

~~RESTRICTED~~



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOV.T.NZ

National Cyber Security Exercise

INTE SITY

Exercise After Action Report



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOVT.NZ

Handling Instructions

This document contains information for CYBER SECURITY STRATEGY COORDINATION COMMITTEE USE ONLY and is NOT FOR PUBLIC DISTRIBUTION.

Exercise INTENSITY was developed by a working group led by the National Cyber Security Centre (NCSC), with support from CERT NZ, NEMA, NZ Police, DPMC and DIA.

Enquiries in relation to any aspect of exercise INTENSITY including this document should be directed in the first instance to:

Cyber Resilience Unit
National Cyber Security Centre



info@ncsc.govt.nz

This INTENSITY after action report has been approved for release and dissemination as follows:

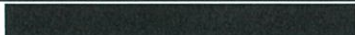
| Date | Approval | Endorsement by | Signature |
|-----------|----------|---|-----------|
| 1/2/2022 | Approved |  Cyber Resilience Unit (NCSC) | |
| 10/2/2022 | Approved | INTENSITY inter-agency steering group | |





Table of Contents

| | |
|--|------------|
| Handling Instructions | 2 |
| Executive Summary | 4 |
| Overview..... | 4 |
| Outcomes..... | 4 |
| Exercise Conduct | 6 |
| Overview..... | 6 |
| Planning and governance..... | 6 |
| Participation..... | 7 |
| Exercise Observations | 8 |
| Pre-ECG coordination..... | 8 |
| Use of the categorisation matrix..... | 8 |
| Escalation..... | 9 |
| Calling an ECG meeting..... | 9 |
| Collaboration and consensus..... | 10 |
| Communications..... | 11 |
| Industry feedback..... | 12 |
| [REDACTED]..... | [REDACTED] |
| Attachment A – Exercise INTENSITY Scenario | 16 |
| Attachment B – Supporting Evidence | 18 |
| Attachment C – CSERP Annexes for ECG | 19 |
| [REDACTED]..... | [REDACTED] |
| Attachment E – Supporting documents for special ideas | 24 |





Executive Summary

1. This report captures the key discussion points raised during INTENSITY, New Zealand's national cyber security exercise for 2021. The exercise successfully met the identified objectives of practicing and testing execution of the Cyber Security Emergency Response Plan (CSERP) and the Emergency Coordination Group (ECG) processes. s 6(a)

Overview

2. In late November 2021, the National Cyber Security Centre (NCSC) delivered a national cyber security exercise. Regular exercises are a key part of promoting a resilient and responsive New Zealand, a priority area of the National Cyber Security Strategy 2019. Exercises support the familiarity of officials with emergency response processes. The Cyber Security Emergency Response Plan (CSERP) recommends regular exercises to test its procedures and support regular review; and also required by the National Emergency Management Agency (NEMA) as part of its National Exercise Program.

Outcomes

3. This report provides a summary of observations from participants, facilitators, and dedicated observers involved in the exercise. s 6(a)
These observations have been reviewed by the inter-agency steering group and a summary is provided below.

Exercise Conduct

4. Feedback from participants indicated the exercise was successful. Participants provided feedback that the exercise both increased their familiarity with CSERP processes, as well as provided them with a valuable opportunity to learn more about other agencies' context. Recommendations from participants on future exercises focused on format, rather than substance.
5. Regardless of the modest scope, the exercise still involved significant planning, consultation, and facilitation, with a wide range of stakeholders. Although the majority of the work was performed by the NCSC's Cyber Resilience Unit, it relied heavily on input from other business units, the inter-agency steering group agencies s 6(a)
6. The support of an exercise steering group was essential to ensuring inter-agency buy-in and participation, as well as making sure the exercise was fit for purpose. This framework will be replicated for future national or sector-based exercises.





GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOV.TZ

Coordination and categorisation

7. There was an imbalance of knowledge across and within agencies regarding incident coordination at MAJOR as opposed to EXTREME. In the exercise scenario provided (see Attachment A) a potentially severe, but also reasonably common, incident highlighted that agencies conduct a large amount of coordination through “Business as Usual” relationships or forums outside the CSERP construct. There was not good visibility of these mechanisms amongst all agencies, despite the influence they had on perceived need for an Emergency Coordination Group (ECG) meeting.
8. The ECG’s success as a mechanism for coordination was heavily dependent on the ability to achieve consensus in a range of areas. Categorisation sits at the core of achieving consensus, where an agreed incident severity level determines the level of formality of coordination and leadership. A clear lead agency was a key dependency for building and maintaining consensus regarding other roles – such as communication. The exercise revealed that this is achievable using in-person roundtable discussion but depends on the appropriate level of representation.
9. It was unclear how this consensus is built and maintained in the face of changing or varying perspectives. s 6(a)
[REDACTED]
[REDACTED]
[REDACTED] When this risk was discussed during the exercise suggested solutions included physical “war rooms” or the need for clearer decision rights and leadership at each categorisation level.

Communication

10. The discussion on communication, both internal and external, also went beyond that described in the CSERP. Information sharing between agencies was a clear expectation, in order to service demands within individual agencies for information. Externally, it was clear that some pre-work would benefit a response; while the specifics of a particular incident could not be known prior, play books for certain general types of events could be agreed.

Industry roles and responsibilities

11. s 6(a)
[REDACTED]
[REDACTED] The INTENSITY table top exercise was planned to run in conjunction with the energy sector exercise (GridEx) s 6(a)
[REDACTED]
[REDACTED]
[REDACTED]





Exercise Conduct

Overview

12. The National Exercise was undertaken in two parts – participation in the industry-led GridEx held on 16 -17 November 2021 followed by the NCSC-hosted exercise INTENSITY held on 29 - 30 November 2021.
13. GridEx was a table top exercise where representatives of various energy companies participated remotely in a scenario s 6(a) Participants responded in real time to events as they happened.
14. INTENSITY was a facilitated discussion exercise. The exercise was based on the scenario described in Attachment A, which was provided to all participants ahead of the meeting. The NCSC provided a Facilitator to lead the discussion, as well as introduce “special ideas” that developed parts of the scenario to further explore focus areas.
15. INTENSITY was split into two sessions. The first followed the usual structure of an ECG as outlined in the CSERP (a link can be found in Attachment C). The second enabled further discussion and clarification of points from Day 1, and the continuation of the typical ECG agenda.
16. The date of INTENSITY was deliberately set so that it occurred after GridEx VI, s 6(a) This enabled the NCSC’s observations from participation in GridEx to be reflected in INTENSITY via the Facilitator, addressing questions raised by industry.

Planning and governance

17. The National Cyber Security Centre (NCSC) led national cyber security exercise planning, supported by an inter-agency steering group. This inter-agency group was formed to ensure the exercise reflected the objectives of all relevant agencies, the Cyber Security Strategy Coordination Committee (CSSCC), as well as the Department of Prime Minister and Cabinets (DPMC) National Exercise Program.
18. The steering group agreed the following focus areas for the exercise:
 - Using the categorisation matrix in the CSERP to understand what incidents constitute a MAJOR rating;
 - Testing coordination of s 6(a) incidents, where the need for national security system intervention is less clear and inter-agency collaboration is more paramount;
 - Processes of agreeing and handling communications during an incident; and
 - Involving industry directly to increase understanding of the processes of government.





GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOVT.NZ

Participation

19. In line with the CSERP, invitations were sent to the agencies listed below to nominate up to three people to participate in INTENSITY. These participants were not required to have a security clearance.
- CERT New Zealand (CERTNZ)
 - Department of the Prime Minister and Cabinet (DPMC)
 - Department of Internal Affairs (DIA)
 - National Cyber Security Centre (NCSC)
 - New Zealand Police (NZ Police)
20. Feedback was received from participants supporting the participant structure (one experienced participant, one with no previous experience, and a communications lead). It was noted that this was giving a broader range of people exposure to the CSERP processes and improving understanding of the dynamics in a cyber incident, particularly helpful for communications representatives.





Exercise Observations

21. Observations were formally collected in participant handbooks, via two observers, a minute taker, and the facilitator. The below represents an aggregation of these comments, as reviewed by the inter-agency exercise steering group.

Pre-ECG coordination

22. The NCSC informed the participants that a weekly operations meeting is held s 6(a)
23. This forum enables coordination for incidents that are 'on the fence', removing the need for default escalation. It also supports regular sharing of categorisation decisions, and a way to check whether agencies are applying it consistently.

s 6(a)

Use of the categorisation matrix

26. The basic concept behind the scenario (Attachment A) was the disclosure of a vulnerability in a commonly used network appliance which caused international panic within the IT community.
27. All parties agreed that with the information provided to them at the time, none of them would have called for an Emergency Coordination Group (ECG) immediately.

28. s 6(a)

29. The following observations were made during the categorisation discussion:

- s 6(a)
-
-
-
-

30. It was agreed that one objective of the ECG should be for agencies to reach agreement on categorisation of an incident, as the category of an incident dictates how CSERP processes are applied.





31. s 6(a) [Redacted]

32. s 6(a) [Redacted]

s 6(a) [Redacted]

Escalation

36. The facilitator asked the participants what information would be required to escalate this incident so that an ECG meeting would be called. It was agreed by all present that the following information would trigger an ECG:

- s 6(a) [Redacted]
- [Redacted]
- [Redacted]

37. These thresholds broadly reflect and validate the categorisation matrix in the CSERP.

Calling an ECG meeting

38. s 6(a) [Redacted] The group agreed that calling an ECG took priority





over other commitments, and there was sufficient membership coverage to get all agencies at each meeting. This reflects the fact that ECG's are not called regularly and only when absolutely necessary.

Collaboration and consensus

39. s 6(a) [Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

40. s 6(a) [Redacted]

41. s 6(a) [Redacted]

42. The lead agency identified by the ECG has the responsibility for producing an overview of the discussion and actions. Other than documenting decisions of the group, participants were not clear if the CSERP gave a lead agency additional authority to make decisions on behalf of the group.

43. s 6(a) [Redacted]

44. The NCSC noted that in the past, items discussed at the ECG have either escalated quickly into the National Security System or as more information has come to light and it has become apparent that the issue has not been as severe as first thought, the ECG has been disbanded. It was suggested that it may not be necessary to over structure the ECG and require it to deliver formalised outputs.





s 6(a)

[Redacted content]

48. s 6(a)

[Redacted content]

Communications

49. INTENSITY highlighted the need for consistent coordinated cross-agency communications at all levels, before and during incidents, to ensure effective cadence and visibility. s 6(a)

[Redacted content]

50. s 6(a)

[Redacted content]

51. s 6(a)

[Redacted content]

52. s 6(a)

[Redacted content]

53. s 6(a)

[Redacted content]





GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOVT.NZ

s 6(a) [Redacted]

54. s 6(a) [Redacted]

55. s 6(a) [Redacted]

s 6(a) [Redacted]

Industry feedback

s 6(a) [Redacted]

[Redacted]

[Redacted]

[Redacted]

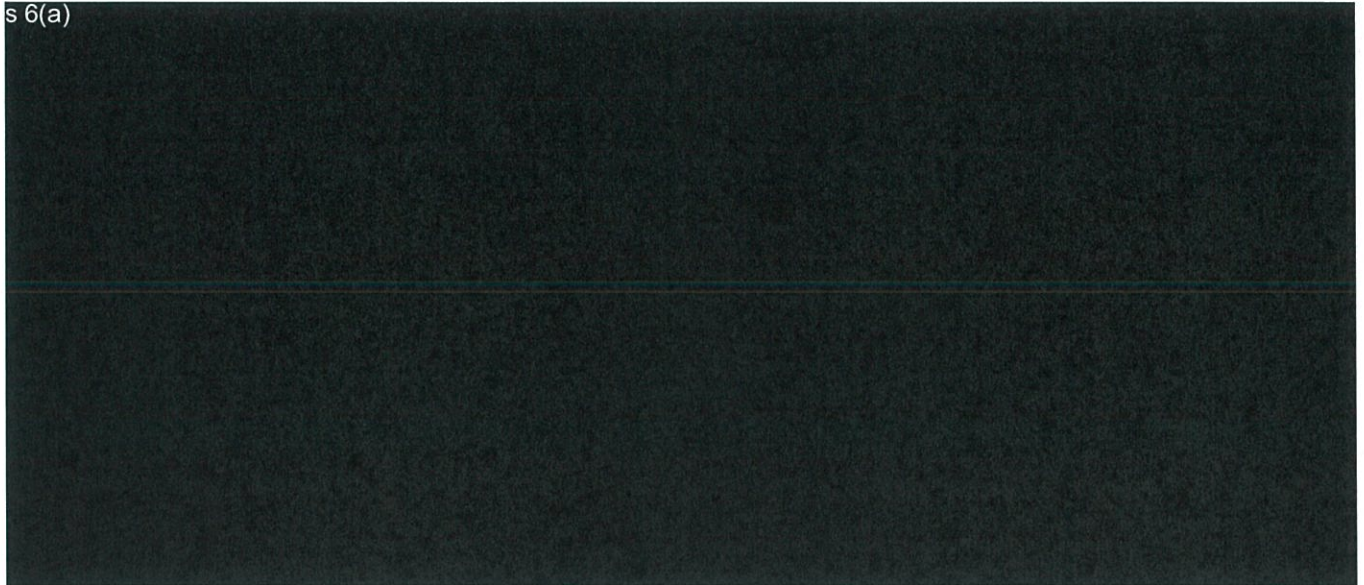


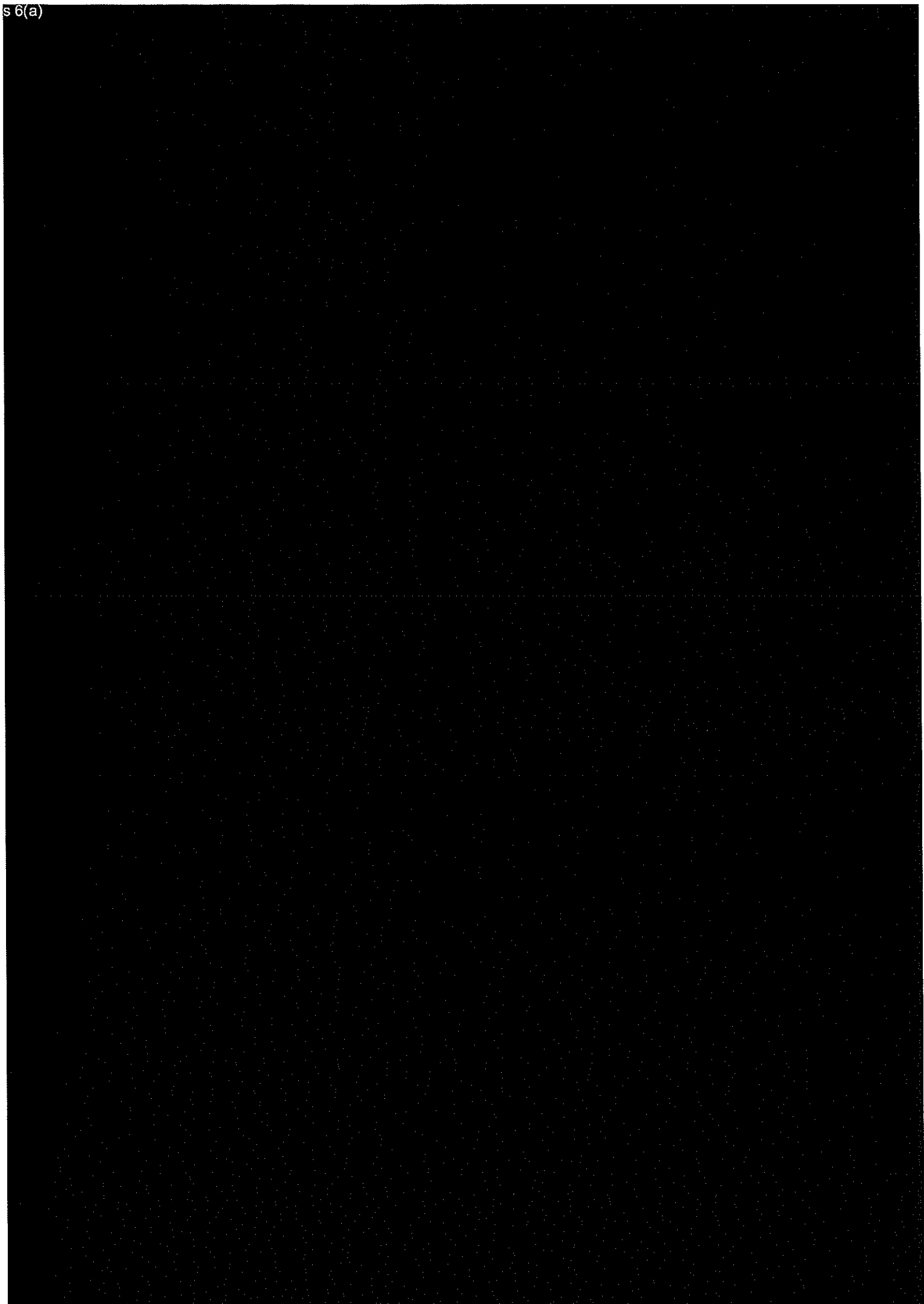


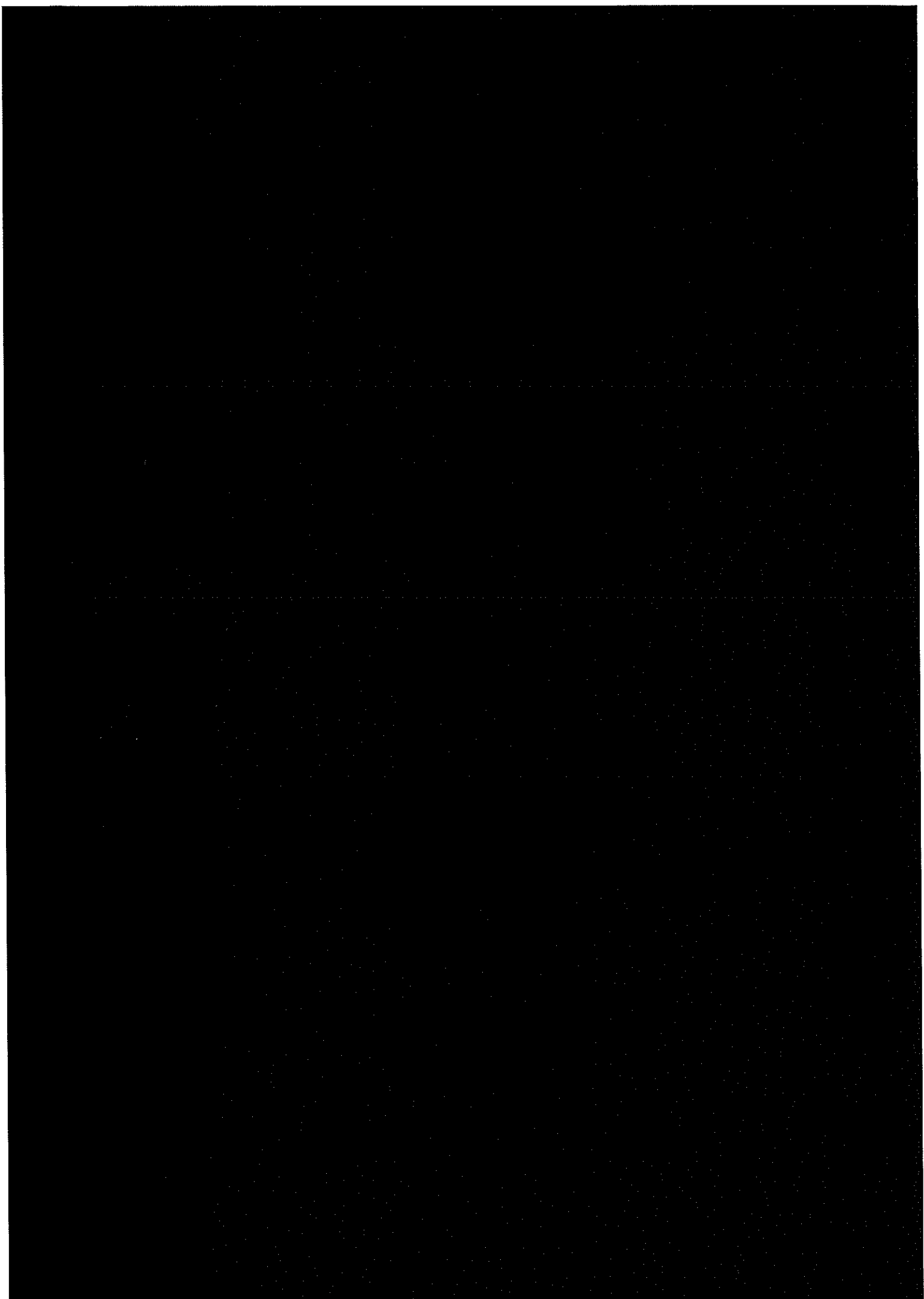
GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOVT.NZ

s 6(a)









Attachment A – Exercise INTENSITY Scenario

Summary

The disclosure of a vulnerability in a commonly used network appliance has caused international panic within the IT community. NCSC analysis of the vulnerability confirms theoretical severity.

Not a great deal is known about the actors trying to exploit the vulnerability or New Zealand's scope of exposure.

Awareness is low regarding the level of difficulty in exploiting actual implementations of the product, including the existence of compensating controls, the effectiveness of current mitigations, or the timeline to patch release.

Initial information suggests that, in worse case scenarios, this vulnerability could yield potentially complex compromises that might require additional coordination.

Timeline

Friday

A cyber security researcher releases a blog post about a vulnerability in a VPN made by OnlyConnect, a company located in a non-Five Eyes country. OnlyConnect's VPN is in the top 10 most used VPNs in the world.

The researcher is releasing the information after the 90-day responsible disclosure period has lapsed. In the blog, the researcher claims that despite multiple attempts to contact the company, OnlyConnect have refused to engage with them about the vulnerability.

The blog post hints that a remote code execution is possible using a vulnerability in the VPN authentication service. This would allow remote unauthenticated users to obtain access and modify files on the VPN management server.

Sunday

A well-regarded dark web monitoring company tweet a teaser from an upcoming report. They say that unattributed actors are talking about the OnlyConnect vulnerability in a dark web forum. The actors claim that they have found the vulnerability and developed an exploit.

The news is being retweeted extensively in the cyber security community. The online conversation reveals the breadth of organisations using the VPN, including extensive use in the US energy sector.

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.





GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOV.T.NZ

In response, OnlyConnect have announced that they are working to fix the vulnerability, but have no timeframe on the release of the patch. They advise customers to implement compensating controls, including a recommended change to server configuration that removes the vulnerability.

The Twitter community blasts OnlyConnect when it is discovered that this re-configuration breaks functionality for basic authentication and older VPN clients. Experts start recommending turning off the VPN until OnlyConnect release a patch.

Monday

The potential seriousness of the rapidly developing situation becomes apparent as people arrive at work on Monday morning.

As New Zealand Government staff arrive, they begin completing basic due diligence, which reveals the following:

- A classified partner report from six months ago which advises that an unattributed group has a pattern of using previous OnlyConnect vulnerabilities. s 6(a)
- Upon outreach to New Zealand resellers of OnlyConnect, they refuse to pass on information about their customers, citing confidentiality clauses in the contracts. However, they noted that when a patch is available it will be pushed to customers receiving their managed maintenance plan.
- Some incident reports were received over the weekend, but nothing with a clear OnlyConnect link.
- s 6(a)
-
- Emails between international partners, including NZ, suggests that advisories on the vulnerability are being developed.
- News stories about the vulnerability are starting to cross over from Twitter and appear in the mainstream media.

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.





Attachment B – Supporting Evidence

OnlyConnect

OnlyConnect are a cyber-security company based in a non-Five Eyes country. The VPN product affected is intended for <250 simultaneous users, but is also intended for use at branch sites as a part of larger deployments.

While the company's exact presence in New Zealand is unknown, there are two resellers in New Zealand: one based in Auckland, and one in Christchurch. Neither will provide information about who their customers are. The website of one of the resellers lists the following as key clients, but not what products or services they receive:

- A District Health Board (DHB)
- An electricity distribution company that provides power to a city in the South Island
- A large manufacturing company
- A fuel supplier
- An electricity distribution company that provides power to a city in the North Island
- A specialist manufacturing company
- An industrial processing facility
- A South Island port
- A logistics company
- A crown research institution

Blog post about the vulnerability

Zero-Day Disclosure: OnlyConnect VPN



[Janae Washington](#)

10:44 am, November 26, 2021

A memory corruption vulnerability exists in **OnlyConnect** VPN authentication service that enables an unauthenticated network-based attacker to modify system files and potentially execute arbitrary code with root privileges.

A sample curl command to test for the vulnerability is:
Curl <https://<server>/authmgt/././vpns/portal/scripts/auth.pl>

If this command is successful then the server is vulnerable to exploit, the memory corruption bug exists in the old authentication script used for basic-auth.

Further details will be available, but at present **OnlyConnect** refuse to acknowledge the bug and are not responding to our emails.

We are posting this blog post to raise awareness for users of **OnlyConnect**.

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.





Attachment C – CSERP Annexes for ECG

Annex A – Guide for Members of Cyber Security Emergency Coordination Group

Purpose of a Cyber Security Emergency Coordination Group

The Cyber Security Emergency Coordination Group may be charged with coordinating the government response to a cyber security emergency with a MAJOR severity rating. Specifically, it is responsible for:

- confirming (or identifying) the strategic aim(s) and supporting objectives that will determine the government's response;
- identifying key risks;
- overseeing the implementation of an action plan (including communications material); and
- Ensuring that appropriate recovery procedures are designed and implemented.

Composition of a Cyber Security Emergency Coordination Group

Depending on the nature of the incident, a Cyber Security Emergency Coordination Group will typically be chaired by the Director CERT NZ, the Director National Cyber Security Centre, the Director National Security Policy Directorate, DPMC, or a senior representative from NZ Police.

The membership of a Cyber Security Emergency Coordination Group is comprised of senior officials from government agencies with a role in incident response. Attendees reflect a balance of operational, communications and policy expertise. While the agencies involved are likely to vary on a case-by-case basis, the group will likely include the

- Department of the Prime Minister and Cabinet
- National Cyber Security Centre
- CERT NZ
- New Zealand Police
- Department of Internal Affairs

Other government agencies and private sector organisations may be involved as required.

Your role within the Cyber Security Emergency Coordination Group

The Cyber Security Emergency Coordination Group will look to you for current information on the impact of the emergency on your organisation, any measures that your organisation is taking in response to the incident (including communications) and any assistance that your organisation would like from government agencies.

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.





GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOV.T.NZ

Other groups which may be activated in response to this incident

Depending on the impacts of the emergency, a Watch Group may be established. Details on the form and functions of a Watch Group are contained in the National Security System Handbook. A copy is available at: <https://www.dpmc.govt.nz/sites/all/files/dpmc-nss-handbook-aug-2016.pdf>

Please note a full copy of New Zealand's Cyber Security Emergency Response Plan is available at: <https://dpmc.govt.nz/publications/new-zealands-cyber-security-emergency-response-plan>

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.





GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOVT.NZ

Annex B – Cyber Security Emergency Coordination Group agenda template

The Cyber Security Emergency Coordination Group Chair is responsible for producing and circulating the Cyber Security Emergency Coordination Group agenda and the meeting record – which should capture the decisions made, the rationale for those decisions, and any actions for follow up. The agenda for the first meeting will typically include:

1. **Introduction**
 - a. Decisions that need to be made immediately
 - b. Governance
 - i. Lead Agency
 - ii. Spokesperson(s)
2. **Situation update**
3. **Assessment**
4. Confirm **strategic purpose and priorities** (this will inform decisions)
5. Consideration of **key risks and implications**
6. **Communications** (public information)
7. **Support requirements and resources**
 - a. Activation of appropriate plans and legislation
 - b. Tasking of additional resources if required
 - c. Activation of specialist support if required
 - d. Support for Ministers
8. **Decisions and action items**

Next meeting

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.



This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.

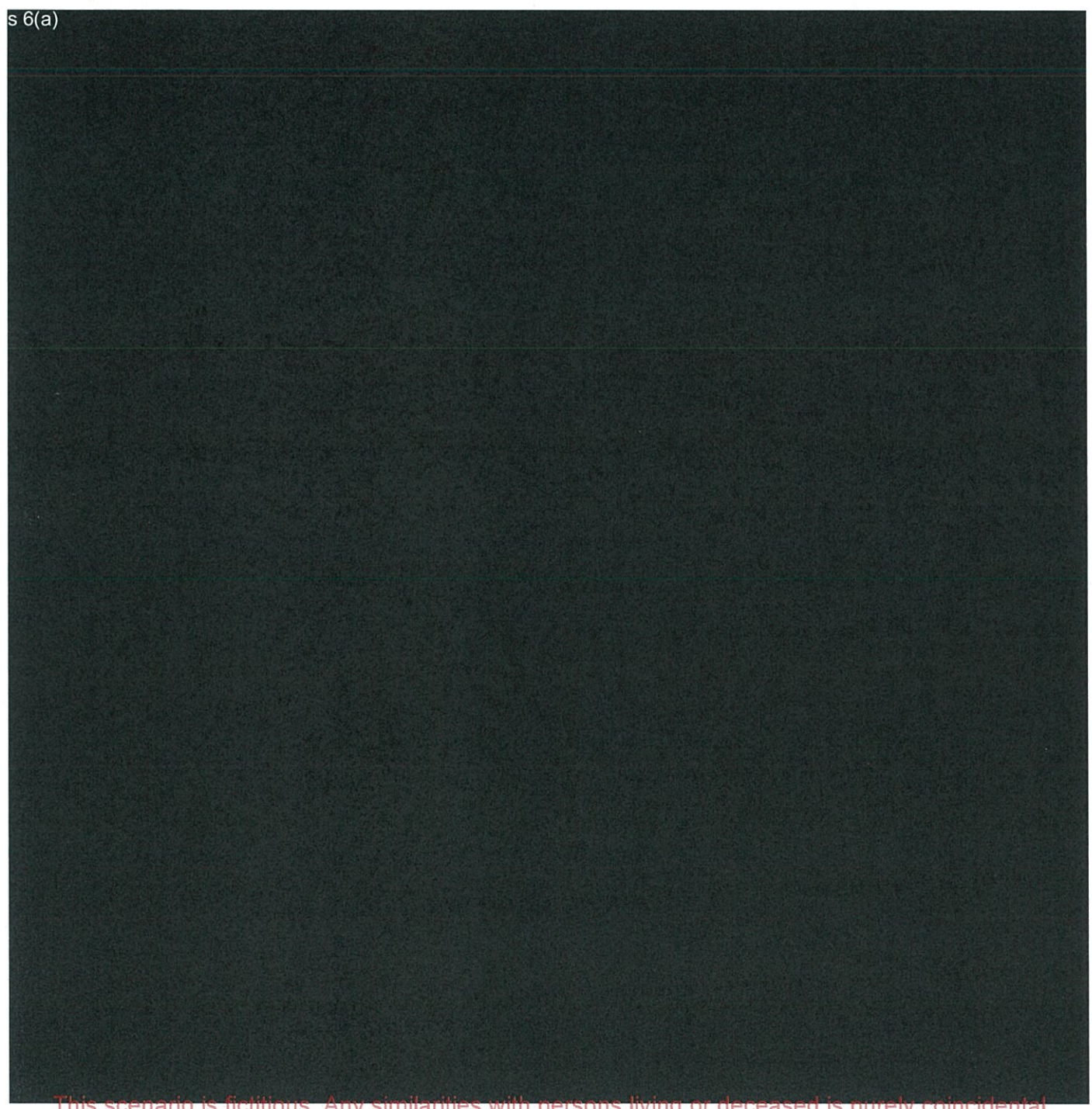
This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOVT.NZ

Attachment E – Supporting documents for special ideas



This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.



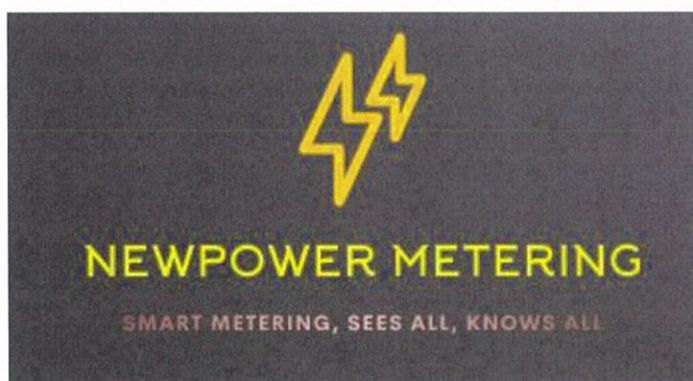


GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

NCSC National Cyber
Security Centre
NCSC.GOV.T.NZ

s 6(a)

Dunedin Company



The company **NewPower Metering** contacts CERT and the NCSC to report that they have suffered a ransomware incident at their main office in Dunedin, and their secondary office in Invercargill. They have no access to any of their computer systems and are requesting support. When asked they confirm that they use the VPN as they have a handful of staff who are based around the country and work from home. They also state that they currently do not have MFA in place for any of their accounts.

They have received a ransom note asking for 5BTC for the decryption key.

They have called in an incident response company for help, and it was recommended that they report this event to CERT/NCSC/Police.

The company has only been operating for 18 months but has already been featured in multiple online articles touting their work in smart metering for energy companies.

This scenario is fictitious. Any similarities with persons living or deceased is purely coincidental.



