GRA

GIBRALTAR REGULATORY AUTHORITY

Guidance to understanding the Network and Information Systems Incident Report Notification

Date 6th May 2022

CS No. 04/22

FOREWORD

Under the provisions of section 42(1) of the Civil Contingencies Act 2007 (the "Act"), Operators of essential services ("OESs") must notify the Gibraltar Regulatory Authority (the" GRA") of any incident having a significant impact on the continuity of the essential service which that OES provides within 72 hours of becoming aware of an incident. Any such incident will be described as a Network and Information Systems incident ("NIS incident").

A NIS incident must be reported to the GRA, without delay, by submitting an Incident Notification Form available on the GRA's website, and which is also attached as an annex to this guide.

CONTENTS

Section A – Requirement to report

1. Network and Information Systems ("NIS") Incident Reporting

Incident reporting is invaluable to:

- build an understanding of the threats affecting the sector and provide early warning
- enable timely advice across the sector and cross-sector where appropriate
- support specific law enforcement response where required
- provide historical context when performing likelihood assessments in future

Operators of essential services ("OESs"), must notify the Gibraltar Regulatory Authority (the "GRA") about any incident which has a significant impact on the continuity of the essential service which that operator of essential services ("OES") provides ("NIS" incident) as per the requirements of section 42(1) of the Act. A NIS incident is an incident, which has an actual adverse effect on the security of network or information systems used in the provision of essential services with reference to the agreed sector specific thresholds.

When an OES becomes aware that an incident has reached the threshold for reporting, it must be reported to the GRA within 72 hours by submitting an Incident Notification Form, which is available on the GRA's website, and which is also attached in the Annex to this guide.

As a result of the notification, the GRA will be aware of the incident but does not have a role in providing support for incident response. Reporting the incident to the GRA will have no impact on how the response process is handled.

A cyberattack may not be immediately identifiable as such, and so OESs may want to look for one or more of the following:

- related security breaches, including physical
- data copied to OT environment or connection of unauthorised removable media
- suspicious requests and/or instructions
- known activation of software or script
- unauthorised access and/or configuration changes to security software

The failure to notify the GRA of a NIS incident is a contravention of section 42 of the Act. However, an incident is not necessarily a contravention of the Act and therefore may not lead to enforcement action being taken.

After receipt of the notification, the GRA may, if appropriate, liaise with the Computer Security Incident Response Team ("CSIRT") or any relevant body to ensure that communications are aligned with the OESs and, if necessary, the general public are informed about the incident and any actions to take.

2. Completing the NIS Incident Notification Report Form

The NIS incident notification report form (refer to Annex) should be completed as follows:

1. **"OES name"**: this should be the name of the OES.

2. **"Incident reference number"**: the reference number given by the OES (if applicable).

3. **"Date and time of occurrence"**: the date and time after becoming aware of the incident.

4. **"Date and time of resolution"**: the date and time when the incident was resolved (if applicable).

5. **"Brief description of incident"**: refer to Section B paragraph 4 of this guidance for commonly used terms when describing the incident.

6. **"Impact"**: refer to Section B paragraph 3.2 of this guidance where it explains in detail each of the categories.

7. **"Current state of incident"**: provide the ongoing state of incident.

8. **"Has the Gibraltar CSIRT been notified?"**: if the incident is severe, and has had a significant impact on your service, it may require the CSIRT to intervene.

9. **"Description of any or any likely cross-border impact"**: if the service relies on interoperability services outside Gibraltar, this may affect cross-border entities if a NIS incident arises.

10. **"Name and contact details for follow up"**: the person to liaise with post-incident.

3. Incident Recovery

The GRA will generally seek to ensure that any necessary regulatory intervention during an incident is kept to a minimum to ensure OESs have the necessary time to respond and recover.

When systems and equipment have been made safe by the OESs, there are further priorities. These may be in order of importance listed below:

1. Starting limited, degraded operation(s) where the risk to safety is acceptable, in accordance with accepted practice.

2. Returning the overall network system to 'normal state' of functioning.

3. Taking any and all remedial action where the point of breach has been identified.

4. Identifying, isolating and preserving evidence for forensic analysis.

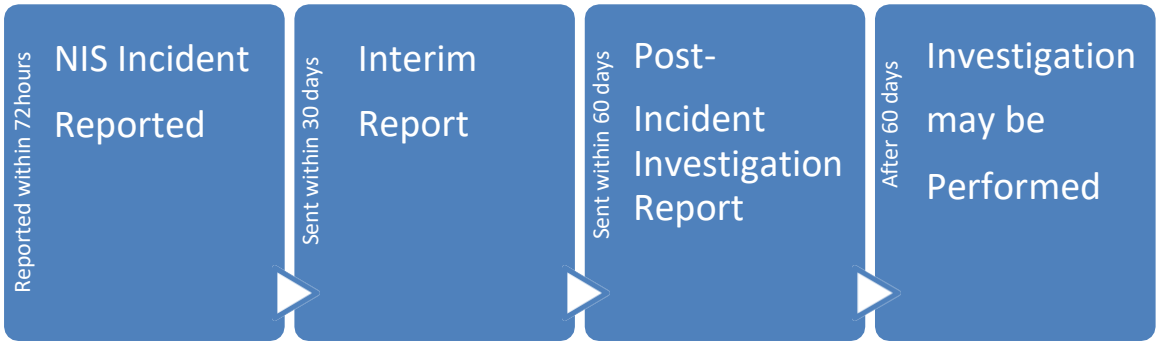
5. Internal investigation into how systems were breached (this should not interfere with any official investigation that may be conducted under section 38(2)(b) of the Act).

6. Remedial action(s) to prevent further breaches.

Affected systems and equipment should be put into a safe state to prevent harm or damage occurring after the initial incident has taken place.

4. Post-Incident Recovery

The diagram below is a high-level process flow in relation to reporting and investigation by the GRA.



Within 30 days of a NIS incident being reported by an OES, the OES is expected to submit an interim report to the GRA.

Within 60 days of a NIS incident being reported by an OES, the OES is expected to submit a post-incident investigation report with lessons learned, to the GRA. Although highly unlikely, it is noted that there may be circumstances that the incident is still ongoing at the 60-day mark. Should an OES believe it will not be able to meet this deadline, the OES should inform the GRA at the earliest opportunity.

Following the receipt of the post-incident investigation report, the GRA may decide whether or not the incident requires further investigation. The purpose of the investigation may be to:

- establish the cause of the incident and assess whether the incident was preventable;
- assess whether effective and reasonable risk management was in place;
- assess whether the OES had appropriate security measures in place; and/or
- assess how the OES responded to and managed the incident.

Should an investigation be appropriate, the GRA may use the OES developed post-incident investigation report as a basis for review. Once the investigation has concluded, the GRA may decide on any appropriate next steps. These may be no action, provision of advice, or carrying out formal enforcement action.

Where a cyberattack has taken place, OESs should consider the risk from further cyber-attacks and the likelihood of this occurring. OESs should capture lessons learned through formal reporting for continual improvement to manage times of crisis and disaster recovery. These lessons may be used to update OES's emergency response and contingency plans.

5. Digital Service Providers

Under section 43(3) of the Act, Digital Service Providers ("DSP") must notify the GRA of any incident that has a substantial impact on the provision of the service they provide. This is referred to as a "substantial incident".

A DSP must submit a substantial incident report within 72 hours after becoming aware of an incident by completing the Incident Notification Form which is available on the GRA's website, and which is also attached in the Annex to this guide.

Section B – Classification of Incidents

1. Introduction

This is divided into two core parts: The nature of the incident, and the impact on services.

2. Nature of the Incident

2.1 Root causes

The first part of the classification is used to classify the type of threat that triggered the incident and the severity of that threat. This can be subdivided into 5 root cause categories:

- **System failures** - The incident is due to a failure of a system, i.e. without external causes. For example, a hardware failure, software bug, a flaw in a procedure, etc. which triggered the incident.
- **Natural phenomena** - The incident is due to a natural phenomenon. For example, a storm, lightning, solar flare, earthquake, etc. which triggered the incident.
- **Human errors** - The incident is due to a human error, i.e. system worked correctly, but was used wrong, for example, a mistake, or carelessness which triggered the incident.
- **Malicious actions** - The incident is due to a malicious action. For example, a cyber-attack or physical attack, vandalism, sabotage, insider attack, theft, etc. which triggered the incident.
- **Third party failures** - The incident is due to a disruption of a third-party service, like a utility. For example, a power cut, or an internet outage, etc. which triggered the incident.

It is understood that the categorisation of the root cause may change over time, as more is known about the incident. Something that seems at first a cyber-attack, may turn out to be a human error, and vice versa.

2.2 Risks

The severity of the threat is used to indicate, from a technical perspective, the potential impact, and the risk associated with the threat.

- **High** – The actual or the potential impact high, with unrecoverable damages, disruption/denial of critical services, no solution available (for the moment), many systems could be affected.
- **Medium** – Potential impact is medium. The damages are recoverable, but there is a (possible) solution. Organisations following industry good practices should be able to protect themselves or recover without major extra efforts.

- **Low** – Low potential impact, but the issue requires some work.

2.3 Considerations

Some factors to take into consideration when assessing the severity of the threat are:

- Risks to your organisation, taking into account likelihood and potential impact;
- Amount of additional effort or costs needed to mitigate, protect or recover;
- Potential damages for your organisation, which could be caused by the threat;
- Rate of spreading (aggressiveness) of the threat, for example criticality of the vulnerability;
- Whether attacks are ongoing (attacks-in-the-wild);
- Criticality of the systems potentially affected (e.g. mission-critical supervisory control and data acquisition ("SCADA") systems);
- Feasibility or availability of solutions or protection measures, which mitigate the threat; and
- Adequacy of industry standard and industry good practices in mitigating the threat.

3. Impact of incident

3.1 Sectors

The second part of the classification is used to classify the impact of the incident on services, and which sector(s) of the economy and society are affected.

The sectors of the society and economy where there is an impact on the services can be one of the following, but is not necessarily limited to:

- **Energy** – The impact is in the energy sector and its subsectors such as electricity or gas, for example, impacting electricity suppliers, power plants, distribution system operators, transmission system operators, oil transmission, natural gas distribution, etc.
- **Transport** – The impact is in the transport sector and subsectors such as air, rail, water, road, for example, impacting air traffic control systems, maritime port authorities, road traffic management systems, etc.
- **Health** – The impact is in the health sector, for example, impacting the hospital, medical devices, medicine supply, pharmacies, etc.
- **Drinking water** – The impact is in the drinking water supply and distribution sector, for example impacting drinking water supply, drinking water distribution systems, etc.
- **Digital infrastructure** – The impact is in the digital infrastructure sector, for example impacting internet exchange points, domain name systems, top level domain registries, etc.

- **Digital services** – The impact is in the digital services sector, for example, impacting cloud services, online marketplaces, online search engines, etc.

3.2 Severity of incident

The severity of the impact is based on the level of disruption to Gibraltar, the level of risks for health and/or safety, the level of physical damages and/or financial costs. The severity of the impact is categorised as follows:

- **Catastrophic:** Use this category when critical services are severely disrupted for a long period of time and when there are serious cascading effects in multiple other critical sectors. High impact on economy and society, high risks for health and safety, high damages and costs.
- **Major:** Serious impact on government and/or essential services affecting a large proportion of the population and/or has substantial impact on economy. Significant risk for public health or safety.
- **Moderate:** Some disruption of critical services.
- **Minor:** Potential disruption of critical services but mitigated or impact is on non-critical services.
- **None:** Business as usual, no disruptions, unlikely to be any impact, hardly any damages or costs.

3.3 Factors to take into account

Factors to take into consideration when assessing the severity of the impact are:

- Risks for health and safety of the population, for example affecting emergency services;
- Impact on economy and society, for example causing high losses;
- Damages and costs for citizens and/or organisations affected;
- Disruption of daily life;
- Cascading effects in critical sectors;
- Media impact and coverage; and
- Political impact and significance.

In case a large number of organisations are affected by incidents with a minor impact, then there may be a large impact in society, in which case it may be more appropriate to indicate a higher level of severity for the incident.

4. Commonly used terms and classifications

The following labels can be used to categorise incidents and is particularly useful to further specify the nature of an incident:

- Abusive Content - For example, spam, harmful speech, defacement, etc.
- Malicious Code – For example, a worm, trojan, spyware, dialler, rootkit, etc.
- Information Gathering - For example, scanning, sniffing, social engineering, etc.
- Intrusion Attempts – For example, exploiting known vulnerabilities, login attempts, etc.
- Intrusions – For example, account compromise, unprivileged account compromise, application compromise, etc.
- Availability – For example, DoS or DDoS attacks, sabotage, outage (no malice), etc.
- Information Content Security – For example, unauthorised access to information, unauthorised modification of information, etc.
- Fraud - For example, unauthorised use of resources, copyright, masquerade, phishing, etc.
- Vulnerable - For example, a vulnerability open for abuse, etc.

Section C – Voluntary notification

Reporting of incidents

Any organisation may on a voluntary basis notify the GRA of cyber incidents that may have a significant impact on the continuity of the services they provide.

The GRA will acknowledge receipt of all voluntary notifications but will not provide direct feedback on how to resolve or mitigate the effects of a cyber incident. The GRA will collate all the information and, if deemed appropriate, will share the details of the incident with the relevant bodies including the CSIRT.

This intelligence will assist the GRA to identify as early as possible any potential harmful activity that may be affecting other entities, including operators of essential services, and will assist in developing appropriate guidance and alerts.

Voluntary cyber incidents may be reported via the GRA online notification form.

Annex – NIS Incident Notification Form

Cyber Security Compliance Division

This report should be submitted to incident@gra.gi

GRA
GIBRALTAR REGULATORY AUTHORITY

Network and Information Systems Incident Report Form

Operators of Essential Services (OESs) and Digital Service Providers (DSPs) should complete this form to report any cyber incident without undue delay and no later than 72 hours after becoming aware of an incident.

1	**OES / DSP name**			
2	**Incident reference number**			
3	**Date and time of occurrence**			
4	**Date and time of resolution**			
5	**Brief description of incident**			
6	**Impact:**	None ☐	Minor ☐	Moderate ☐
		Major ☐	Catastrophic ☐	Not yet known ☐
7	**Current state of incident:**	Reported or newly discovered ☐		Containment Achieved ☐
		Ongoing investigation ☐	Restoration achieved ☐	Incident Remediated ☐
8	**Has the Gibraltar CSIRT been notified?**		Yes ☐	No ☐
9	**Description of any or any likely cross-border impact**			
10	**Name and contact details for follow up**			

CONTACT US

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

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