IONIZE

Report Developed for the Digital Transformation Agency

CovidSafe Penetration Test

Table of Contents

Document Control

Document Details	Description
Title	CovidSafe Penetration Test
Author	s 22
Version	1.0
Last Modified Date	26/05/2020
Release Date	26/05/2020
Release Status	Finalised Version
Document Authority	s22

Version	Date	Author	Reason
0.1	15/05/2020	s 22	Initial Version
1.0	26/05/2020	s 22	Finalised Version

Key Terms

The following table contains a listing of key terms used throughout this document.

Term	Meaning
Android	The open source operating system used on Android mobile devices
APK	Android Application Package – The package file format used by the Android operating system for distribution and installation of mobile applications
API	Application Programming Interface – A set of functions exposed by a server that clients can call to perform actions such as retrieve or save data
IPA	iOS App Store Package – The package file format used by the Apple for distribution and installation of mobile applications
iOS	iPhone Operating System – The operating system used on Apple mobile devices
OWASP	Open Web Application Security Project – an industry standard for web application security testing
SDK	Software Development Kit

Executive Summary

During the period between the 24th of April and the 6th of May, Ionize conducted a penetration test against the CovidSafe source code, mobile applications, and backend infrastructure. The key goals for testing were to ensure the confidentiality, availability and integrity of user data submitted to the application. Special focus was placed on potential reputational damage, as, due to its prominence, the app was likely to be reverse engineered by members of the public, and potentially criticized for any unusual behaviour.

s 33

Suggested remediation for each of the issues has been included in the report. It is recommended that all the risks identified are assessed by the organization's internal risk assessment processes to determine if further action should be taken.

Introduction

Background

The Digital Transformation Agency enlisted the help of Ionize to conduct a source code review, mobile application pentest, and infrastructure analysis of the CovidSafe application.

Objective

The primary objective of the security testing was to provide Digital Transformation Agency with assurance that the CovidSafe applications are not susceptible to attacks by malicious actors, do not expose its users to unacceptable risk and do not expose Digital Transformation Agency to reputational risk.

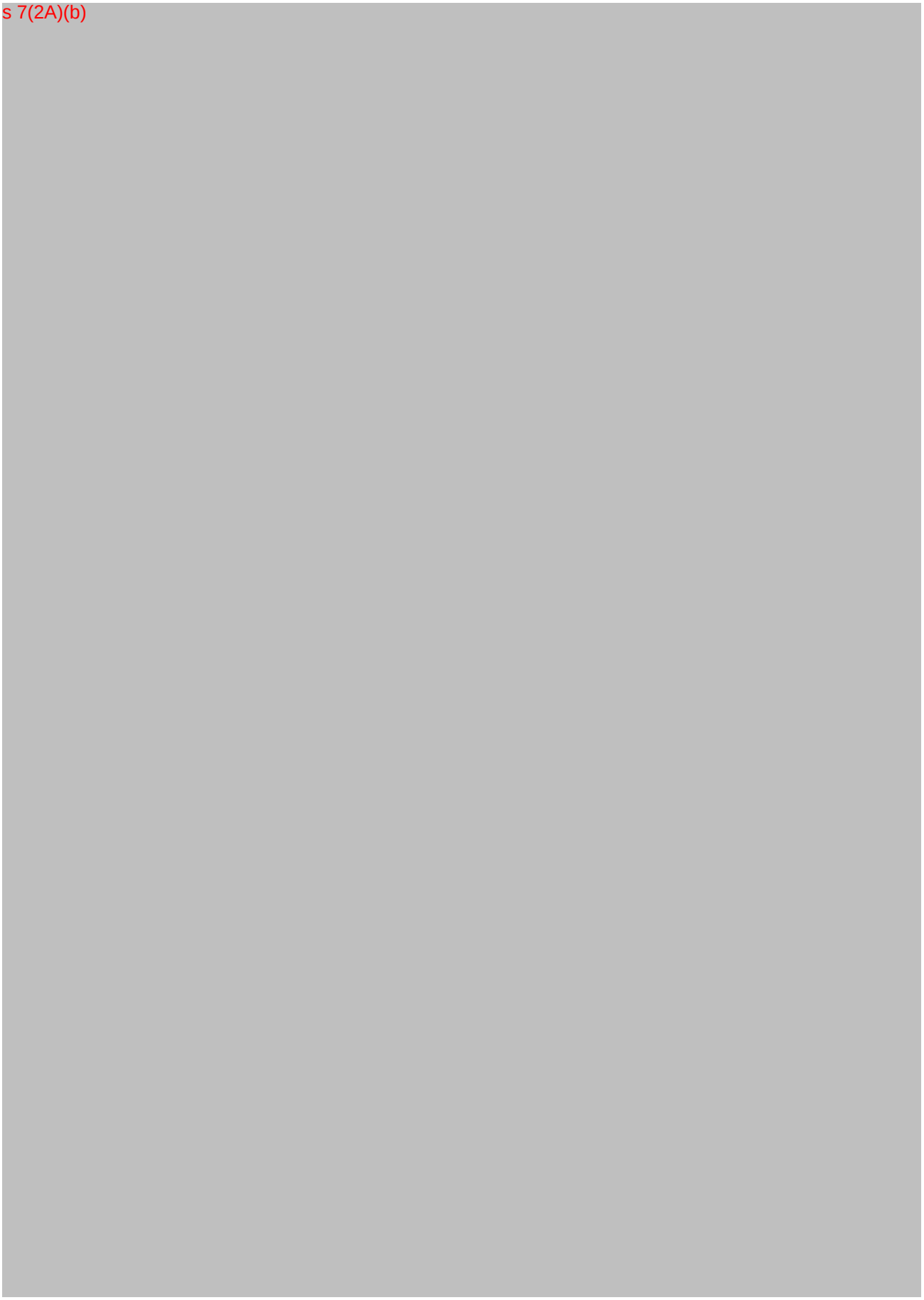
Scope

s 33

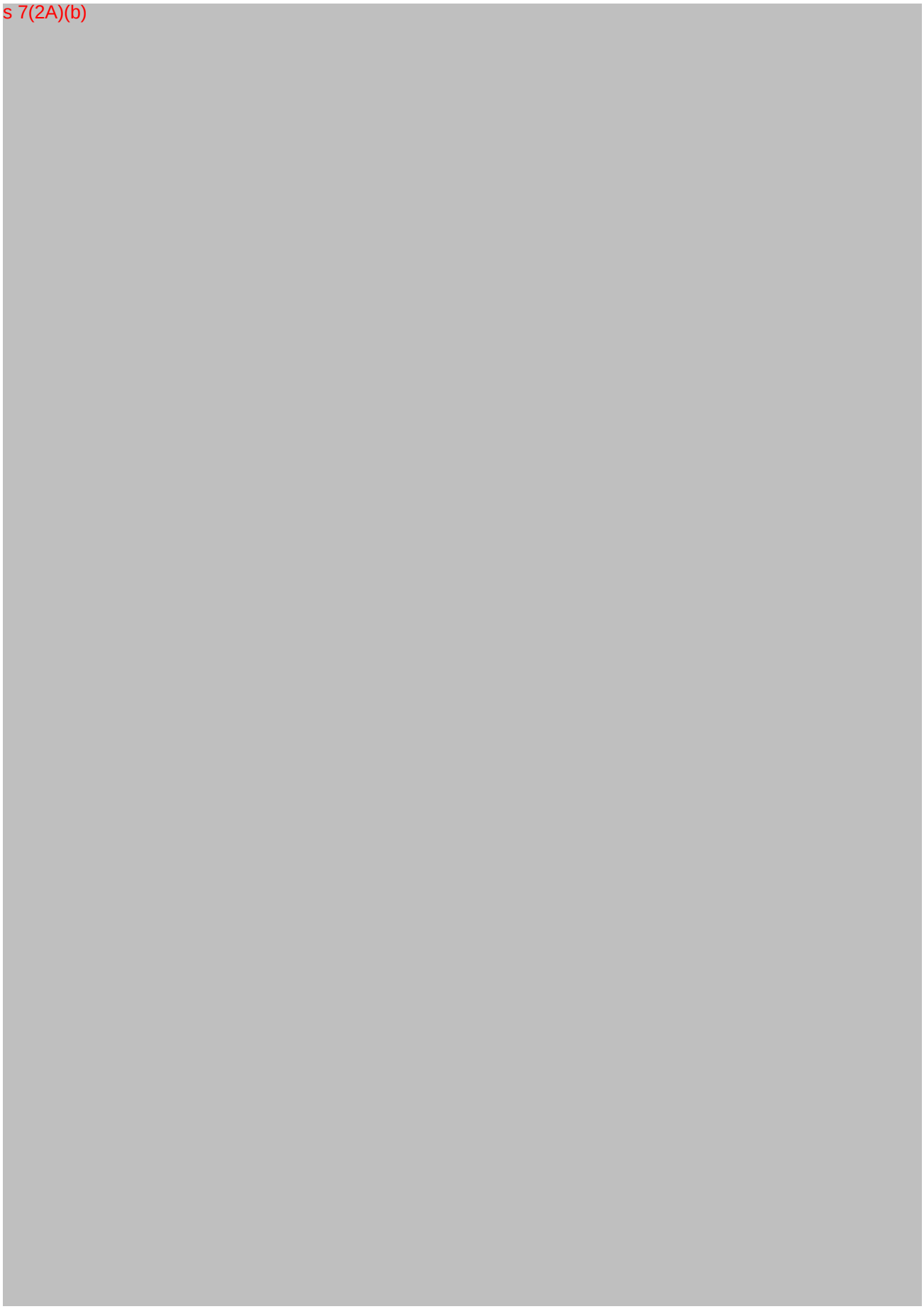
Out of Scope

s 33

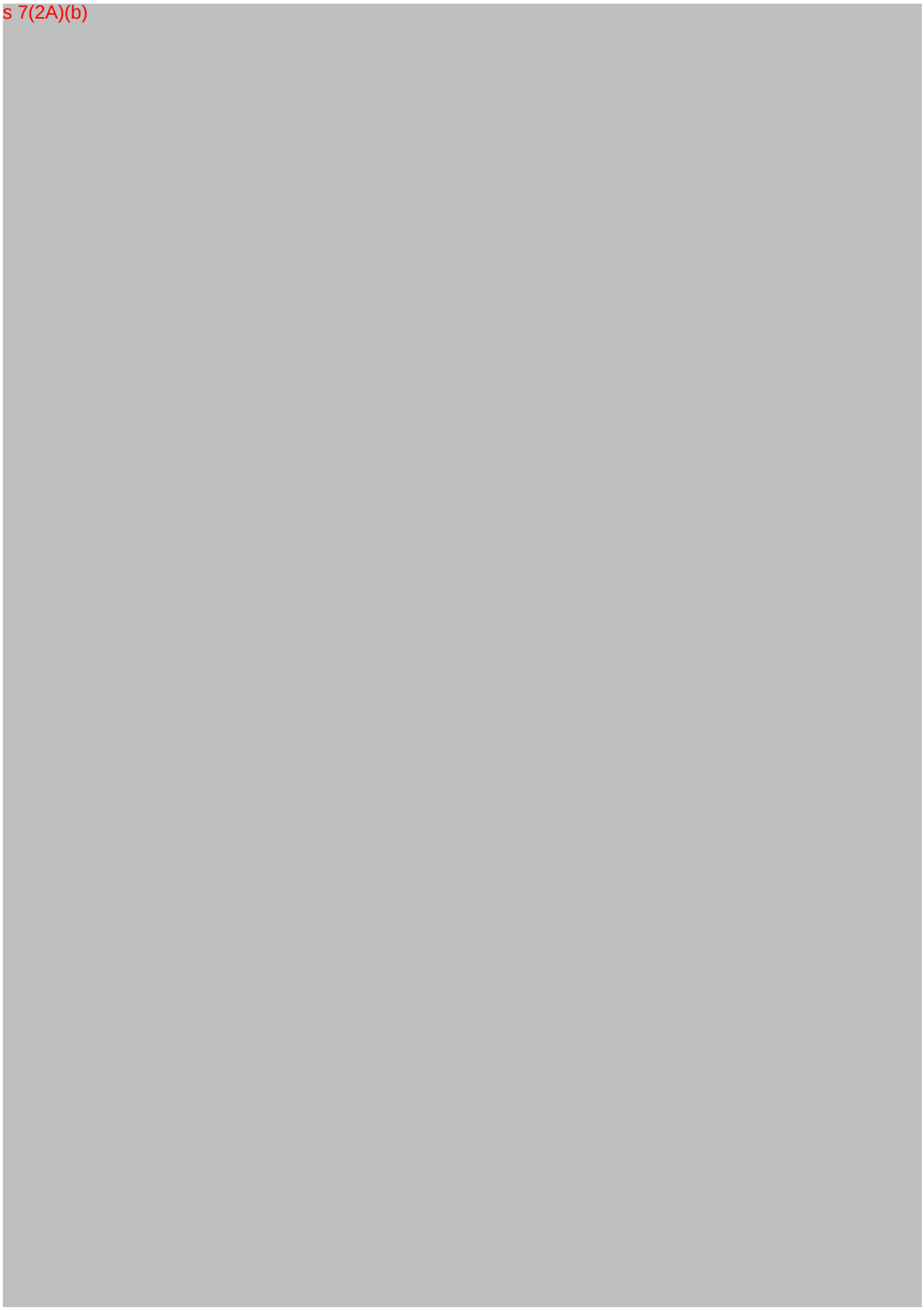
s 7(2A)(b)



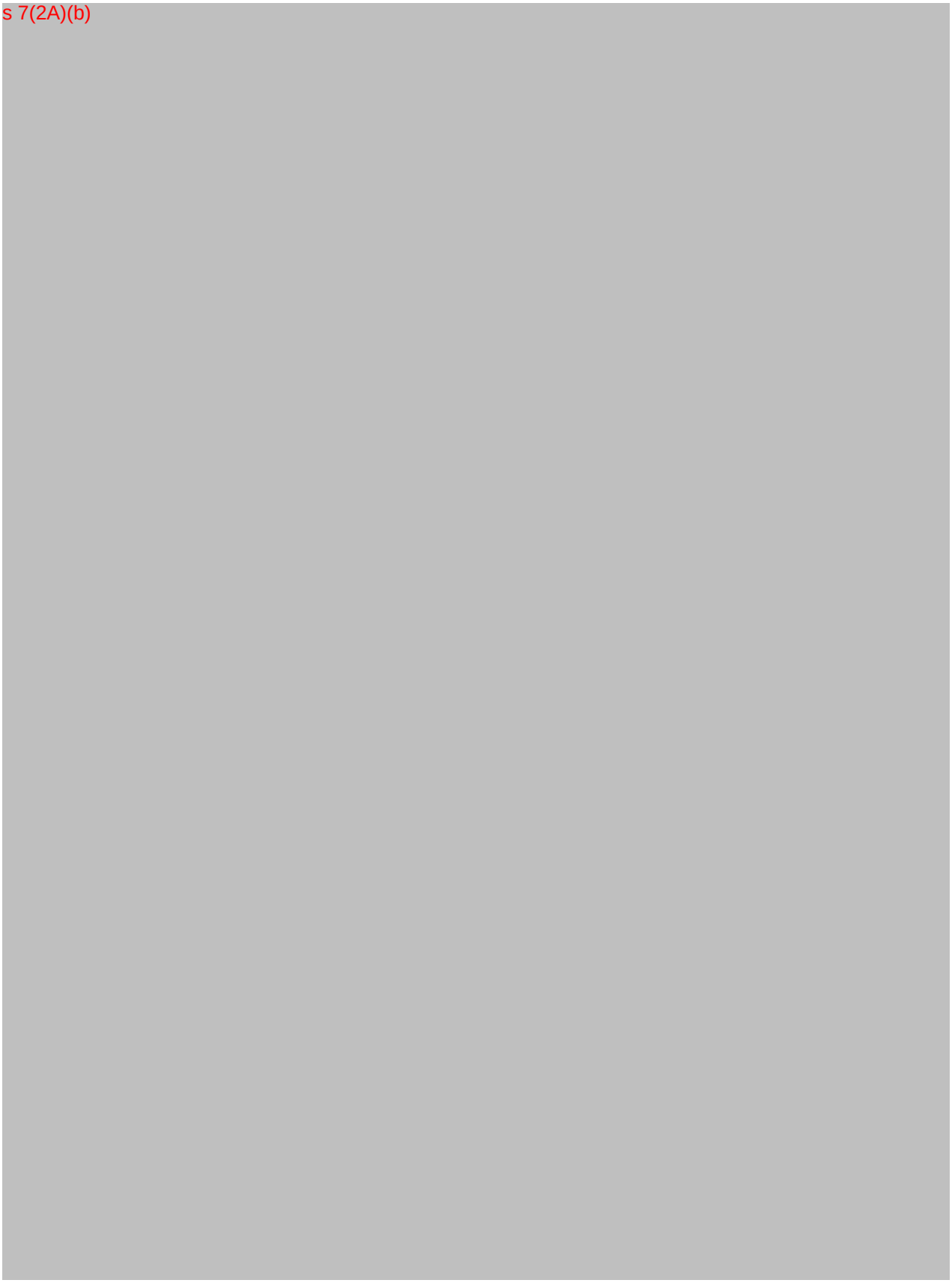
s 7(2A)(b)



s 7(2A)(b)

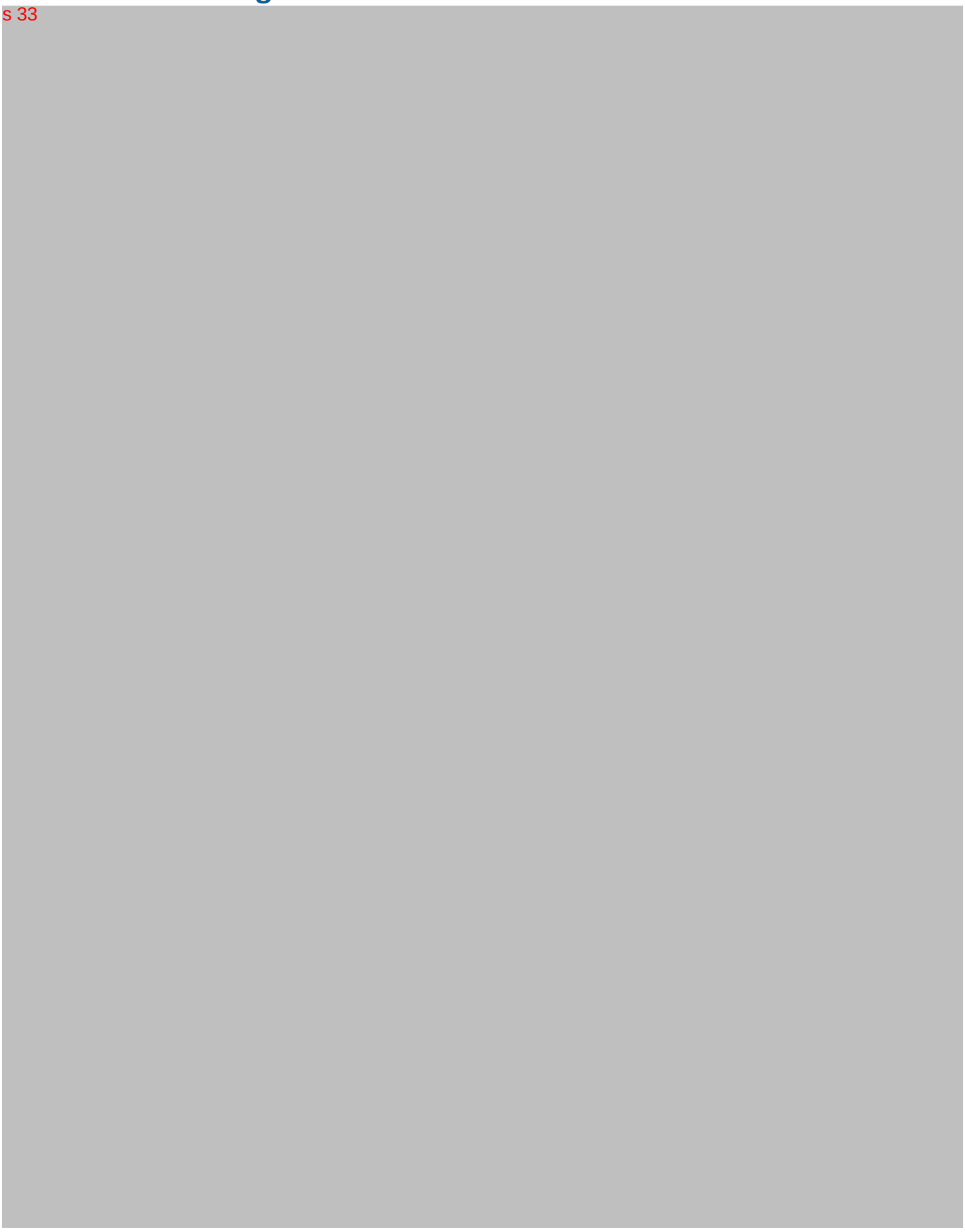


s 7(2A)(b)



Ionize Risk Register

s 33



s 33

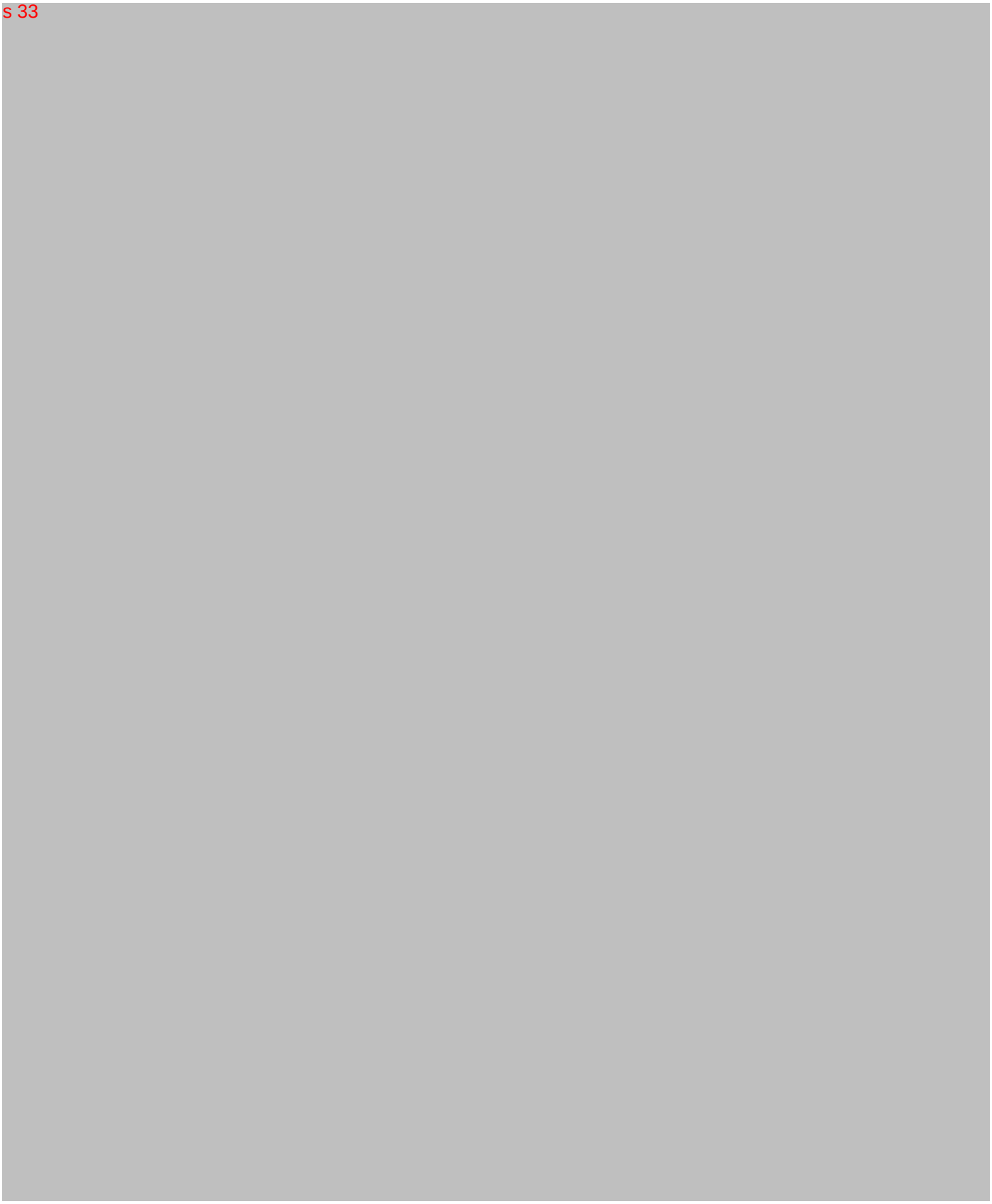
Severity Matrix

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Very Unlikely	Informational	Low	Low	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Possible	Low	Medium	Medium	High	High
Likely	Medium	Medium	High	High	Critical
Almost certain	Medium	Medium	High	Critical	Critical

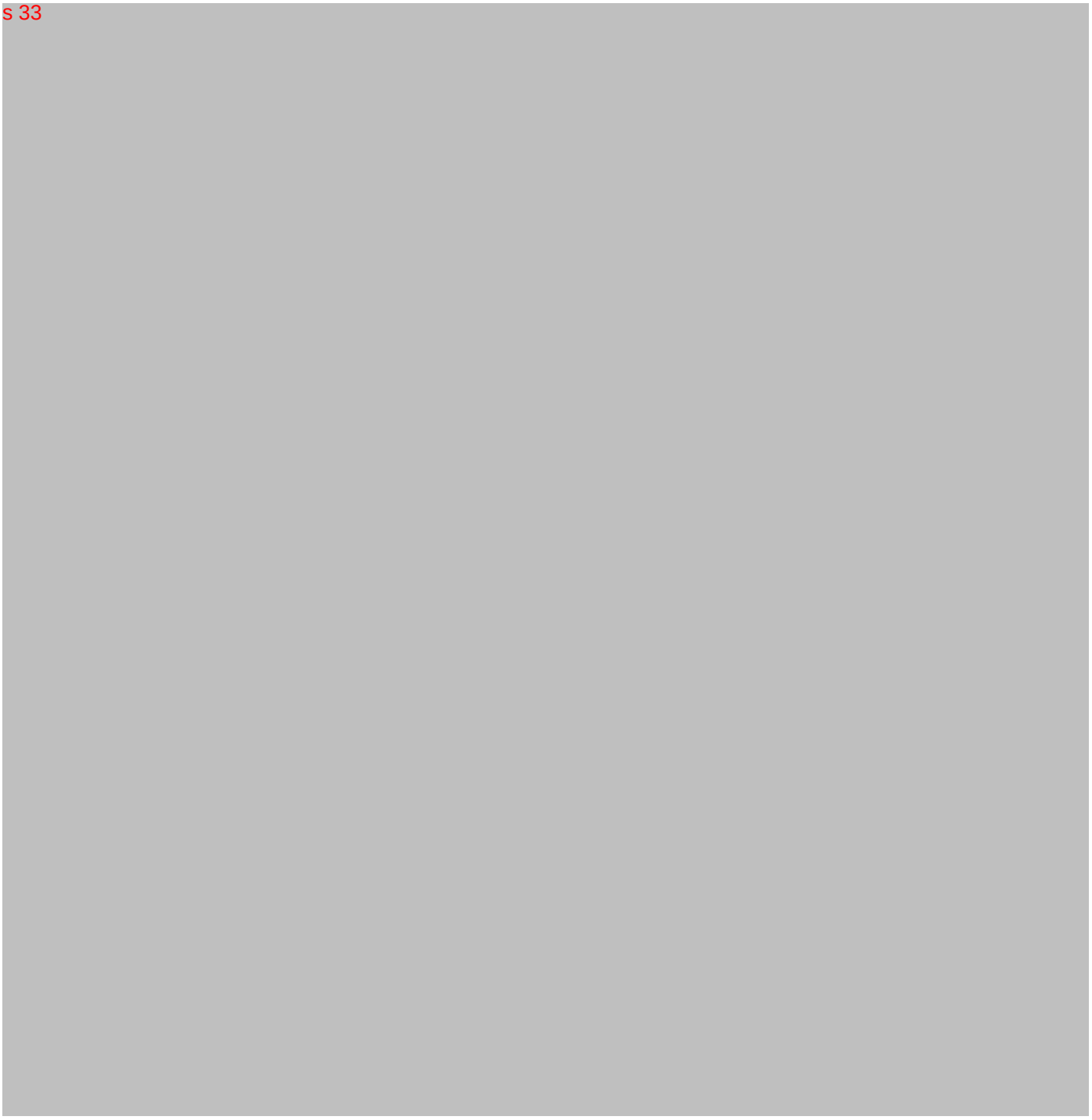
The severity of an issue is based on the *likelihood* of exploitation occurring (often determined by ease of exploitability, or the requisite preconditions), and the resultant *consequence* (i.e. the likely impact on the organisation).

Detailed Issue Summary

s 33



s 33



Mobile testing notes

Architecture, Design and Threat Modelling

The application interacts with the AWS API Gateway for registration and uploading of data. This data can then be viewed by health professionals via a health portal which interacts with a separate AWS API Gateway s 33

Data Storage and Privacy

s33 This is acceptable as these tempIDs are anonymised and change frequently.

On Android, all data for this application is stored within the `/data/data/<APP Name>/folder`. As such, no other applications on the device can view any data from this application.

s 7(2A)(b)

s33

Network Communication

All communication was conducted over HTTPS. This is a standard configuration for mobile applications s 33

Platform Interaction

API endpoints were tested against a variety of different web, database, and JSON based attacks. s33

Code Quality and Build Settings

s33 Should new code be added to the solution, the current

process of auditing code should be used. This will help to reduce the risk of unprofessional code being published to the public repository, and the subsequent reputational damage that could do.

Resiliency Against Reverse Engineering

No anti-reverse engineering or obfuscation were identified within the applications. This is likely due to public concerns about what the application is doing on the backend. As such, this application does not require any protections against reverse engineering.

Appendix A: Engagement and Report Context

Intended Audience

Audience	Objective
Digital Transformation Agency Project Manager	• Understand the areas focused on by the security testers to better understand which risks have been assessed. • Engage with the tester to resolve security issues and vulnerabilities discovered during testing. • Understand the business implications of security issues outlined within the document. • Understand the limits of testing, such as areas which were unable to be tested due to scope or time constraints
CovidSafe Development and Infrastructure Teams	• Understand the issues identified and their likely root cause • Understand possible mitigations to remediate the issues found • Understand the effectiveness of current security controls applied to network and web application assets. • To assess and implement suggested controls at the web host and infrastructure layers.

Schedule

The schedule below was the timeline of the engagement.

Date	Activity
24/04/2020	Commence Penetration Test
06/05/2020	Conclude Penetration Test
15/05/2020	Deliver Draft Report
22/05/2020	Deliver Final Report

From: s 22
To: s 22
Cc: s 22
Subject: RE: Formalised Report [SEC=OFFICIAL]
Date: Tuesday, 26 May 2020 9:48:19 AM
Attachments: image001.png
CovidSafe Mobile Application Penetration Test Report Final.pdf

---

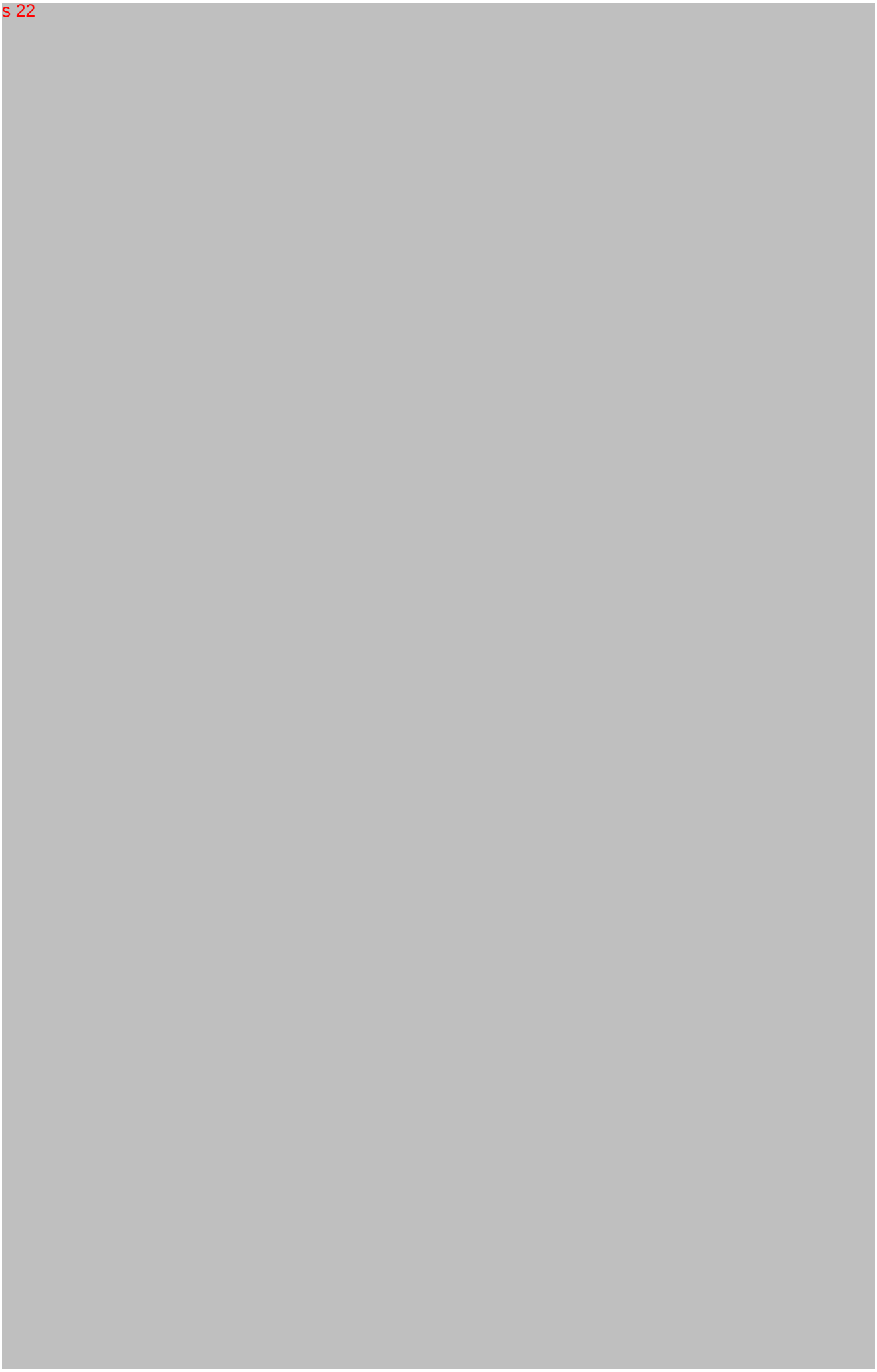
Hi s 22 ,

Thanks for spotting that.
Here is the finalised copy.

Regards,
s 22 .

---

s 22


s 22


s 22