infrastructure which is proportional to a potential threat to the security of the critical infrastructure;

"process-based security management system" means a security management system that views security management as a collection of key activities managed to achieve an acceptable level of assurance that critical infrastructure is secure;

"security", **"security manager"**, **"security measures"**, **"security personnel" and "security service provider"** has the meaning ascribed to it in the Act;

"security plan" means a plan, as developed from time to time, to counter an identified threat to the security of a critical infrastructure;

"security policy" means a framework for the development of a process-based security management system;

"security zone" means a zone identified in the security plan where pre-determined security measures are put in place in terms of a graded approach;

39. Responsibility for security policy and plan

(1) The person in control of critical infrastructure is ultimately responsible for the physical security of that infrastructure and has the powers and duties set out in Chapter 4 of the Act.

(2) The security manager appointed in terms of section 24(7) of the Act and the Joint Planning Committee must support the person in control in the exercise of his or her functions under the Act and these regulations.

(3) The person in control of a critical infrastructure must develop a draft security policy and plan for that specific infrastructure for consideration by the National Commissioner in terms of section 9(3)*(f)* of the Act.

(4) The person in control must satisfy him- or herself that the security policy and plan conforms to the requirements of these regulations and any requirements of another regulatory authority.

(5) The National Commissioner may propose amendments to the security policy and plan for consideration by the person in control after which the security policy and plan must be submitted to the Joint Planning Committee for inputs.

(6) The role players in the Joint Planning Committee must ensure that their individual security plans are aligned with the security policy and plan of the critical infrastructure concerned.

40. Security policy

(1) A security policy for critical infrastructure must establish a framework for a process-based security management system.

(2) A security policy must contain, at a minimum the following:

(a) the purpose and scope of the policy;

(b) references to any governance rules;

(c) where applicable, definitions and abbreviations;

(d) responsibilities of—

(i) the critical infrastructure management;

(ii) the security manager;

(iii) the control security officers;

(iv) security personnel;

(v) employees;

(vi) security service providers if any; and

(vii) Joint Planning Committee role players.

(e) particulars of revision of the security policy; and

(f) a statement of intent in which the physical security objectives and the commitments to physical security of the critical infrastructure are set out.

41. Security plan

(1) A security plan must set out the key physical security processes that form part of the overall security plan.

(2) The security plan must, at a minimum, contain plans for the key physical security processes related to—

(a) access and egress control, subject to regulation 42;

(b) security awareness and preparation, subject to regulation 43;

(c) quality assurance, subject to regulation 44; and

(d) incident response, subject to regulation 45.

(3) The provisions of this regulation does not preclude measures in respect of information- or cybersecurity, personnel security, health and safety, or service continuity to supplement the security plan.

(4) The security plan must be viewed as a dynamic process that must be reviewed and adapted from time to time based on potential threats to the critical infrastructure and the vulnerabilities that the critical infrastructure may be exposed to.

(5) The security plan must not only provide for measures to mitigate, respond to or counter threats from persons outside the critical infrastructure who pose a threat to the critical infrastructure, but also from persons employed or contracted by the critical infrastructure.

42. Access and egress control

(1) Access and egress control must follow a graded approach to limit access and egress to and from the critical infrastructure or restricted areas, facilities, buildings, assets, elements or security zones of the critical infrastructure as set out in section 25 of the Act.

(2) An access and egress control plan must, at a minimum, contain the following:

(a) a map broadly setting out the perimeter and restricted areas or security zones of the critical infrastructure;

(b) an indication of physical security measures deployed in each of the restricted areas or security zones of the critical infrastructure;

(c) responsibilities of the security manager, control security officers, security personnel, security service providers and other employees;

(d) a system of identification and authorisation of employees or classes or categories of employees, visitors and service providers in respect of access to and egress from the critical infrastructure or restricted areas, facilities, buildings, assets, elements or security zones of the critical infrastructure; and

(e) subject to section 25(6) of the Act, procedures for searching of employees or classes or categories of employees, visitors and service providers, to effectively manage access and egress to and from the critical infrastructure or restricted areas, facilities, buildings, assets, elements or security zones of the critical infrastructure;

(f) reporting procedures in the case of a threat or potential threat, malfunction and breach or potential breach of the access and egress control measures;

(g) procedures for removal of a person under the circumstances contemplated in section 25(4) of the Act;

(h) procedures for taking into custody and removal of any article that may be removed as contemplated in section 25(7) of the Act;

(i) a parking management plan for employees or classes or categories of employees, visitors and service providers; and

(j) any further directive issued by the security manager in terms of section 25(2)*(a)* of the Act.

(3) The physical security measures referred to in subregulation (2)*(b)* must include measures pertaining to—

(a) authentication and authorisation measures, including but not limited to key and access card control, keypad, password or biometric control;

(b) record keeping in respect of access to and egress from the critical infrastructure; and

(c) a system of visible identification of employees, visitors and service providers.

(4) The person in control must ensure that the security manager—

(a) makes a determination referred to in section 25(2)*(b)* of the Act;

(b) compiles a list of dangerous and prohibited goods that are applicable to that specific critical infrastructure to be displayed at the entrance to the critical infrastructure; and

(c) places the notices referred to in sections 24(8) and 25(8) of the Act.

(5) The notice referred to in section 24(8) of the Act must—

(a) be at least 60 centimetre wide and 60 centimetre high;

(b) be placed on the perimeter of the critical infrastructure concerned wherever such placement is possible and practicable, but preferably not more than 500 meters apart;

(c) contain reflective lettering which is large enough to be legible from at least 10 meters;

(d) contain the particulars as required by section 24(8) and section 25(8) of the Act respectively.

(6) The notice referred to in section 25(8) of the Act may be combined with the notification referred to in section 25(1)*(b)* of the Act unless it is impractical to do so.

(7) The notices referred to in section 25(2)*(b)* or section 25(8) of the Act, or the combined notice referred to in subregulation (6) must—

(a) contain lettering which is large enough to be legible from at least 10 meters;

(b) contain a list of prohibited and dangerous objects; and

(c) be placed at every entrance to the critical infrastructure in a place where it is clearly visible; and

(d) in the case of a notice referred to in section 25(2)*(b)* of the Act, contain the particulars as required by that section, including a list of dangerous and prohibited goods contemplated in subregulation (4)*(b)*.

43. Security awareness and preparation

(1) The person in control must ensure that security awareness and preparation is developed and maintained to create a culture of security awareness and readiness at the critical infrastructure.

(2) The security awareness and preparation must focus on physical security of the infrastructure and set out the role of security personnel, employees on all levels, visitors to the critical infrastructure, and service providers.

(3) Security awareness campaigns and preparation must be viewed as a dynamic process that must be reviewed and adapted from time to time based on potential threats to the critical infrastructure and the vulnerabilities that the critical infrastructure may be exposed to.

44. Quality assurance

(1) Regular quality assurance by the security manager and the Joint Planning Committee must ensure that the key physical security processes are monitored and reviewed regularly for purposes of quality assurance.

(2) The purpose of quality assurance must be to ensure that the potential threats to the critical infrastructure and the vulnerabilities that the critical infrastructure may be exposed are mitigated in the manner in which the security plan is designed, implemented, operated and maintained.

(3) For purposes of quality assurance and compliance monitoring, the security plan must provide for regular incident response simulation exercises as contemplated in regulation 46.

45. Incident response

(1) The security plan must contain a comprehensive incident reporting management plan setting out—

(a) roles and responsibilities of the management of the critical infrastructure, Joint Planning Committee role players, security personnel, security service providers, and all employees;

(b) procedures for incident reporting;

(c) detailed reporting channels;

(d) procedures in the event of a threat materialising, including the manner in which a heightened response will be effected;

(e) security personnel response and activation of the Joint Planning Committee, law enforcement, disaster management or other authorities; and

(f) record keeping.

(2) The security plan must further contain a comprehensive management plan for emergency response, including—

(a) command structures;

(b) evacuation procedures; and

(c) communication procedures.

46. Incident response simulation exercises

(1) The person in control must, in consultation with the Critical Infrastructure Protection Regulator, ensure that incident response simulation exercises are planned and carried out annually.

(2) The person in control must, in consultation with the Joint Planning Committee, develop credible scenarios related to the physical security of the infrastructure based on potential threats to the critical infrastructure and the vulnerabilities that the critical infrastructure may be exposed to.

(3) The scenarios referred to in subregulation (1) must consider—

(a) insider as well as outsider adversaries who may pose a threat to the physical security of the critical infrastructure; and

(b) any threat that damage, harm or loss to the critical infrastructure or interference with the ability or availability of the critical infrastructure to deliver basic public services may have on other critical infrastructure.

(4) Incident response simulation exercises may consist of a desk top exercise annually but at least one real time incident response simulation exercise must be conducted—

(a) in the case of critical infrastructure categorised as low-risk, every 48 months;

(b) in the case of critical infrastructure categorised as medium-risk, every 36 months; or

(c) in the case of critical infrastructure categorised as high-risk, every 24 months.

(5) The objective of an incident response simulation exercise must be to evaluate—

(a) the incident response of the critical infrastructure and the Committee to a simulated threat;

(b) the incident response capabilities of the security personnel and the Committee role players;

(c) the effectiveness of the Security Operations Centre of the critical infrastructure concerned; and

(d) the effectiveness of the security policy and plan of the critical infrastructure concerned.

(6) The person in control must, in consultation with the Committee, prepare a report after each incident simulation exercise and submit such report to the person in control of the critical infrastructure as well as the National Commissioner.

(7) The provisions of this regulation do not detract from any other exercise required by an official regulatory authority in terms of other legislation.

CHAPTER 9

INSPECTIONS

47. Designation of inspectors

(1) Police officials designated as inspectors by the National Commissioner in terms of section 9 of the Act, must resort under the command and control of the Head of the Critical Infrastructure Protection Regulator.

(2) The National Commissioner may determine the requirements that need to be complied with before a police official is designated as an inspector, and more specifically—

(a) the rank level which may not be less than that of a Warrant Officer;

(b) the level of experience in inspections or physical security assessments under this Act or the National Key Points Act 102 of 1980;

(c) any recognised training that the person must have completed successfully; and

(d) the level of security clearance.

(3) A certificate issued to an inspector in terms of section 10(2) of the Act must be in the form of a card and contain the following minimum information:

(a) on the front of the certificate:

(i) a photograph of the inspector designated in terms of section 10(1) of the Act; and

(ii) the official insignia of the South African Police Service; and

(b) on the back of the certificate:

(i) the number, rank, full names and identity number of the inspector;

(ii) the words "*has been designated as an inspector in terms of section 10(1) of the Critical Infrastructure Protection Act No. 8 of 2019*";

(iii) the date on which the certificate was issued; and

(iv) the rank and name of the person issuing the certificate.

48. Inspections

(1) An inspection under section 11 of the Act may consist of the following:

(a) a physical security assessment for purposes of an application as contemplated in section 17*(b)* of the Act;

(b) a physical security audit contemplated in regulation 50; or

(c) a physical security evaluation of the physical security measures at a critical infrastructure facility contemplated in regulation 51.

(2) The National Commissioner may request—

(a) the State Security Agency;

(b) a regulating authority of a particular critical infrastructure or class of infrastructure; or

(c) any other relevant government organ,

to designate a suitably experienced member of that security service, regulating authority or government organ to assist with an inspection, when required.

49. Physical Security Assessment

(1) A physical security assessment is conducted to determine the level of physical security measures deployed at infrastructure where an application was lodged to declare that infrastructure as critical infrastructure.

(2) The purpose of a physical security assessment is to—

(a) verify the information in the application;

(b) assess the risk category in which such infrastructure or parts thereof may be categorised;

(c) confirm whether the current physical security measures deployed by the person in control of the infrastructure comply with the measures and standards prescribed in these regulations for the protection of the infrastructure; and

(d) provide the person in control of that infrastructure with an opportunity to make written submissions regarding the physical security assessment.

(3) An inspector must engage the security manager to arrange for a suitable date for such physical security assessment and may, where applicable,

consult an official contemplated in section 11(8) of the Act or an official designated by the State Security Agency.

(4) On the agreed date, the inspector must inspect the security measures deployed at the particular infrastructure to determine the existence thereof, as well as the quality and nature of those security measures.

(5) After the physical security assessment, the inspector must compile a physical security assessment report and, where applicable, do so in consultation with any official contemplated in section 11(8) of the Act or an official designated by the State Security Agency.

(6) The physical security assessment report must be classified in accordance with the Minimum Information Security Standards approved by Cabinet from time to time.

(7) A copy of the report must be submitted to the person in control who may make written submissions to the National Commissioner *via* the Head of the Critical Infrastructure Protection Regulator within 30 days after receiving the report.

(8) The report, with recommendations on the physical security measures and standards thereof, as well as the written submissions of the person in control, if any, must accompany the application for declaration as infrastructure as critical infrastructure for submission to the Critical Infrastructure Protection Council.

(9) In all cases where the infrastructure concerned houses or contains information technology needed for the functioning of society, the Government or enterprises of the Republic, the physical security assessment report must be submitted to the State Security Agency.

50. Physical Security Audit

(1) After declaration of infrastructure as critical infrastructure, an inspector may conduct a physical security audit of the physical security measures at that critical infrastructure.

(2) The purpose of a physical security audit is to determine whether—

(a) the conditions referred to in section 21(1)*(c)* of the Act which the Minister deemed necessary to impose for purposes of securing the critical infrastructure, were adequately complied with by the person in control;

(b) any other recommendations to the person in control on the physical security measures and standards of the critical infrastructure are necessary; or

(c) an incident at the critical infrastructure indicated a deficiency in the existing physical security measures.

(3) An inspector must engage the security manager to arrange for a suitable date for such physical security audit and may, where applicable, consult an official contemplated in section 11(8) of the Act or an official designated by the State Security Agency.

(4) In all cases where the infrastructure houses or contains information technology needed for the functioning of society, the Government or enterprises of the Republic, the physical security audit may be done with the assistance of an official designated by the State Security Agency.

(5) On the agreed date, the inspector must inspect the security measures deployed at the particular infrastructure to determine the existence thereof, as well as the quality and nature of those security measures.

(6) After the physical security audit the inspector must compile an audit report with recommendations and submit a copy of such report to the person in control.

51. Physical Security Evaluation

(1) After declaration of infrastructure as critical infrastructure, an inspector must, from time to time, conduct a physical security evaluation of the physical security measures at that critical infrastructure.

(2) The purpose of a physical security evaluation is to confirm whether the physical security measures at the critical infrastructure adequately comply with the conditions of declaration referred to in section 21(1)*(c)* of the Act as well as the measures and standards prescribed in these regulations.

(3) An inspector must engage the security manager to arrange for a suitable date for such physical security evaluation.

(4) On the agreed date, the inspector must inspect the physical security measures deployed at the particular infrastructure to determine the existence thereof, as well as the quality and nature of those security measures.

(5) After the physical security evaluation, and upon being satisfied that the physical security measures are in compliance with the Act and these regulations, the inspector must compile an evaluation report and submit a copy of such report to the person in control.

52. Compliance notices

(1) Where the person in control of a critical infrastructure refuses or fails to allow an inspector access to the critical infrastructure concerned, an inspector may issue a compliance notice to the person in control of the critical infrastructure, requiring of that person to provide an inspector with access to the critical infrastructure within seven days, for the purpose of conducting the inspection.

(2) The compliance notice must be in a form that corresponds with Form 5 of Annexure A to these regulations and set out the—

(a) name of the inspector concerned;

(b) purpose of the inspection;

(c) particulars of the infrastructure concerned;

(d) date or dates on which the inspector was refused access;

(e) date before which an inspector must be granted access, which must be within seven days of receiving the compliance notice;

(f) notification that refusal or failure to comply with a compliance notice may constitute an offence in terms of section 26(5)*(b)* of the Act; and

(g) the particulars of the person to whom the compliance notice was issued as well as the time, date and place of service.

(3) A compliance notice must be issued in accordance with section 11(7) of the Act.

53. Written notices

(1) Where an inspector has reasonable grounds to believe that any method or practice of safeguarding or securing the critical infrastructure in question or any failure or refusal to comply with this Act, may negatively affect the physical security measures of that critical infrastructure, such

inspector may issue a written notice contemplated in section 11(4) of the Act, to the person in control.

(2) The written notice must be in a form that corresponds with Form 6 of Annexure A to these regulations and issued in accordance with section 11(7) of the Act.

(3) A written notice must set out—

(a) the name of the inspector concerned;

(b) particulars of the critical infrastructure concerned;

(c) the date of inspection;

(d) particulars of the method or practice of safeguarding or securing the critical infrastructure in question, or the particular failure or refusal to comply with the Act or these regulations, which may negatively affect the physical security measures of that critical infrastructure;

(e) the steps that the person in control must take in respect of the physical security of the critical infrastructure to rectify the deficiency identified as contemplated in paragraph *(d)*; and

(f) the time period within which the person in control must take such steps;

(g) notification that refusal or failure to comply with a written notice issued in terms of section 11(4) of the Act, may constitute an offence in terms of section 26(5)*(b)* of the Act; and

(h) the particulars of the person to whom the written notice was issued as well as the time, date and place of service.

(4) In the event that a person in control fails or refuses to take any or all of the steps specified in the written notice and that failure or refusal creates a substantial risk of a threat being materialised, the inspector must compile a report on such failure.

(5) The report referred to in subregulation (3) must set out—

(a) the grounds on which the inspector believes that the physical security at the critical infrastructure will be affected;

(b) the possible risks created by such failure or refusal;

(c) possible risks created for other critical infrastructure; and

(d) steps proposed to mitigate the risk.

(6) The report referred to in subregulation (3) must be submitted to the National Commissioner for a decision whether failure or refusal of the person in control is of such a serious nature that—

(a) the matter should be referred to the National Prosecuting Authority; and

(b) a recommendation should be made to the Minister to exercise his or her powers in terms of section 11(5) or section 11(6) of the Act.

CHAPTER 10

SECURITY PERSONNEL

54. Definitions

In this Chapter, unless the context indicates otherwise—

"SASSETA" means the Safety and Security Sector Education and Training Authority established in terms of the Skills Development Act, 1998 (Act No. 97 of 1998);

"security equipment" means any physical resource, facility or equipment required to perform a security function at critical infrastructure and includes canine and equine resources;

"security officer" means an individual member of the security personnel contemplated in this Chapter and includes a security manager and a control security officer as may be required by the context;

"security personnel" bears the same meaning as in the Act and, for purposes of this Chapter, includes a security manager and chief security officer as may be required by the context

"suitable person" means a person who—

(a) is registered as a security officer in terms of section 21 of the Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001);

(b) is not disqualified in terms of regulation 60;

(c) completed a criminal record check by the South African Police Service;

(d) completed the relevant training courses related to critical infrastructure protection as set out in regulation 59; and

(e) complies with the relevant requirements set out in regulation 59.

55. Security manager

(1) A person in control of critical infrastructure must appoint a suitable person in the employ of that critical infrastructure as security manager to perform the functions set out in section 24(7) of the Act and to implement the conditions of declaration as critical infrastructure as contemplated in section 20(1)*(d)* of the Act.

(2) The person in control must ensure that the contract of employment between the critical infrastructure and the security manager contains—

(a) a provision that such contract is subject to the Act and these regulations; and

(b) a procedure in terms of which the appointment as security manager may be withdrawn in the event that the security manager is no longer a suitable person to be employed as a security manager.

(3) The provisions of subregulation (2) does not have retrospective application.

(4) A security manager must—

(a) be registered with PSIRA;

(b) in the case of a—

(i) medium- or high-risk critical infrastructure be registered as a grade A security officer; or

(ii) low-risk critical infrastructure be registered at least as a grade B security officer; and

(c) be in possession of a valid certificate of competency issued under regulation 58(4).

(5) In the event that a security manager becomes disqualified, the person in control must take the necessary steps to ensure that the appointment of that security manager as security manager is withdrawn.

56. Control security officer

(1) A person in control must, as may be required to implement the conditions of declaration as critical infrastructure as contemplated in section 20(1)(d) of the Act and for the effective implementation of the security policy and plan, appoint a number

of suitable persons in the employ of that critical infrastructure as control security officers to serve under the command and control of the security manager.

(2) The security manager must deploy a control security officer to be present at the critical infrastructure to manage the day-to-day safeguarding of that critical infrastructure and, more specifically, the deployment of security personnel and security service providers and their equipment in accordance with the security policy and plan for that critical infrastructure.

(3) In the case of medium- and high-risk critical infrastructure, the person in control must ensure that a control security officer is present at the critical infrastructure on a 24 hour basis.

(4) The person in control must ensure that the contract of employment between the critical infrastructure and the control security officer contains—

(a) a provision that such contract is subject to the Act and these regulations; and

(b) a procedure in terms of which the appointment as control security officer may be withdrawn in the event that the control security officer is no longer a suitable person to be employed as a control security officer.

(5) The provisions of subregulation (3) does not have retrospective application.

(6) A control security officer security must—

(a) be registered with PSIRA;

(b) in the case of a—

(i) medium- or high-risk critical infrastructure be registered as a grade B security officer; or

(ii) low-risk critical infrastructure be registered at least as a grade C security officer; and

(c) be in possession of a valid certificate of competency issued under regulation 58(4).

(7) In the event that a control security officer becomes disqualified, the person in control must take the necessary steps to ensure that the appointment of that control security officer as control security officer is withdrawn.

57. Security personnel and security service providers

(1) Subject to subregulation (2), a person in control of critical infrastructure must—

(a) appoint a sufficient number of security personnel; or

(b) appoint one or more security service providers with a sufficient number of security personnel in their employ,

to implement the conditions of declaration as critical infrastructure as contemplated in section 20(1)*(d)* of the Act and for the effective implementation of the security policy and plan.

(2) Before appointment of any security personnel or any security service provider, a person in control of critical infrastructure must—

(a) satisfy him- or herself that—

(i) such security personnel or security service providers are registered with the National Commissioner and issued with a certificate of competence to provide security services at critical infrastructure; and

(ii) each security officer is registered with PSIRA;

(iii) in the case of a—

(aa) medium- or high-risk critical infrastructure, each security officer is registered as a grade C security officer; or

(bb) low-risk critical infrastructure, each security officer is registered at least as a grade D security officer; and

(b) ensure that any agreement for the rendering of security services by such security personnel or security service provider contains a provision that the agreement is subject to—

(i) the Act and these regulations; and

(ii) the effective implementation of the security policy and plan.

(3) A person in control must, at the end of each calendar month, furnish the National Commissioner with particulars in connection with security personnel and security service providers which were deployed at the critical infrastructure concerned during that month on the applicable form available on the website of the South African Police Service at www.saps.gov.za.

58. Application for certificate of competence to render security services at critical infrastructure

(1) No person may render security services at critical infrastructure unless such person is in possession of a certificate of competence issued by the National Commissioner in terms of this regulation.

(2) Security personnel must, in order to apply for a certificate of competence to render security services at critical infrastructure, complete the applicable application form available on the website of the South African Police Service at www.saps.gov.za and submit the application form to the person in control of that critical infrastructure together with the following documents or information:

(a) full name and identity number of the applicant;

(b) a certified copy of applicant's identity document;

(c) a recent ID or passport photo of the applicant;

(d) two full sets of applicant's fingerprints;

(e) applicant's current residential and postal address and the addresses and places where he or she lived and worked during a period of five years prior to the date of his or her application;

(f) applicant's marital status;

(g) applicant's citizenship and, where applicable, particulars concerning his or her naturalisation or registration as a citizen;

(h) certified copies of applicant's educational and professional qualifications, including security-related qualifications;

(i) particulars of applicant's state of health;

(j) full particulars of any previous convictions; and

(k) any other document that the National Commissioner may require from time to time.

(3) On receipt of the application contemplated in subregulation (1), the person in control must lodge such application and accompanying documents with the National Commissioner.

(4) The National Commissioner must verify the information in the application and, upon being satisfied that the applicant is a suitable person, register the applicant on the database of security personnel held by the National Commissioner, and issue

the applicant with a certificate of competence in respect of the critical infrastructure in question.

59. Qualifications and requirements

(1) The National Commissioner may accept any security-related qualification accredited by SASSETA or PSIRA.

(2) Security officers must, in order to be registered as set out in regulation 58(4), have undergone training in the following subjects and matters:

(a) fire prevention and fire-fighting measures;

(b) handling of weapons, including firearms, where applicable;

(c) weapons which persons who pose a threat to critical infrastructure are likely, in the opinion of the National Commissioner, to use;

(d) medical first-aid measures;

(e) rules of the South African private and public law, and in particular those rules which are concerned with the execution, application and maintenance of security measures at critical infrastructure, including the provisions of the Act, these Regulations, the Criminal Procedure Act, 1977 (Act No. 51 of 1977), the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004), and the Criminal Matters Amendment Act, 2015 (Act, No. 18 of 2015);

(f) physical education;

(g) communications; and

(h) such other subjects or matters determined from time to time by the National Commissioner.

(3) Security officers performing certain functions must, in addition to the courses outlined in subregulation (2), comply with following additional requirements:

(a) a security officer who is required to carry a firearm in the performance of his or her functions must be in possession of the relevant valid competency certificate issued in terms of the Firearms Control Act, 2000 (Act No. 60 of 2000);

(b) a security officer who is required to use a service dog in the performance of his or her functions must—

(i) be registered with PSIRA as a dog handler; and

(ii) have successfully completed the relevant PSIRA approved canine-related courses;

(c) a security officer who is required to use a horse in the performance of his or her functions, must have successfully completed the relevant PSIRA approved equine-related courses; and

(d) a security officer who is required to use a drone in the performance of his or her functions must comply with the requirements of Part 101 of the Civil Aviation Regulations, 2011 and the Air Services Licensing Act, 1990 (Act No. 115 of 1990).

60. Disqualifications

(1) A person is disqualified from being appointed as a security manager, control security officer or as security personnel if he or she—

(a) is not registered with PSIRA;

(b) has in the preceding 10 years, in the Republic or elsewhere, been sentenced to imprisonment without the option of a fine in respect of—

(i) any offence of fraud, theft or corrupt activities under the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004), or any other offence of which dishonesty is an element; or

(ii) any offence under the Act, the National Key Points Act, 1980 (Act No. 102 of 1980), the Prevention of Organised Crime Act, 1998 (Act No,121 of 1998), the Financial Intelligence Centre Act, 2001 (Act No.38 of 2001), the Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001) or section 3 of the Criminal Matters Amendment Act, 2015 (Act No. 18 of 2015);

(c) has in the preceding 10 years been convicted of an offence in terms of the Act or the National Key Points Act, 1980 (Act No. 102 of 1980), irrespective of the sentence imposed, and was within five years after the conviction again convicted of an offence in terms of any of the said Acts and sentenced to a fine exceeding R1 000;

(d) is unfit to possess a firearm as contemplated in section 102 or 103 of the Firearms Control Act, 2000 (Act No. 60 of 2000);

(e) is an unrehabilitated insolvent;

(f) does not reside permanently in the Republic; or

(g) in the case of a security manager or control security officer, has a direct or indirect financial or personal interest in any security service provider.

(2) The National Commissioner may, on good cause shown and on grounds which are not in conflict with the objects of this Act, condone any disqualification contemplated in this regulation.

(3) A person in control must take steps to determine the fitness of a security manager to remain in the employ of the critical infrastructure as a security manager in the event that the particular security manager is no longer a suitable person.

61. Security equipment

(1) The person in control of critical infrastructure must ensure that security personnel employed or contracted by that critical infrastructure have access to sufficient security equipment to enable them to safeguard that critical infrastructure and perform the functions required by the security policy and plan.

(2) The person in control must ensure that security equipment is stored in a safe place within the critical infrastructure during times when it is not used by security personnel for the performance of security-related functions.

(3) Security personnel may not take any security equipment outside the boundary or security limit of the critical infrastructure except to perform security-related functions specified in the security policy and plan, or with the permission or on the authority of the person in control.

(4) Security personnel must, at all times, while performing functions at critical infrastructure, have the following documentation, cards or permits with them available for inspection by the security manager, control security officer, an inspector or any other person authorised by the National Commissioner:

(a) current valid PSIRA certificate;

(b) certificate of competence issued by the National Commissioner;

(c) where applicable, valid firearm permit;

(d) where applicable, the identity document issued by the relevant security service provider which must, at a minimum, contain the name and PSIRA number of the security service provider, the personnel number and name

of the security officer as well as a head-and-shoulder photograph of the security officer; and

(e) any other licence or permit which may be required in terms of national legislation.

(5) The security manager must ensure that an appropriately qualified security officer is designated to oversee the day-to-day management of any canine or equine working animals.

(6) The designated person referred to in subregulation (5) must ensure that national legislation relating to working animals is complied with and that the relevant records are kept as may, from time to time, be required in terms of any Ministerial directive.

(7) The Minister may, in terms of section 27(4) of the Act, issue a practice directive in respect of other equipment that must be maintained by security personnel, including but not limited to uniforms, bullet resistant vests, non-lethal weapons, canine and equine equipment, crowd management equipment,

62. Security Operations Centre

(1) The person in control of critical infrastructure must ensure that a Security Operations Centre is established at that critical infrastructure.

(2) The Security Operations Centre must comply with the minimum physical security standards determined by the Minister in terms of section 20(1)*(d)* of the Act.

63. Occurrence Book and registers

(1) A security manager must ensure that an occurrence book is kept in which a control security officer shall record full particulars of any incident that took place at that critical infrastructure.

(2) A security manager or control security officer must notify the relevant office of the Regulator as soon as practically possible of any incident which occurs or is committed at the critical infrastructure.

(3) In addition to the particulars of an incident, security personnel must record reports, handing over of duties, injuries, visits by supervisors, visits by inspectors or any other occurrence.

(4) The occurrence book must be available at all times for inspection by an inspector appointed in terms of the Act or by a person authorised thereto by the National Commissioner**.**

(5) A security manager must ensure that the following registers are kept separately from the occurrence book:

(a) a firearms register in which the particulars of—

(i) each firearm at the critical infrastructure;

(ii) each security officer to whom such a firearm is issued; and

(iii) the date and time of issue,

is recorded, together with any particulars required in terms of the Firearms Control Act, 2000 (Act No. 60 of 2000);

(b) an attendance register which where date and time of attendance of each of the security personnel at the critical infrastructure is recorded;

(c) a visitor's register in accordance with the security policy and plan of the critical infrastructure; and

(d) any other register that may, from time to time, be required in terms of any Ministerial directive.

64. Powers of arrest

(1) A security manager and a security officer may, in order to exercise the functions assigned to the security manager and security personnel in section 25 of the Act and, subject to subregulation (2), without warrant arrest any person reasonably suspected of committing an offence or attempting to commit an offence —

(a) set out in section 26 (1) of the Act; or

(b) which has a direct bearing on the security of that critical infrastructure.

(2) The provisions of subregulation (1) does not derogate from any power assigned to a person under Chapter 5 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977).

(3) A security officer who arrests any person must inform the control security officer immediately of such an incident and arrest.

(4) The security manager or control security officer must, without unnecessary delay, inform the provincial office of the Critical Infrastructure Protection Regulator of the arrest and record the incident in the occurrence book.

(5) The security manager, control security officer or security officer must, without unnecessary delay, hand such person over to the South African Police Service to deal with such person in terms of Chapter 5 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977).

65. Directive in respect of search of persons body

(1) The security manager at critical infrastructure may, under section 25(2)*(b)*(vi) and 25(5) of the Act, determine that any person entering or leaving critical infrastructure must be searched by the security manager or security personnel.

(2) A search of a person's body may, in terms of section 25(6)*(c)* of the Act, only be performed if—

(a) a reasonable suspicion exists that such a person did not declare a dangerous or prohibited object in his or her possession or under his or her control; and

(b) the manner of or place where the search is performed does not infringe upon the privacy and dignity of the person to be searched.

(3) Before a person is subjected to a body search, security personnel must, as far as possible, use a metal detector, other electronic equipment or canine resource to determine whether such person has any dangerous or prohibited object in his or her possession or under his or her control.

(4) Any search of a person's body must take place with strict regard to the right to privacy and dignity and must be in accordance with the provisions of section 25 of the Act and these regulations.

(5) A "pat-down search" contemplated in section 25(6)*(b)* of the Act is a search of an individual conducted by security personnel running their open hands over the person's outer clothing and must be utilised for purposes of section 25 of the Act and this regulation.

(6) In exceptional circumstances a person to be searched may be requested to remove a coat or other heavy outer garment which may prevent a proper pat-down search.

(7) Before a person is searched, he, she or they must be informed of—

(a) the purpose of the search; and

(b) the provisions of section 25(6)*(d)* of the Act in that a person to be searched must—

(i) be informed of the gender of the person who will conduct the search, the manner of search and the place where the search will be performed; and

(ii) be provided with an opportunity to express a preference regarding the gender of the member of the security personnel who must conduct the search.

(8) A body search must be conducted in private and not in a reception area. If a separate search facility is not available, persons being searched should be shielded from the sight of others, using a privacy screen or similar apparatus.

(9) A body search may only be conducted in the presence of another security officer of the same gender as the person being searched, subject to such person's preference under section 25(6)*(d)*(ii) of the Act.

(10) Where a body search reveals that the person who was searched has a dangerous or prohibited object in his or her possession or under his or her control, the person must be provided with an opportunity to hand over such dangerous or prohibited object to the security personnel for further handling.

(11) The security manager must ensure that a search register is maintained and that the following information is recorded for each body search—

(a) particulars of the person searched;

(b) particulars of preferred gender as contemplated in subregulation (6)*(b)*(ii);

(c) name of security officer conducting the body search;

(d) name of security officer present during the search as contemplated in subregulation (9);

(e) reason for body search;

(f) any dangerous or prohibited object found; and

(g) signature of the security officer conducting the body search.

66. Refusal for search or examination

(1) If a person entering the critical infrastructure refuses to subject him- or herself or the articles in his or her possession voluntarily to a search or examination by a security officer as provided for in section 25 of the Act, the security manager or

security personnel may refuse such person access to the critical infrastructure or any area, facility, building, asset or element of the critical infrastructure.

(2) If a person leaving the critical infrastructure refuses to subject him- or herself or the articles in his or her possession voluntarily to a search or examination by a security officer as provided for in section 25(5) of the Act, the security manager or security personnel may refuse such person egress from the critical infrastructure or any area, facility, building, asset or element of the critical infrastructure until such search or examination has taken place.

(3) The security manager or security personnel concerned must inform the person referred to in subregulations (1) and (2) of the provisions of section 26(1)(d).

(4) A security officer who is not a security manager or control security officer must, without unnecessary delay, report the refusal referred to in subregulation 2 to a control security officer, the security manager or the person in control, and in the meanwhile prevent such person from leaving the critical infrastructure or any area, facility, building, asset or element of the critical infrastructure or passing the security limit until the arrival of the control security officer, security manager or person in control.

(5) The person in control, security manager or the control security officer may grant permission to the person concerned to exit the critical infrastructure, if it appears to him or her that under the circumstances the granting of such permission does not, or is not likely to, affect the security of the critical infrastructure prejudicially, and that there exists no reason on the basis of which such person may be arrested.

67. Dangerous objects

(1) Whenever a person intends entering critical infrastructure, a security officer may take control of any dangerous object which, in his or her opinion, may cause injury to another person or threaten the safety or security of that critical infrastructure.

(2) The person in control must ensure that there is sufficient storage space at the security checkpoint to allow for safekeeping of dangerous objects such as firearms or other weapons, for the period that the person intending to enter the critical infrastructure, may be present at the critical infrastructure.

(3) In the event that a security officer is of the opinion that a dangerous object cannot be stored safely for safekeeping, he or she may remove such object to a safe place and inform the control security officer accordingly.

(4) Where a dangerous object may present a threat to the critical infrastructure, the control officer must report the matter to the police station of the precinct in which the critical infrastructure is situated.

68. Prohibited objects

(1) Whenever a person intends entering critical infrastructure, a security officer may take control of any prohibited object.

(2) The person in control must ensure that there is sufficient storage space at the security checkpoint to allow for safekeeping of prohibited objects such as cellular phones, cameras or other electronic devices, for the period that the person intending to enter the critical infrastructure, may be present at the critical infrastructure.

69. Search of arrested person

(1) A security officer may search the body of an arrested person to determine whether such person is in possession or control of any object which—

(a) is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence related to the critical infrastructure

(b) is intended to be used or are on reasonable grounds believed to be intended to be used in the commission of an offence related to that critical infrastructure;

(c) may afford evidence of the commission or suspected commission of an offence related to that critical infrastructure;

(d) may endanger any person present at that critical infrastructure; or

(e) may present any other threat to that critical infrastructure.

(2) Any object found during such a search may be seized by the security officer and must be handed over to the South African Police Service who must deal with such objects as required by the Criminal Procedure Act, 1977 (Act No. 51 of 1977) or any specific national legislation regulating the seizure of a specific object.

CHAPTER 11

GENERAL

70. Offences and Penalties

Any person who unlawfully—

(a) as a person in control, fails or refuses to take the steps specified in the notice contemplated in regulation 26(1);

(b) as a person in control, fails or refuses to take the steps specified in the notice contemplated in section 26(1) of the Act within the period specified in that notice referred to in regulation 26(2);

(c) as a person in control, fails or refuses to establish a Joint Planning Committee as required by regulation 27(1);

(d) as a person in control, fails or refuses to maintain a Joint Planning Committee as required by regulation 27(1);

(e) as a person in control, fails or refuses to designate a person as chairperson of the Joint Planning Committee as contemplated in regulation 29(1);

(f) as a chairperson of a Joint Planning Committee, fails or refuses to convene a meeting of the Joint Planning Committee as required by regulation 30(2);

(g) as a chairperson of a Joint Planning Committee, fails or refuses to convene a meeting of the Joint Planning Committee as required by regulation 31(2);

(h) as a person in control, fails or refuses to ensure that incident response simulation exercises are planned and carried out annually as required by regulation 46(1);

(i) as a person in control, fails or refuses to comply with regulation 55(2);

(j) as a person in control, fails or refuses to withdraw the appointment of that security manager as security manager as required by regulation 55(5);

(k) as a person in control, fails or refuses to appoint or deploy a sufficient number of control security officers as required by regulation 56(3);

(l) as a person in control, fails or refuses to take steps to determine the fitness of a security manager to remain in the employ of the critical infrastructure as a security manager as required by regulation 60(3);

(m) as a person in control, fails or refuses to ensure that security personnel employed or contracted by that critical infrastructure have access to sufficient security equipment as required by regulation 61(1);

(n) as a person in control, fails or refuses to ensure that a Security Operations Centre is established at critical infrastructure as required by regulation 62(1);

(o) as a security manager, fails to ensure that an occurrence book is kept at critical infrastructure as required by regulation 63(1);

(p) conducting a search in contravention of regulation 65,

commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment or, in the case of a corporate body as contemplated in section 332 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), a fine not exceeding R1 million.

71. Manner of service of notice

Unless specifically provided for in the Act or these regulations, any notice referred to in these regulations may be served by a police official delivering such notice to the person concerned by hand, registered mail, courier or electronic mail.

72. Repeal

The Interim Critical Infrastructure Protection Regulations, 2022 as promulgated by Government Notice No. 3387 in *Gazette* No. 48526 dated 5 May 2023, are hereby repealed.

73. Commencement

These regulations shall be called the Critical Infrastructure Protection Regulations, 2023, and shall come into operation on the date of coming into operation of the Act.

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Contact Centre Tel: 012-748 6200. eMail: info.egazette@gpw.gov.za
Publications: Tel: (012) 748 6053, 748 6061, 748 6065