Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Security Assessment of the COVID Alert Exposure Notification Service

PRACTITIONER

TLP:WHITE

Canada

FOREWORD

ITSP.10.003 Security Assessment of the COVID Alert Exposure Notification Service is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security.

For more information on this publication, contact the Canadian Centre for Cyber Security's Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613)-949-7048
1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on January 14, 2021.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	January 14, 2021

OVERVIEW

This document outlines the methodology and the activities that the Canadian Centre for Cyber Security (Cyber Centre) used to assess the security of the Government of Canada's (GC) COVID Alert Exposure Notification Service. The COVID Alert mobile application launched on July 31, 2020.

In June 2020, the Prime Minister of Canada announced the plans for Canada to launch a COVID-19 exposure notification service through Health Canada. This service will help Canada and the provinces and territories identify and isolate the spread of the COVID-19 virus quickly while ensuring the highest degree of privacy and security. The implementation of this service, in particular a mobile app and supporting infrastructure, was led by the Canadian Digital Service (CDS) and supported by the Cyber Security Division at Treasury Board of Canada Secretariat (TBS) and the Cyber Centre. To build in privacy and security, a rigorous security approach was adopted consisting of system security and privacy engineering, as well as security assessment activities. CDS and TBS were supported by external parties including Blackberry and the Cyber Centre to conduct independent security reviews and assessments. The Cyber Centre assessed the service to improve its availability, security, and integrity and assure the security and privacy of Canadians using the service.

As the project authority for the system, TBS was responsible for performing risk assessments, conducting functional testing, and prioritizing source code changes and bug fixes. CDS was also the primary developer of the service, which was initially derived from COVID Shield open source project created by volunteers working at Shopify, and was responsible for implementing code changes and source code fixes to mitigate discovered issues.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This publication outlines the approach and the activities that the Cyber Centre took to conduct an independent security architecture review and vulnerability assessment of the GC's COVID Alert Exposure Notification Service. The service is based on the framework developed by Google and Apple and the open source code base, COVID Shield.

The Cyber Centre created a multidisciplinary team of vulnerability researchers and IT security engineers to assess the security of the service. The Cyber Centre assessed the service to improve its availability, security, and integrity and assure the security and privacy of Canadians using the service. During the assessment, the Cyber Centre identified and reported vulnerabilities to TBS and provided guidance and recommendations for improving the overall security of the service.

The team used IT security best practices, coding best practices, and guidance published by the Cyber Centre, such as *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [1][1] and *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [2], and the Open Web Application Security Project's (OWASP) *Mobile Security Testing Guide* [3].

Section 2 outlines the security architecture analysis in which the Cyber Centre worked with TBS to assure the service met its security and privacy requirements.

Section 3 focuses on the vulnerability assessment, outlining the Cyber Centre team's approach and high-level activities.

[1] Numbers in square brackets refer to references cited in the Supporting Content section of this document.

2 SECURITY ARCHITECTURE ANALYSIS

To ensure the security of the COVID Alert Exposure Notification Service, the Cyber Centre team worked with CDS developers and Health Canada's operational authority. The Cyber Centre's team assessed the security of the following components of the service:

- The backend architecture of two servers set up in the Amazon Web Service (AWS) cloud;
- The key submission server and the key retrieval server;
- Both the Android and the iOS mobile applications; and
- The COVID Alert Portal.

The COVID Alert Exposure Notification Service uses provincial portals to obtain diagnosis keys. However, the team did not include these portals in the assessment.

Note that Blackberry assessed the security of the service's framework and system, and AWS used their Well-Architected Framework, which describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. These assessments have been incorporated into the overall system analysis.

2.1 ASSESSMENT APPROACH

The goal of the Cyber Centre's assessment was to ensure that the COVID Alert Exposure Notification Service had the appropriate security controls in place to achieve an acceptable level of risk.

The Cyber Centre team examined TBS's security assessment and authorization (SA&A) process for the COVID Alert Exposure Notification Service. The SA&A process, which is identified in ITSG-33 [2], includes identifying the scope of the architecture to be assessed, the vulnerabilities and identified threat levels, and the associated levels of risk. The Cyber Centre worked with TBS to achieve the following outcomes:

- Discuss and assist with assigning risk to the identified categories;
- Ensure the risk register was complete and accurate;
- Examine and characterize certain identified vulnerabilities; and
- Review the overall architecture.

The Cyber Centre team also analyzed threat scenarios and reviewed the overall system architecture to ensure the appropriate security controls were implemented.

2.2 ANALYSIS FINDINGS

While analyzing the security architecture, the Cyber Centre found that TBS conducted its own security assessment according to the SA&A process defined in ITSG-33 [2]. This security assessment process was thorough and exhaustive, demonstrating a mastery-level understanding of the ITSG-33 framework and its processes. Given the short timeline and the framework, there were risks identified with the service. However, TBS integrated mitigations into the system architecture, which adjusted the risks to a level that achieves an acceptable level. TBS worked with the Cyber Centre to ensure all vulnerabilities were identified and mitigated according to the acceptable levels of risk. The Cyber Centre team provided decision makers with all the information available on the residual risk (i.e. the level of risk remaining after security controls are implemented) at the time of system authorization.

3 VULNERABILITY ASSESSMENT

The Cyber Centre team also conducted a vulnerability assessment of the COVID Alert Exposure Notification Service to identify existing gaps in the service's security protections and improve its overall security. As a result of the assessment, vulnerabilities were identified and reported to TBS. The team also provided TBS with additional recommendations on IT security best practices, coding best practices, system parameter changes, and validated cryptographic libraries.

The team assessed the following aspects of the service:

- Mobile application, key server components, and related data;
- COVID Alert Portal (limited evaluation);
- Google-Apple Exposure Notification Application programming interface (EN API) frameworks [4] [5] (limited evaluation);
- Cryptographic algorithms and protocols; and
- Device-to-server and device-to-device communications.

The service uses provincial and proprietary components. However, these components were not assessed by the Cyber Centre.

Note that Blackberry performed its own security review of the service.

3.1 ASSESSMENT APPROACH

The assessment tasks were broken down based on security requirements and technology. The researchers adhered to privacy considerations throughout all their assessment activities. The assessment included techniques such as static code analysis, dynamic analysis, fuzz testing, penetration testing, forensic artifact investigation, traffic pattern evaluation, and endpoint authentication verification. These techniques are defined as follows:

- **Static analysis – security code auditing**: Researchers reviewed the application's source code and the source code of the main dependencies to identify potential security issues, such as uninitialized variables, memory management issues, or logic errors.
- **Static analysis – reverse engineering**: Researchers investigated machine code artifacts for which source code was not available to identify potential security issues.
- **Dynamic analysis**: Researchers observed and interacted with application components to identify logic errors, memory leaks, and potential race conditions.
- **Fuzz testing**: A specific application of dynamic analysis. Researchers examined how the application reacted to abnormal inputs to validate that the application was hardened against unexpected interactions.
- **Penetration testing**: The practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker can exploit. Penetration testing can include all the techniques listed above.
- **Forensic artifact investigation**: An investigation focused on a detailed examination of volatile and persistent memory (such as file systems) in the system being tested.

- **Traffic pattern evaluation:** Detailed examination of the network interactions between devices and between a device and the server.
- **Endpoint authentication verification:** Study of the protocols used by the application to authenticate legitimate users with the server and validate data sent by the server to the users.

3.2 ASSESSMENT ACTIVITIES

To assess the service, the team broke down the mobile application and the key server into their major functional components. Each component was assessed individually and as part of the overall functioning solution. See Figure 1 for a visual breakdown of how the application, key server, and web portal were assessed.

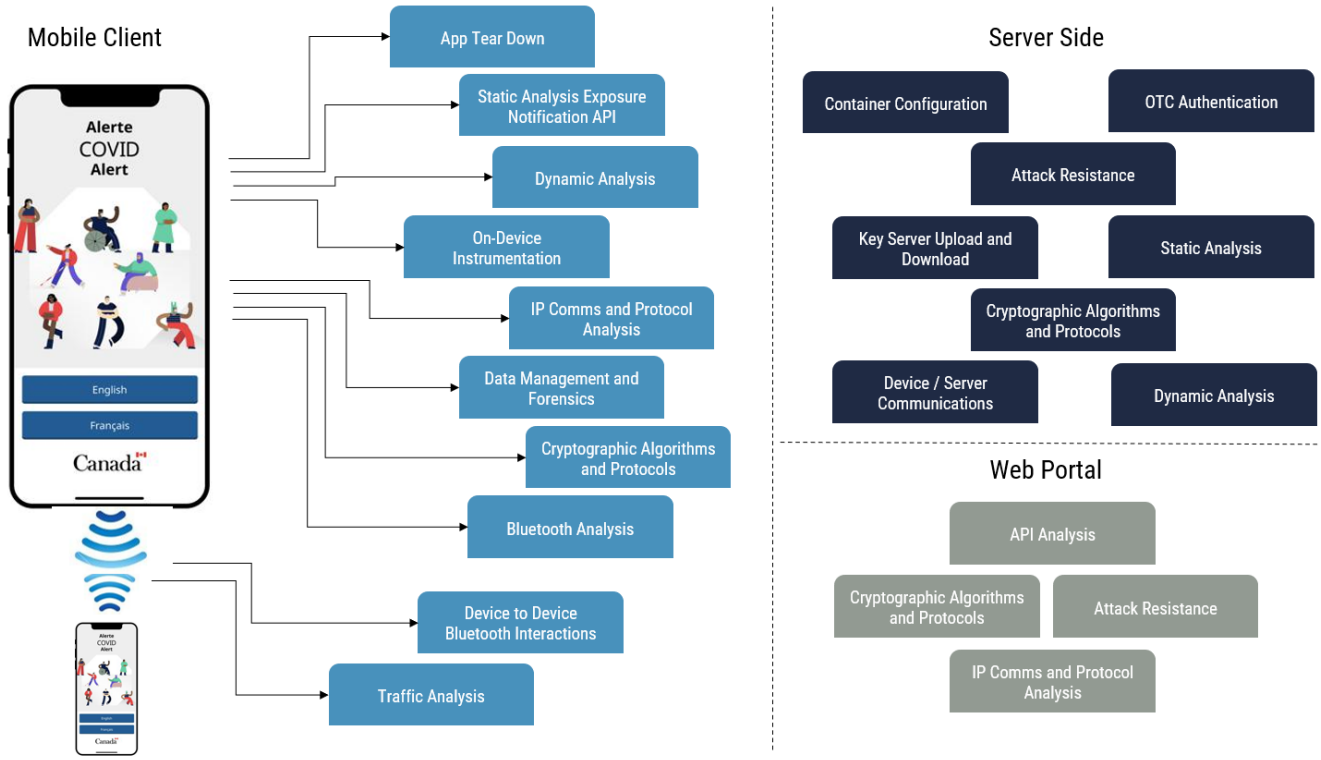

Figure 1: Breakdown of Vulnerability Assessment Testing

The Google-Apple EN API implementations [4] [5] were assessed on their respective platforms.

The team analyzed the cryptographic implementations used by the service to determine their security and cryptographic strength. The mobile client to key server communications and the mobile client to mobile client Bluetooth communications [6] and traffic were analyzed in the Communications Security Establishment's (CSE) labs.

The team also reassessed and verified the security fixes and code changes made by TBS.

3.2.1 MOBILE APPLICATION

Various Android and iOS mobile applications components were analyzed using a combination of static and dynamic analysis. These components included the application's source code, data management and on-device instrumentation, and network communications protocols.

STATIC ANALYSIS OF SOURCE CODE

Static analysis was performed on the available mobile application source code, libraries, and related configuration files. The codebase is comprised of several languages, including TypeScript, JavaScript, Java, Kotlin, Objective-C, and Ruby, as well as pre-compiled Shared Libraries. The team's analysis focused on ensuring that the mobile application satisfied privacy and security requirements and followed best practices for coding and application development.

DATA MANAGEMENT AND ON-DEVICE INSTRUMENTATION

The team analyzed the way in which the application manages data. A combination of the following activities was used:

- Investigate where application data is stored and how it is used by the application during runtime;
- Investigate forensic artifacts during application's lifetime and after its deletion;
- Perform static analysis;
- Conduct functional testing; and
- Analyze logs.

To ensure the application met the privacy and the security requirements, analysis included the following actions:

- Verify the generation and protection of Rolling Proximity Identifiers (RPI)s and Temporary Exposure Keys (TEKs);
- Determine if the app attempts to access or store data it is given access to (e.g. other app info, location data);
- Verify the security settings against best practice guidelines;
- Verify that data is generated at the right frequency; and
- Identify configuration differences between iOS and Android versions that could lead to potential security issues.

INTERNET PROTOCOL COMMUNICATIONS

The team analyzed the network communications protocols that the service uses and conducted penetration testing using a client-server test framework to generate test network traffic. The main goals were as follows:

- Verify client anonymity in communication patterns;
- Verify endpoint authentication of TLS certificates; and
- Determine what data is exchanged between the app and the server and whether the underlying traffic is susceptible to attacks.

3.2.2 KEY SERVER

Static analysis was performed on the upload and download key server. While all types of vulnerabilities were considered, the team focused on problematic issues such as race conditions and logic errors at the source code level.

Server-database interactions and some of the external Go libraries used by the server were analyzed with the following considerations in mind:

- How health care providers generate a one-time code and the key upload handling of the server;
- How the server handles key uploads; and

- How and what external Go libraries are used by the application.

The team further investigated the environment in which the server runs and the docker environment. Fuzz testing of the server endpoints was also conducted to identify flaws not seen during static analysis. This was done by submitting arbitrary data to the server end points.

3.2.3 COVID ALERT PORTAL

Static analysis was performed on the COVID Alert Portal, which is comprised of a Django and Python code base. As with the key upload and download server, the team considered all types of vulnerabilities, but focused specifically on logic and race conditions.

3.2.4 GOOGLE-APPLE EN API

The Google-Apple EN API frameworks [4] [5] were analyzed. At the onset of the investigations, the source code for these components was not available. As such, the team performed binary analysis to look for basic flaws.

Both Apple and Google later released source code related to some of these functions, which assisted the investigation.

3.2.5 CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

Several areas of the service use cryptographic algorithms and protocols. The team assessed these areas to ensure that the algorithms and protocols selected for the communication channel between the app and the server adhere to the Cyber Centre's published guidance, such as ITSP.40.111 [1] and *ITSP.40.062 Guidance on Securely Configuring Network Protocols* [7].

Using the tests from the National Institute of Standards and Technology's (NIST) *SP800-90B Recommendation for the Entropy Sources Used for Random Bit Generation* [8], the team also assessed the source of entropy that is used to generate one-time codes for a positive diagnosis.

3.2.6 BLUETOOTH/BLUETOOTH LOW ENERGY (BLE) COMMUNICATIONS

Bluetooth/BLE communications [6] were analyzed using test devices in an isolated environment in a CSE lab. This was done through traffic capture and packet analysis to verify that the Bluetooth behaviour satisfied privacy and security requirements. The team took specific notice of the RPI lifespan and the synchronization of RPI and Bluetooth device address rollovers.

4 DOCUMENTATION AND REPORTING PROCESS

Tasks, findings, and proposed mitigations were documented using a common issue management solution. This information was communicated back to TBS in real time using dashboards and formal status updates. If TBS decided to implement a suggested mitigation based on their own risk assessment and prioritization, they communicated this decision and the status of applicable code changes by providing direct feedback.

Researchers used regular technical reviews and chat channels to exchange information.

Figure 2 outlines the high-level analysis and reporting flow of the assessment.

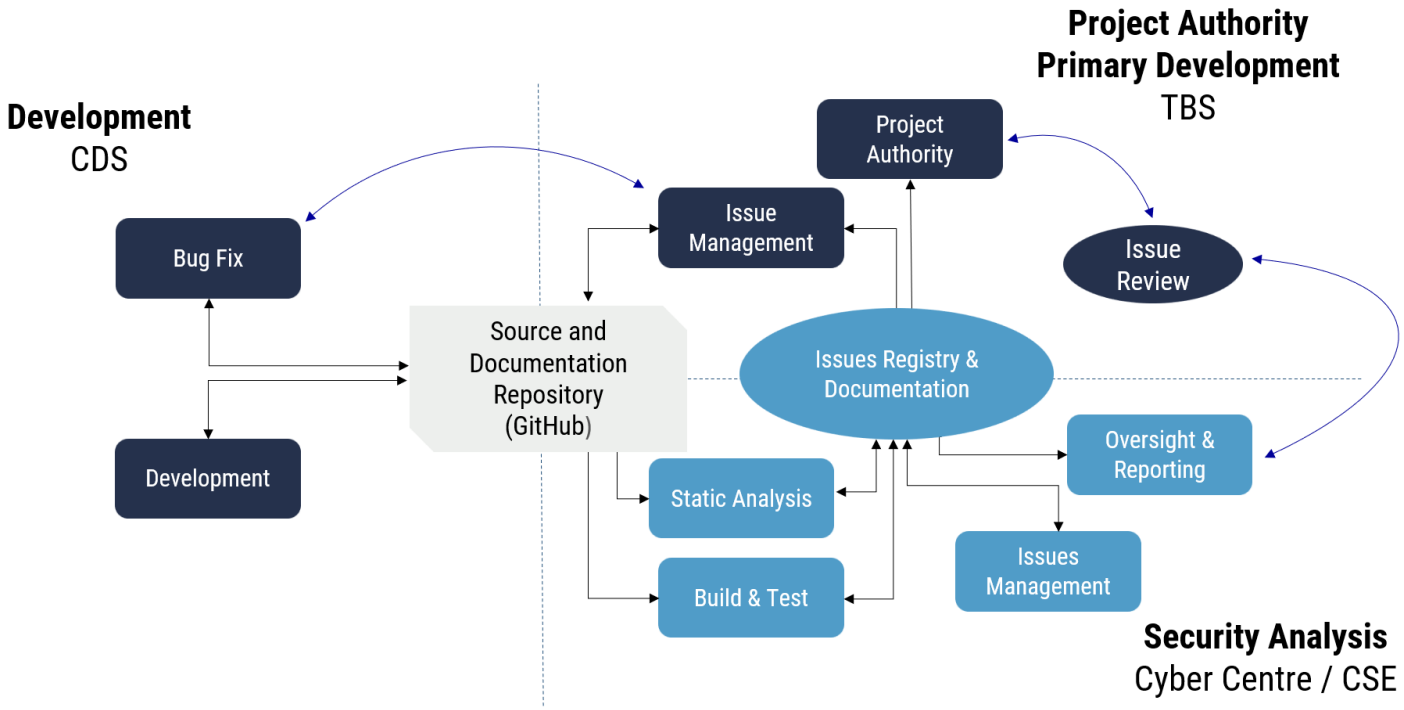

Figure 2: High-Level Analysis and Reporting Flow

4.1 ISSUE MANAGEMENT PROCESS

Vulnerabilities and suggested IT security changes were categorized as follows:

- **Vulnerability / Privacy Consideration**: An actual vulnerability in the service and/or an impact on the application's privacy requirements; and
- **Suggestion**: Code review style comment; suggestion for how the code should work or be implemented instead.

Vulnerabilities were further categorized as high, medium, or low priority, depending on their potential severity. TBS reviewed each submitted issue and performed a risk analysis to determine the overall severity and impact to the service.

Occasionally, the Cyber Centre suggested mitigation options for CDS developers to review and consider. The developers made and tracked updates and source code fixes in the open source CDS GitHub repository [9]. Once a code change was reviewed and flagged by TBS for reassessment, the Cyber Centre researcher who originally assessed and reported the issue verified that the mitigation was correctly implemented. The vulnerability researchers also verified that the mitigation resolved the underlying issue without introducing new vulnerabilities. After reassessing and verifying the change, the researcher marked the ticket as complete.

5 SUMMARY

To support TBS's effort with the COVID Alert Exposure Notification Service, the Cyber Centre created a multidisciplinary team of vulnerability researchers and IT security engineers. The team assessed the overall security of the service, conducting vulnerability assessments and analyzing the service's security architecture.

During the security architecture assessment, the Cyber Centre found that TBS conducted its security assessment according to the SA&A process defined in ITSG-33 [2]. TBS security assessment process was thorough and exhaustive, demonstrating a mastery-level understanding of the ITSG-33 [2] framework and its processes. TBS worked with Cyber Centre to ensure all vulnerabilities were identified and mitigated according to the acceptable levels of risk.

As a result of the Cyber Centre's assessment, a number vulnerabilities were identified and reported to TBS. The team also provided TBS with additional recommendations on IT security best practices, coding best practices, system parameter changes, and validated cryptographic libraries.

There is a very high degree of confidence that the process and results yielded a secure system. The residual risk was identified and characterized for decision makers at the time of system authorization. TBS is continuing its work to find and mitigate risk during system operation.

5.1 CONTACT INFORMATION

For more information, contact the Cyber Centre's Contact Centre by email or phone:

Contact Centre
contact@cyber.gc.ca
(613)-949-7048
1-833-CYBER-88

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
AWS	Amazon Web Services
BLE	Bluetooth Low Energy
CDS	Canadian Digital Service
CSE	Communications Security Establishment
EN API	Exposure Notification Application Programming Interface
GC	Government of Canada
IT	Information Technology
NIST	National Institute of Standards and Technology
RPI	Rolling Proximity Identifiers
TBS	Treasury Board of Canada Secretariat
TEK	Temporary Exposure Keys
TLS	Transport Layer Security

6.2 GLOSSARY

Term	Definition
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Compromise	The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity, or availability.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Protected B	A federal government security designation that applies to information or assets that, if compromised, could cause serious injury to an individual, organization, or government.
Residual risk	The likelihood and impact of a threat that remains after security controls are implemented.
Risk	The likelihood and impact of a threat exploiting a vulnerability to access an asset. Usually expressed in level (e.g. high, medium, low).
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of IT assets. Security controls can be applied by using a variety of security solutions that can include security products, security policies, security practices, and security procedures.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.
Vulnerability assessment	A process to determine existing weaknesses or gaps in an information system's protection efforts.

6.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information*. August 2016.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
3	Open Web Application Security Project Foundation. *OWASP Mobile Security Testing Guide*. N.D.
4	Apple. *Exposure Notification API Framework.* N.D.
5	Google Inc. *Google Exposure Notification API*.
6	Bluetooth SIG Inc. Bluetooth Specifications.
7	Canadian Centre for Cyber Security. *ITSP.40.062 Guidance on Securely Configuring Network Protocols*. Version 2. October 2020.
8	National Institute for Standards and Technology. *SP800-90B Recommendation for the Entropy Sources Used for Random Bit Generation*. January 2018.
9	Canadian Digital Service and GitHub. Canadian Digital Service GitHub Repository. N.D.
10	Electronic Frontier Foundation (EFF). *Apple and Google's COVID-19 Exposure Notification API: Questions and Answers*. April 2020.
11	National Institute of Standards and Technology. Cryptographic Algorithm Validation Program.
12	National Institute of Standards and Technology. Cryptographic Module Validation Program.
13	Ministry of Health, the Minister of Technology Innovation (Italy), and GitHub. *Immuni's Traffic Analysis Mitigation*. N.D.
14	National Cyber Security Centre (UK). *NHS Test and Trace App Security Redux*. August 2020.
15	National Institute of Standards and Technology. *SP 800-115 Technical Guide to Information Security Testing and Assessment*. September 2008.
16	Office of the Privacy Commissioner of Canada. "The Privacy Act".