GRA

GIBRALTAR REGULATORY AUTHORITY

The Role of the GRA on Cyber Security Compliance

Date 6th May 2022

CS 01/22

FOREWORD

This guide explains the role of the Gibraltar Regulatory Authority as the designated Competent Authority under Part 7 of the Civil Contingencies Act 2007.

CONTENTS

Background

The European Union ("EU") 2016/1148 Directive on Security of Network and Information Systems (the "NIS Directive"), provides legal measures to protect essential services and infrastructure by improving the security of their network and information systems ("NIS") used by those administering these.

The aim of the NIS Directive is to encourage a culture of security across sectors which are vital for our economy and society and, moreover, rely heavily on technology, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Organisations in these sectors are identified as operators of essential services ("OESs") and these must take appropriate security measures and notify serious incidents to the relevant national authority. Also, key digital service providers ("DSPs") (such as search engines, cloud computing services and online marketplaces) need to comply with the security and notification requirements under the NIS Directive.

The NIS Directive was formally transposed into Gibraltar legislation on 10th May 2018 and is found in Part 7 of the Civil Contingencies Act 2007 (the "Act"). Although Gibraltar is no longer in the EU, the requirements contained in the Act still play a key part in ensuring that Gibraltar has in place, an effective cyber security framework to protect Gibraltar's critical national infrastructure.

Competent Authority

Section 38 of the Act designates the Gibraltar Regulatory Authority ("GRA"), as the Competent Authority for the security of NIS in respect of designated OESs.

Under the Act, the GRA is responsible for the following:

- Regulating, supervising and enforcing compliance;
- Establishing a list of OESs;
- Establishing a list of DSPs;
- Investigating breaches;
- Issuing guidance to operators of essential services or DSPs;
- Drawing up Codes of Practice;
- Recording and reporting incident notifications; and
- Conducting or organising inspections.

Single Point of Contact

The Act also designates the GRA as the single point of contact ("SPOC") for the security of NIS for Gibraltar. The SPOC's role is primarily a liaison role, facilitating cross-border cooperation and communication.

Computer Security Incident Response Team

Her Majesty's Government of Gibraltar Information, Technology & Logistics Department, is the Computer Security Incident Response Team ("CSIRT") under the Act.

The CSIRT's role is to provide incident support and assistance to OESs on cyber matters. The responsibilities of the CSIRT include the following:

- monitor incidents in Gibraltar;
- provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

- respond to any incidents;

- provide dynamic risk and incident analysis and situational awareness;

- participate and cooperate in the CSIRTs network;

- must establish cooperation relationships with the private sector; and

- must facilitate cooperation by promoting the adoption and use of common or standardised practices for incident and risk-handling procedures and incident, risk and information classification schemes.

Operators of Essential Services

Under the Act, the GRA may designate an entity to be an operator of essential services ("OES") if it provides a service which is essential for the maintenance of critical societal or economic activities (an "essential service"), such service relies on NIS, and, if in the GRA's view, an incident affecting the provision of that essential service is likely to have significant disruptive effects on the provision of that essential service.

Section 35 of the Act gives the GRA powers to designate an entity as an OES. Before designating, the GRA must have regard to the following factors:

- the number of users relying on the service provided by the entity;

- the degree of dependency of the other relevant sectors on the service provided by that entity;

- the likely impact of incidents on the essential service provided by that entity, in terms of its degree and duration, on economic and societal activities or public safety;

- the market share of the essential service provided by that entity;

- the geographical area that may be affected if an incident impacts on the service provided by that entity;

- the importance of the provision of the service by that entity for maintaining a sufficient level of that service, taking into account the availability of alternative means of essential service provision; and

- any other factor the GRA considers appropriate to have regard to.

Obligations for Operators of Essential Services

Section 41 of the Act sets out the NIS obligations for OESs.

OESs must:

- take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of NIS which it uses in its operations; and
- take appropriate measures to prevent and minimise the impact of incidents affecting the security of NIS used by it for the provision of the essential services in respect of which it is designated as an OES, with a view to ensuring the continuity of the provision by it of those services.

Section 41(3) provides that the measures taken shall ensure a level of security of NIS appropriate to the risks posed. It is the responsibility of the OESs to demonstrate that they are complying with the security and incident notification obligations under the Act.

Cyber Assessment Framework

In order to comply with the requirements of the Act, the designated OES must take appropriate and proportionate technical and organisational measures to manage the risks to the security of NIS which support the delivery of essential services.

The Cyber Assessment Framework ("CAF") was developed to provide OESs and DSPs with a self-assessment tool and, in turn, provides the GRA with the capability to assess the extent to which OESs are achieving the required levels of cyber security. The CAF is based on the UK's framework and as such is quite general. The GRA liaises with the OESs to tailor the CAF to each specific sector. The OESs are required to work towards a set of 14 cyber security principles written in terms of outcomes.

The CAF is based on the following 4 main objectives:

- Managing security risk;
- Protecting against cyber attack;
- Detecting cyber security incidents; and
- Minimising the impact of cyber security incidents.

The CAF is further broken down into the specific principles that are based on sets of indicators of good practice.

Incident Notification

The Act also makes it mandatory for an OES to notify the GRA of incidents affecting NIS that have a significant impact on the continuity of the essential service.

There are two ways incidents can be reported to the GRA:

- Mandatory notifications under the Act by OESs (which are only required when the level of disruption caused by an incident meets a specified threshold); and
- Voluntary reporting by entities not designated as an OES or DSP.

Mandatory notifications

The Act requires OESs to notify the GRA of incidents without undue delay and no later than 72 hours after the OES is aware that a notifiable incident has occurred. The Incident Notification Form is available on the GRA's website.

The report should include:

- the operator's name and the essential services it provides;
- the time the NIS incident occurred;
- the duration of the NIS incident;
- information concerning the nature and impact of the NIS incident;
- information concerning any, or any likely, cross-border impact of the NIS incident; and
- any other information that may assist the GRA.

Upon receipt of a mandatory notification the GRA may, if it deems necessary, liaise with the CSIRT or any relevant body and ensure that communications are aligned with the OES or DSP and, if necessary, inform the general public about the incident and any actions to take.

Voluntary reporting of incidents

Entities not designated as an OES or DSP, may voluntarily report any significant cyber incidents to the GRA. This intelligence will assist the GRA to identify as early as possible any potential harmful activity that may be affecting other entities, including OESs or DSPs.

Any entity that provides a voluntary notification shall not have any obligations imposed on them. All voluntary notifications will be acknowledged and will assist the GRA in gaining an overview of the current risk to the critical national infrastructure. However, the GRA will not provide any feedback on any actions taken.

After receipt of a voluntary notification, the GRA may, if it deems necessary, liaise with the CSIRT or any relevant body.

The Voluntary Incident Notification Form can be found here.

Power of inspection

The powers granted to the GRA under section 49 of the Act allows for inspections of OESs. The GRA can also appoint an inspector to conduct the inspection on its behalf, as well as directing an OES to appoint an inspector approved by the GRA.

Section 49 mandates that OESs:

- pay the reasonable costs of the inspection;
- co-operate with the person conducting the inspection;
- allow reasonable access to their premises;
- must allow the inspector to carry out its duties relevant to the inspection by allowing the copying or removing of documents, including information held electronically; and
- must allow the inspector access to any person should the inspector seek any information relevant to the inspection.

Enforcement

Any enforcement action by the GRA will be dealt with on a proportionate basis, considering the seriousness of any contravention(s) of an OES' duties under Part 7 of the Act.

Such duties are set out in sections 41 and 42 of the Act as follows:

> ***The security duties of operators of essential services***
>
> *41(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.*
>
> *(2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information*

systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

The duty to notify incidents

42(1) An OES must notify the designated competent authority about any incident which has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident").

The occurrence of a "NIS incident" itself does not necessarily mean that there has been a failure by an OES to comply with its security duties or notification duties. The key factors for determining enforcement will be:

- *whether or not appropriate and proportionate security measures were in place and were being followed for OES' security duties in terms of section 41; and/or*
- *whether NIS incidents are notified to the GRA in terms of section 42.*

The GRA will follow the steps set out below:

Step 1: Advise and persuade

When any non-compliance is identified, the initial approach taken by the GRA will be to engage and discuss these with the OES. This will include discussing what the failing or deficiency is, how and when it should be addressed and in what timescale. The GRA may review any remedial actions proposed by the OES (including when these actions should be completed). Should this be appropriate, the GRA may follow up with further inspections to ensure these actions have been addressed appropriately.

The GRA may issue information notices under section 48 of the Act requiring the OES to provide specified information to support any assessment of compliance.

Step 2: Enforcement notice

Where the initial collaborative approach has not worked or is not appropriate and/or failings are not being addressed, a formal enforcement notice may be issued under section 50 of the Act. The enforcement notice will include the failings identified, the steps (if any) to be taken to rectify the failures, the time period in which they must be completed and how and when representations on the enforcement notice may be made.

Step 3: Penalty notice

Where the OES has failed to take adequate steps to rectify a failure identified in an enforcement notice or the GRA is not satisfied with the representations made by an OES in response to the enforcement notice, the GRA may impose a financial penalty under section 51 of the Act.

In determining the value of the financial penalty, the GRA will consider the appropriate and proportionate level within the prescribed limit by reference to the tiered limitations set out under section 51(6) of the Act.

If an infringement occurs which breaches Part 7 of the Act and another regulatory requirement or legislation, the GRA will have regard to this and where appropriate discuss the best approach.

Step 4: Reviews

It should be noted that section 52 of the Act sets out that an OES may request an independent review of penalty decisions taken by the GRA in order to challenge the following matters:

a) the grounds for imposing a penalty notice;

b) the sum that is imposed; and

c) the time period within which the penalty notice must be paid.

Any request to conduct a review must be made in writing and copied to the GRA setting out the reasons for requesting a review and any relevant evidence, within 30 days of receipt of the penalty decision.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
csc@gra.gi
www.gra.gi