GIBRALTAR REGULATORY AUTHORITY

2nd Floor, Eurotowers 4
1 Europort Road
Gibraltar

Tel: +350 20074636
Fax: +350 20072166
info@gra.gi
www.gra.gi

COMMUNICATIONS ACT 2006

DIRECTION ISSUED TO AUTHORISED NETWORK PROVIDERS ON NETWORK SECURITY AND INTEGRITY

DIRECTION NOTICE C04/18

In exercise of the powers conferred on it by Section 34B the Gibraltar Regulatory Authority hereby issues this Direction.

1. Introduction

Communications services play an ever more central role in the daily routine of citizens and consumers. The reliance of individuals and businesses on these services, and the networks which support them, is often not apparent until they fail in a visible way. The reliance on communications by other parts of the critical national infrastructure, such as power or transport, can also mean that its failures or security problems can be the cause of potentially very damaging consequences in seemingly unconnected sectors.

Until now the Electronic Communications Framework[1] ("the Framework") which governs communications regulation in Europe has sought to protect consumers by focussing on areas such as universal supply and effective competition in services, but has said little in relation to the security and reliability of their operation. However, revisions to this framework[2], which came into force in Gibraltar on the 26th May 2011 as a result of changes to the Communications Act 2006 (the "Act"), has changed this by imposing new requirements on providers of public communications service and networks, and on the GRA ("the Authority").

This document gives high level guidance on how the Authority will apply the new requirements. It sets out the main evidence we will be looking for from providers to demonstrate they have taken appropriate measures to manage security, in the event that we need to investigate this. It also explains the process for complying with the new requirements to report significant security breaches and outages to the Authority.

---

[1] DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ [2002] L108/33.

2 DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009.

The main requirements placed on providers by the changes to the Act can be summarised as follows:

- network and service providers must take appropriate measures to manage risks to security, in particular to minimise the impact on end users and interconnected networks;

- network providers must take all appropriate steps to protect, so far as possible, network availability;

- network and service providers must notify the Authority of breaches of security or reductions in availability which have a significant impact on the network or service.

Despite the limited amount of existing formal regulation, the majority of providers already take security and availability very seriously. In most cases there are clear commercial drivers for this, but corporate responsibility and reputation management also play a part. For these providers, we do not expect the new provisions will require significant changes to their existing activity. Where existing security activity is more limited, and there is an objectively justifiable reason for this, we aim to take a proportionate and flexible approach. However, it is likely that complying with the new requirements will impose a greater cost on these providers, relative to their size.

One area which will be new to all providers is the requirement to report significant incidents to the Authority. Having considered the thresholds given in this guidance, smaller providers may determine the reporting requirements will not apply to their networks or services. Where it does apply, the reporting process is intended to minimise the burden on providers as far as possible, while still ensuring no significant incidents go unreported. We expect that affected providers will have internal monitoring and incident management processes which already capture most of the incidents that will be reportable. Therefore, while reporting to the Authority will be new, the burden should be relatively low.

This document sets out a number of areas which we expect providers will normally need to have considered to demonstrate compliance with the new requirements. The precise measures required in each area will vary by provider, depending on the networks and services they operate and the customers they serve.

In summary, the areas are:

- risk management procedures;

- basic security measures;

- transparent information for customers;

- measures to maintain the availability of services;

- measures to protect interconnecting networks, either by compliance with established security standards, or equivalent activity; and

- reporting incidents which exceed the thresholds outlined in this guidance.

We expect to revise this guidance from time to time to reflect feedback from stakeholders and the experience gained from implementing the new requirements, for example in the operation of the reporting scheme in order to ensure the effective and proportionate implementation of the new Framework.

Background

This document provides high level guidance on the new requirements for providers of public electronic communication networks and services to maintain security and resilience, and to report significant breaches or outages to the Authority. These requirements were introduced by new measures in Section 34A and 34B of the Act which came into force on the 26th May 2011, in line with revisions to the Electronic Communications Framework by the European Commission.

The Authority's intention in publishing this document is to give affected Authorised Network Providers ("ANPs") clarity about our normal interpretation of the new requirements and the steps that should be considered to demonstrate compliance. We expect this guidance will be updated as required.

Security and resilience requirements

The Framework[3] set by the European Commission applies to all transmission networks and services used for electronic communications in European Member States. The Framework Directive is one of five Directives making up the Framework. It was originally agreed in 2002 and had in-built provision for review.

In November 2007, the Commission published a number of proposals for updating the Framework and these were agreed in November 2009. The revised Framework[4], among many other changes, extends the obligations on Member States, national regulatory authorities and industry in relation to the security of networks and services. These new obligations were introduced in Article 13a and 13b of the Framework Directive and Member States were required to implement them in national law by 26th May 2011.

This guidance applies to all ANPs.

These security and resilience requirements were introduced in Gibraltar by changes to the Act. These changes have largely been achieved by copying text from the requirements set out in Article 13a and 13b.

In summary, the changes are:

- network and service providers must take appropriate measures to manage risks to security, in particular to minimise the impact on end users and interconnected networks;
- network providers must take all appropriate steps to protect, so far as possible, network availability;
- network and service providers must report to the Authority breaches of

[3] See footnote 1 above.

[4] See footnote 2 above.

security or reductions in availability which have a significant impact on the network or service;

- The Authority must, where we think it appropriate, notify regulators in other Member States, the European Network and Information Security Agency (ENISA), and members of the public, of any reports received;

- The Authority must send an annual report of all significant reports received to the European Commission and ENISA;

- The Authority may require a network or service provider to submit to, and pay for, an audit of the measures they are taking to comply with the new requirements; and

- The Authority can use the information gathering and enforcement provisions in the Act to investigate, rectify, and penalise any infringement of the new requirements.

The first three bullets above represent new regulatory requirements on providers of public networks. It is not appropriate for the Authority to attempt to determine at this stage, and for all providers, what will be required to be compliant. Only ANPs themselves have sufficient understanding of the operation of their networks and services, the requirements of their different customers and the changing threats to security and availability which they face. In the first instance, it will be for ANPs to determine how the new legislative requirements affect them and take any necessary measures that result.

In the event that the Authority investigates any potential non-compliance, we will have to consider each case on its merits. However, the intention of this document is to present high-level guidance on how we will approach this issue. It explains our interpretation of the new requirements, and the steps we would normally expect ANPs to undertake in order to demonstrate compliance.

This guidance may be revised from time to time to reflect feedback from stakeholders and the experience gained from implementing the new requirements, for example in the operation of the reporting scheme. We will also update our guidance as necessary to reflect the final outcomes of ongoing work being led by the ENISA to develop a common approach to implementation across member states.

Many ANPs already have plans in place to ensure that their networks and services operate with an appropriate degree of resilience and security. In some cases, customers may have service level agreements with their providers, setting out the minimum level of service they expect, including availability and security measures. In practice this means that most providers, especially those serving customer groups with higher security or resilience demands, are likely to be doing much of what is required under the new obligations already.

For many companies, this focus on security and resilience represents a very significant investment. It may culminate, for example, in certification against key security standards.

One area which will be new for all ANPs is the requirement to notify the Authority of significant security or availability incidents. Even here however, most organisations

have well established internal incident management and reporting schemes, which are likely to generate the information required.

Article 13a(4) of the revised Framework Directive gives the Commission the ability to introduce technical harmonising measures in the future, based on European and international standards. This provision would allow the Commission to specify more precisely the steps ANPs have to take to comply with the new requirements. There is no indication at this early stage whether the Commission will exercise this option in the future. However, there are clear benefits from having a co-ordinated approach across Europe which can be achieved even without formal harmonising measures.

A harmonised European approach would benefit consumers as security and resilience issues may span international borders due to the interconnected nature of communications networks. This means that poor security in one country could potentially affect consumers in another. For industry, with many ANPs operating in multiple countries, a consistent approach across European countries is important. This will minimise the extent to which pan-European ANPs need to adopt a different approach in each country and ensure ANPs in one country do not incur a greater regulatory burden than in others. A further benefit would come from Member States generating and submitting the required reports to the Commission and ENISA using a consistent approach.

In light of these factors, ENISA has established the process to develop guidance on a common implementation approach across Member States discussed above. There are currently two main strands of work being undertaken:

- establishing minimum standards for ANPs. This aims to draw together existing technical standards and agree a minimum set that can be applied to all ANPs for the purposes of ensuring compliance with Article 13a; and

- reporting templates and metrics. This aims to define a common template for annual incident reporting to ENISA and agree on thresholds which will determine which incidents are to be reported and how they should be categorised.

The outputs of the ENISA process will not be binding on Member States but will be drafted with the intention of acting as a guide for national implementation. However, any formal harmonisation that the Commission subsequently imposes is required to take utmost account of ENISA's views. It is likely that the output of ENISA's current work would be used for that purpose if necessary.

Guidance for Providers

This section considers the new requirements placed on ANPs by Section 34A and 34B of the Act. It discusses how the Authority intends to apply the new requirements and what we consider this will mean for ANPs, both in terms of internal activity and in the reporting of incidents to us. This guidance sets out at a high level the main steps we think ANPs may need to take to be compliant with the requirements. If we take enforcement action against any ANP for potential non-compliance, we will normally be looking for evidence that these steps have been taken, or explanations of why any alternative approaches have been pursued.

Section 34A of the Act introduces the new requirements for ANPs to take the appropriate steps to manage the risks to their network and to minimise the disruption on end- users and interconnected networks:

Under Section 34A(1) providers will need to take steps to appropriately manage the security risks to their networks and services. 34A(2) and (3) clarifies that these measures should minimise the impact of security incidents on end users and on network interconnections and to take all appropriate steps to protect availability of their public networks. 34A(4) requires ANPs to notify the Authority of any breaches of security or loss of integrity.

The Authority's interpretation of security in this context is the usual meaning used in the context of information security, namely protecting confidentiality, integrity and availability.

These requirements do not imply the need to mandate specific process for ANPs to follow, and that ANPs are likely to take different approaches depending on the network and service type and the service levels offered to the customer.

The requirements under 34A can be summarised into five areas:

- management of general security risks;
- protecting end users;
- protecting network interconnections; and
- maintaining network availability; and
- notifying the Authority of any breaches or loss of service.

Management of general security risks

We expect that to be compliant with 34A(1), ANPs will need to undertake some degree of risk management and be able to demonstrate that a range of basic security measures have been taken. If we were to undertake an investigation into compliance, the Authority would normally expect to see documentary evidence of the risk management and security procedures used. Compliance with any relevant industry Codes of Practice covering security issues would also be beneficial in demonstrating compliance with the new obligations.

The appropriate degree of risk management will vary greatly between ANPs, depending on factors such as the scale of the network or service under consideration, its criticality and customer expectations. We understand that most ANPs already undertake risk management. For some this may involve compliance with specific, standards-based, risk management procedures. For others, the approach may be more informal.

As a minimum, we would normally expect that ANPs should periodically consider the main security risks to their networks and services and develop and implement a plan to undertake any appropriate management or mitigation.

For demonstrating that basic security practices have been adequately undertaken many larger ANPs are likely to be able to rely on their existing compliance with information security standards.

We will expect that all ANPs with networks or services within the scope of 34A will generally be able to demonstrate that appropriate activity against these topics have been undertaken. We understand that for some ANPs, especially smaller organisations, achieving formal certification may be inappropriate. In these cases, we will be interested to understand the decision not to obtain relevant certification and what other measures have been taken to ensure the issues above have been adequately addressed. We will expect to see documentary evidence of the steps that have been taken.

Protecting end users

Alongside the general requirements outlined above, we consider that appropriately protecting end users will require transparent information for customers and measures to maintain the availability of services.

In the context of protecting end users, we consider that protection of access to the emergency services is a special case on which we place particular importance. There are existing obligations under the Notice on General Conditions No. C08/2017[5] ("the Notice") requiring certain ANPs to provide such access and for them to meet requirements such as providing caller location information.

The range of measures that may be appropriately taken to protect end users from network or service security incidents is potentially very wide. To explain, it is unlikely, for example, to be appropriate to take the same measures to protect customers of a consumer internet access service as those of a service supporting the clearing of high value financial transactions. This makes it particularly difficult to give generalised guidance on what is required of ANPs in this area.

Some groups of end users place significant importance on the security of the services they purchase and the networks that underpin them and are well-placed to ensure their requirements are met. These customers, typically larger businesses, are likely to have contracts in place which specify the degree of protection they will receive and the commercial implications if this is not delivered. With informed customers such as these, and commercially incentivised providers, there is a strong likelihood that appropriate measures will be taken.

For smaller business and residential customers, these drivers may not be present, not least because these customers are less likely to have the resources or understanding to fully consider the security of the services they purchase.

One approach to addressing this potential issue would be for the Authority to specify the measures that must be put in place to protect these end users from security incidents. However, within these market segments, there is still a high degree of variability in customer requirements and hence appropriate measures. Additionally, ANPs are best placed to understand the needs of their customers. We therefore consider that the market remains the best mechanism to ensure security measures

[5] Notice on General Conditions C08/2017
https://www.gra.gi/communications/documents/notices/notice-on-general-conditions-c08-17

are appropriately matched to end users' needs, but that this mechanism can only function effectively with a suitable degree of customer transparency. This is not easy to achieve as it is a complex area, and the information should be made available in a way that can be readily understood.

We expect ANPs to provide information about the security of their services within three months of publication of this document to allow all customers to make informed purchasing choices. Service Level Agreements (SLAs) although complex and involve the management of commercial risk, we would expect that ANPs offering particular levels of security or availability can demonstrate they have taken appropriate measures to deliver them. We would therefore not normally expect to investigate the breach of an SLA, but repeated material breaches may be an indicator of a potential concern.

For service providers, we consider that the requirement to take appropriate steps to protect end users from the impact of security incidents includes appropriately protecting the availability or continuity of supply of their services. In the case of resellers, this in turn requires appropriate contractual arrangements to be in place with any wholesale suppliers, including network providers.

In considering any enforcement action, the Authority will take into account the technical and commercial feasibility of a service provider achieving the appropriate protection measures. For example, it may not be feasible for network independent undertakings to ensure the underlying network delivers the desired level of service continuity where there is no contractual relationship involved. In this situation we would still expect the relevant information made available to customers to be truthful.

Protecting network interconnections

The requirements to protect end users under 34A(2) are largely aligned with the commercial incentives of ANPs to look after their own customers. However, the interconnected nature of communications networks means that an ANP can influence the outcomes for end users beyond its own customer base – end users which it has no direct commercial interest in protecting. This leads to the need to ensure ANPs appropriately protect the security of one another when they come to interconnect.

Maintaining network availability

For the purposes of 34A(3) we consider that ensuring the continuity of supply of services means protecting its ability to provide continuity of supply for the services that use it. As with the general management of risks discussed above, we consider that in most instances the appropriate steps to protect availability are best determined by an ANP in light of their understanding of the nature of the network and the wholesale or retail services it supports, and the needs of their customers. Under any enforcement action, we would normally expect to see evidence that ANPs have considered the requirements of their customers and provided a suitable level of availability.

Where network providers offer wholesale services to service providers or resellers, we expect that the contractual arrangements between these parties will adequately deliver the level of availability which the service provider or reseller has purchased. In this situation we would therefore expect that network providers should deliver

levels of availability appropriate to their direct customers and that consideration of end user needs would be for the service providers or resellers.

An important exception to the principle that network providers should determine the appropriate levels of availability based on their customers' needs is for networks offering public access to the emergency services. For these networks, and the services they support, strict requirements for maintaining availability are imposed by the Notice[6], and will continue to apply. For those networks within its scope, we expect that compliance with the Notice will imply compliance with 34A(3).

Notifying the Authority of any breaches or loss of service

Section 34A(4) of the Act introduces requirements for ANPs to submit reports to the Authority on security incidents which have a significant impact on the operation or availability of their networks and services. In this section we set out the reporting process and provide guidance on the thresholds for reporting incidents to us.

For the purpose of this reporting requirement, we consider an incident to be an information or network security event which has a significant impact on the continuity of the communications network and services. This interpretation is in line with ENISA's working definition of incidents.

The reports submitted to the Authority are expected to contribute to a number of important outcomes:

- compliance of individual ANPs with the new security and resilience requirements;
- promotion of best practice for all ANPs;
- better informed policy decisions by the Authority; and
- reporting to government, the European Commission and ENISA to inform policy decisions by these bodies.

Under the requirements of Section 34A(5), where we consider it appropriate, the Authority is required to notify the national regulatory authorities (NRAs) in other member states and ENISA of the notifications they receive. We understand that the intention of this requirement is to warn other countries about incidents we have become aware of which may have cross border implications. 34A(6) similarly requires us the notify the public of an incident where we consider it in the public interest to do so.

For the majority of incidents, it seems unlikely that this type of onward reporting will be required. The cause and the effect of many incidents are likely to be localised in nature. For most issues which are truly cross-border, we expect ANPs will become aware of threats which may affect them, such as software vulnerabilities, independently. We also expect that as a result of their own implementation of Article 13a, other NRAs will already be aware of incidents affecting ANPs in their country. However, there may be occasions where our onward reporting will have value, for

[6] See footnote 5 above.

instance in allowing other NRAs to take action to mitigate against the impact of an incident.

While receiving incident reports, it is important to note that the Authority will not normally have a role in the real time management of incidents. Therefore, we are not planning to monitor received reports outside of normal office hours, although this may be reviewed if required following the introduction of the reporting arrangements. For the most major incidents, the Authority may occasionally need to provide input, or perform a co-ordinating role, in relation to certain aspects.

Section 34A(7) sets out the new responsibility for the Authority to submit an annual report to the Commission and ENISA summarising the notifications received and the action taken in response.

Reporting Approach

We are adopting a two-stage reporting process. The threshold for reporting in the first stage is set at a level intended to minimise the risk of significant incidents going unreported. We consider this particularly important in the early stages of the process when our knowledge of the nature and range of incidents, and which of them may prove to be significant, is necessarily quite limited. The opposing risk of imposing undue burden due to the volume of reports is mitigated by making these first stage reports as lightweight as possible. For incidents which require additional information, which we expect to be few in number, a second stage of follow up reports will be used. We may revise the process and the thresholds in light of the experience gained from operating it.

For most incidents, the initial report should be submitted within a few days of the incident, but where the incident may be life affecting (such as an outage with an impact on accessing the emergency services), we expect to be notified within 24 hours. For major incidents, for example multiple outages which affect a large area the Authority would also expect to be notified within 24 hours.

All initial incident reports should be submitted to the Authority via the Network Security and Integrity Incident Report Form found on the GRA website: https://www.gra.gi/communications/direction-issued-to authorised-network-providers-on-network-security-and-integrity

There may be incidents which are not initially viewed as sufficiently serious to be notifiable to the Authority, but which develop over time. Alternatively, it may not be possible to place an accurate value of the likely impact in the early stages of the incident. However, we expect to be notified as soon as the ANP could reasonably be expected to become aware that the incident has, or is likely to affect supply of service. Where precise data on any of the required fields, including the impact of the incident, is not available, an estimate should be included in the initial report.

In order to minimise any disruption to resolving the incident itself, the information required in the initial report is deliberately high-level and brief. The information to be reported includes the date and time of the incident or detection, the root cause and a summary of the impact.

For a small subset of the incidents that are reported to the Authority, we may request

additional information from the provider(s) concerned to understand the incident better, either as it develops or following its resolution. This may include additional data that we are required to include in our annual summary to ENISA, such as the measures taken post incident. This approach will also allow for the provision of more detailed follow up information, which may not be available during the incident itself.

Auditing and Enforcement

Sections 34B(1) and 34B(2)(b) of the Act set out the main additional powers given to the Authority in relation to security and resilience. Under 34B(2)(b) we can request that a network or service provider undergoes an independent audit of their security and resilience arrangements, at the provider's expense. 34B(1) extends the Authority's existing enforcement powers to enforcement of the obligations on security and resilience. We intend to use these new powers alongside our existing enforcement powers where we have concerns that a provider has not met the security requirements as set out in this guidance.

We may open investigations due to complaints or disputes which have not been successfully resolved through the company's complaint resolution procedure[7]. We may also open own initiative investigations where we become aware of a breach of this Direction that may merit further examination. These issues may be drawn to our attention from a number of sources, including:

- Pattern of incidents identified from consumer complaints or general trends in incident reports; or

- The lack of reporting of significant incidents.

Incident reports may form, or contribute to, the basis for an enforcement action in some cases. However, it is important to stress that there is no direct correlation between the Authority receiving an incident report and our launching an investigation. Indeed, the opposite may be true – the failure to report a significant incident may be grounds for enforcement action. We expect to receive more reports than the number of enforcement activities we will undertake. A request for more detailed follow up information about an incident does not imply that we are intending to open an enforcement action in relation to that incident. There are a range of reasons why we may require more information on a particular incident.

In addition to the enforcement powers, Section 34B gives the Authority the power to request that ANPs undergo an independent audit. We expect to use this only in a small number of cases. For example, where appropriate, we may ask for evidence from the provider to demonstrate that they have sufficient measures in place to manage the risks to their network. If we have concerns that remain unaddressed, we may request an independent audit to determine whether that provider has suitable risk management procedures in place.

In some cases, we may decide to take formal enforcement action to ensure compliance with the new requirements. We may ask a provider to undergo further audits to investigate whether the binding instructions have been followed.

[7] In line with Sections 14.3 & 14.4 of Notice on General Conditions C08/2017 and Regulation 29 of Universal Service and Users' Rights Regulations 2006.

2. Directions:

The GRA directs Authorised Network Providers to;

a) establish risk management procedures;

b) set basic security measures to ensure customer protection;

c) provide clear and transparent information for customers on the security measures which are included as part of the product or service they are purchasing;

d) establish measures to maintain the availability of services;

e) protect interconnecting networks;

f) report incidents to the Authority which compromise the security and/or integrity of a network or service.

3. Compliance:

This Direction comes into effect on the date of issue and Authorised Network Providers are required to comply forthwith.

Dated this 26th day of September 2018

Paul J Canessa
Chief Executive
Gibraltar Regulatory Authority