Road Safety Camera Commissioner

REPORT TO THE MINISTER FOR POLICE ON THE MALWARE INFECTION TO THE FIXED DIGITAL ROAD SAFETY CAMERA SYSTEM

3 May 2018

The Road Safety Camera Commissioner respectfully acknowledges the Traditional Owners of the land of Victoria and pays respect to their culture and their Elders past, present and future.

TABLE OF CONTENTS

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

EXECUTIVE SUMMARY

1 On the morning of 22 June 2017, journalist and broadcaster Mr Neil Mitchell telephoned the Minister for Police, the Honourable Lisa Neville, to ask her about some information that he had received. Mr Mitchell told the Minister, in effect, that 55 road safety cameras had been struck by a virus. In response to this information, the Minister made enquiries of Department of Justice and Regulation and was, for the first time, informed that a virus had infected the Road Safety Camera System computer network.

2 On 22 June 2017, I was requested by the Minister for Police to investigate and report on, *inter alia,* the causes, effects, consequences and lessons from a malware infection found in the Victorian Fixed Digital Road Safety Camera System. On 6 July 2017, I delivered an interim report, with preliminary findings as a consequence of my investigation to that date. This is the final report and is supported by the very substantial advice of consultants engaged to assist my investigation:

3 In summary, in my interim report I made the following findings:

- There was no evidence that the infection had affected the integrity of Speed and Red-Light camera infringements.
- I was satisfied that the mechanisms that construct and communicate the infringement data were unaffected by the virus.
- I was satisfied that there was no evidence of any infringement data being in any way compromised.
- I was satisfied that devices which measure and record speed are external to the infected computers and were unaffected by the virus.
- I was satisfied with the accuracy and integrity of the infringements issued 6 June 2017 to 22 June 2017 (and thereafter).
- I was satisfied that there was no evidence of any ongoing effect on the systems.

4 I wish to acknowledge that in reaching the conclusions that I have and as I set out in this report, I have been well assisted by the expert opinions of:

- Mr Stuart McCormack, ByteSmart Pty Ltd;
- Mr Cameron Crofts and Mr Paul Wilson, Blue Connections Pty Ltd; and
- KPMG, in particular the team led by Mr Jeeva Maistry.

Summary of my key findings

5 The Victorian Fixed Digital Road Safety Camera System is part of the State's Towards Zero road safety program. The public rightly expects accuracy and integrity in the system. Any possible compromise of that accuracy or integrity are newsworthy topics. In May 2017 the WannaCry virus had become notorious by reportedly infecting more than 230,000 computers in over 150 countries. It had reportedly disrupted organisations including the British National Health Service, Russian Interior Ministry, Deutsche Bahn railways, and well known manufacturers and service organisations. There was also substantial public interest in whether the ransomware had compromised the Road Safety Camera System (interchangeably referred to in this report as "the **Program**").

6 My investigation involved meeting with and speaking to dozens of people involved in the management and maintenance of the system, of tracing through written records of the events, and looking, with 20/20 hindsight, at potential improvements.

7 I am satisfied that the cameras which were infected have been identified. They came to be infected because the security to the computer network was breached, due to insufficient security measures and an inadequate adherence to set practices.

8 I am satisfied that there have not been any inappropriate infringements issued across the Victorian Road Safety Camera System as a result of the virus.

9 I am satisfied that there has not been any damage caused to data held by any of the Victorian Road Safety Cameras as a result of the virus.

10 I am satisfied that the impact on the Victorian Road Safety Camera System has been limited to periods of downtime on a significant number of cameras (and their computers), but otherwise has not resulted in any damage.

11 Whilst the infection's direct impact was limited to computer downtime, this will have flowed on to affect enforcement of Victoria's road safety laws, and so impeded progress of the Towards Zero objective.

12 I am satisfied that there has not been any impact on the accuracy of the Victorian Road Safety Camera System.

13 The integrity of the system has come under scrutiny, and I make recommendations for improvement.

14 The experts I engaged found that some of the systems were infected with malware due to vulnerable operating systems that did not have critical anti-viral "patches". The viral infection and subsequent spread was assisted by poor Network topology, and security design.

15 The infection was probably as a result of bad luck and probably inevitable; but the spread through the Road Safety Camera System occurred because of inadequate design of the system, system security measures and governance.

RECOMMENDATIONS

16 That the Department of Justice and Regulation in conjunction with other key stakeholders:

- Implement a strategic governance framework, in particular defining the future strategy of the Program, and thereafter implement a governance framework to support the strategy;
- Subsequently review the Program's operations model to ensure that it is being delivered in the most economic efficient and effective way.

These and related activities will need to be underpinned by a strong change management program.

17 That the Department of Justice and Regulation in conjunction with other key stakeholders work to develop a strong Program-wide, positive, open, collaborative, transparent and values-based culture. Improvements should include:

- Open and transparent culture;
- Values and behaviours;
- Continuous improvement.

18 There is a need for enhanced risk management capability. This should occur through:

- Enhancing risk management Program wide;
- Formalising risk management and reporting, especially in DJR.

19 That there be greater scrutiny over the reporting and escalation of issues, incidents and performance of the Program. This should include:

- Incident identification escalation;
- Use of data and information, and monitoring and evaluation of overall Program performance;
- Enhancing the role of the Office of the Road Safety Camera Commissioner;
- Enhancing the scrutiny regarding reporting on the performance of the Program.

20 That there be greater streamlining of processes to reduce data integrity risk, and inefficiency of manual process on already constrained resources:

- Move to greater automating and streamlining;
- Improve capital and procurement processes.

21 Network practices be enhanced:

- Need for improved physical security;
- Need to ensure that the network operator is continuously improving;
- Determine if IMES should continue to be the network operator.

22 That there be segmentation of the Fixed Digital Road Safety Camera (FDRSC) network from all third parties and contractors.

23 That FDRSC dedicated centralised firewalls be put in place to protect the network. All traffic to the FDRSC network will be controlled by firewall policies where full packet inspection and threat prevention profiles will be configured.

24 That a specialist organisation oversee the reconfiguration of the FDRSC network and then periodically review its operation.

25 That there be regular security auditing of the FDRSC contractors.

26 That in the event of a future infection, for every infected system:

- copies of the Windows Event logs are retained. (System, Application and Security logs) and
- for each class of infected hardware, a hard drive should be removed and "bagged"; that is, removed from use and maintained in an unmodified state.

27 That there be improvements to SiteTrak:

- That SiteTrak be modified to ensure that records clearly categorise the reasons for site deactivations;
- That SiteTrak be modified to ensure it maintains a transparent accurate historical record.

28 [redacted]

29 That there be improved emphasis in IMES on Good Management Practice, including the need for continuous improvement, and a plan of action

30 That the powers of investigation of Road Safety Camera Commissioner (RSCC) need clarification. I recommend that the powers should include power to compel prompt thorough co-operation from within the Victorian public sector. Any behaviour inconsistent with the Victorian Public Service Code of Conduct should result in relevant consequences.

ACKNOWLEDGEMENTS

31 My report has been achieved thanks to many people and organisations who have generously shared their knowledge, expertise, ideas for innovation, and time. These include:

- Mr Stuart McCormack of ByteSmart Pty Ltd
- Blue Connections Pty Ltd
- KPMG
- Bureau Veritas Asset Integrity and Reliability Services Pty Ltd
- CEOS Industrial Pty Ltd
- Department of Justice and Regulation
- Enex Pty Ltd
- GATSO Australia Pty Ltd (now Sensys Gatso Australia Pty Ltd)
- JENOPTIK Australia Pty Ltd
- Redflex Traffic Systems Pty Ltd
- SERCO Traffic Camera Services (Vic) Pty Ltd
- SGS Australia Pty Ltd
- Telstra
- Transurban
- VicRoads
- Victoria Police
- Vipac Engineers & Scientists Ltd

Thanks also to members of the Road Safety Camera Commissioner's Reference Group for their helpful insights:

- Professor Brian Fildes
- Ms Pauline Kostiuk
- Prof Carolyn Unsworth
- Ms Tia Orton

I am particularly grateful to staff of the Office of the Road Safety Camera Commissioner, for their insightful and enthusiastic input, without which this report could not have been as comprehensive or as analytical.

ACRONYMS & DEFINITIONS

Camera	In the context of a road safety camera system, this term is used to include the relevant camera system and associated computer.
Camerassavelives	Website administered by IMES, https://www.camerassavelives.vic.gov.au/
CCU	Camera Control Unit
CCV	Civic Compliance Victoria
DJR	Department of Justice and Regulation
FDRSC	Fixed Digital Road Safety Camera
FDRSCN	Fixed Digital Road Safety Camera Network
ICT	Information and Communication Technology
IMES	Infringement Management and Enforcement Services A unit of DJR which at the time was primarily responsible for the management of, and accountability for, the end to end infringement system, including the promotion of the objectives of the *Infringements Act 2006* through community information and education. As at 1 January 2018, IMES managed the infringements system in Victoria whilst Fines Victoria managed enforcement and processes infringement notices, warrants and payments.
Infringement	In the context of this report an infringement is a "traffic infringement" as defined in the Road Safety Act 1986 and regulations made thereunder and that relates to driving in excess of the speed limit or failing to obey traffic signals.
IP Address	Each device that is connected to a computer network is assigned an Internet Protocol address (IP address). It is a numerical identification label.
OoB Server	(Out-of-band) A server situated outside a primary network that provides secure access and control of IT assets on the primary network.
Patch	Software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the computer's usability or performance.
Program	Road Safety Camera Program
Ransomware	A type of malicious software that contains a threat to publish the victim's data or perpetually block access to it unless a ransom is paid. Often it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. Typically, digital currencies such as Bitcoin are used for the ransoms, making it difficult to trace the perpetrators. Ransomware attacks are also typically carried out using a "Trojan" that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment.
SiteTrak	A database used by IMES to record "Work Authorisations" and work done on FDRSC systems.
SmartDip	A system deployed on FDRSCs to report data such as primary and secondary detected speeds, image location detail and, where possible, the number plate of the detected vehicle.
Subnet	A subnetwork or subnet is a discrete part of a network. Typically, a subnet might consist of all of the machines at one geographic location, or in one building, or on the same local area.
Towards Zero	Victoria's Road Safety & Action Plan. See: https://www.towardszero.vic.gov.au/
VicPol	Victoria Police
Work Authorisations	The formal documentation required by IMES as a record of work to be undertaken

PURPOSE

32 On 22 and 24 June 2017, the Minister for Police, the Honourable Lisa Neville, requested that I investigate issues associated with the WannaCry Ransomware virus infection that struck computers associated with Victoria's Road Safety Camera System (see **Annexure A**). The Minister wishes to ensure that the public can be confident in the Road Safety Camera System, and she asked for my investigations to cover:

- which cameras across the Victorian Road Safety Camera System were infected with a virus, and how the cameras came to be infected;
- whether there have been any infringements issued across the Victorian Road Safety Camera Network from 6 June 2017 that could be inaccurate as a result of the virus and that should be withdrawn;
- whether any damage may have been caused to the data held by any of the Victorian Road Safety Cameras as a result of the virus;
- whether there has been any impact on the accuracy or reliability of the Victorian Road Safety Camera System;
- whether there may be any future impact on the accuracy or reliability of the cameras as a result of the infection; and
- whether additional security measures need to be employed in order to protect the Road Safety Camera System in future.

BACKGROUND

33 Computers crash. Anyone who deals with computers knows the uncertainties (and sometime unreliability) of working with them. Put a computer outdoors, exposed to the elements, and the uncertainties and unreliability are multiplied. As such it was not necessarily strange for the computers associated with road safety cameras to cease working, or to reboot, as happened on 6 June 2017. However, shortly after 6 June it was clear the problem was spreading, and the higher levels of the DJR, Victoria Police, and the Minister for Police, as well as the Victorian public, needed to be told.

34 Speed is the major factor both in the involvement and severity of motor vehicle collisions. Speed causes driver control to be reduced, driver reaction time shortened, and speed also results in more severe outcomes. The Road Safety Camera Program managed by the DJR represents a key component of the State Government's strategy to save lives and reduce trauma on Victorian roads. To effectively manage the vast Fixed Digital Road Safety Camera Network (**FDRSCN**), a suite of independent contractors has been engaged by IMES. At the time these included three separate camera vendors, five camera testers and an independent infringement verification reviewer. The enforcement of identified infringements is managed by Victoria Police (**VicPol**), in conjunction with independent third parties (Tenix and CCV) to support the enforcement process.

35 In Victoria, two independent **speed** measuring devices must agree within a tight tolerance before a potential infringement can be initiated. An additional manual check is carried out by two assessors, sitting independently. Further processes are in place to ensure the integrity and accuracy of the Road Safety Camera System. If a potential **red light** infringement has been detected, the images recorded by the road safety cameras are scrutinised during manual processing by two assessors, sitting and assessing independently of each other. An infringement does not proceed unless they conclude that the images show the identified vehicle had entered the intersection or pedestrian crossing against a red light or red arrow.

36 In 2010, using 2006 data, the federal Bureau of Infrastructure Transport and Regional Economics (BITRE) estimated the social costs of road crashes in Australia at $17.849 billion. A chart in this regard is **Annexure G** to this RSCC report; the BITRE research report can be found at : https://bitre.gov.au/publications/2010/report_118.aspx

37 On the morning of 22 June 2017, journalist and broadcaster Mr Neil Mitchell telephoned the Minister for Police to ask her about some information that he had received. Mr Mitchell told the Minister, in effect, that 55 cameras had been struck by a virus. In response to this information, the Minister made enquiries of DJR and was, for the first time, informed that a virus had infected the Road Safety Camera System computer network. My office also was first informed by a journalist/producer working with Mr Mitchell, prior to any communication from DJR.

38 My investigations have revealed that at some point on or prior to 6 June 2017 (*not 7 June as I stated in my interim report*), a variant of the WannaCry ransomware virus breached the perimeter of the FDRSC network.

39 The **WannaCry** ransomware virus/worm is a particular type of ransomware, which encrypts data on a computer and threatens to lock the owner out of the data unless a "ransom" payment is made.

40 A number of variants of the **WannaCry** virus exist. In summary, each consists of three major components:

- a "viral worm" to spread the virus;
- an encryption system designed to deny users access to valuable files; and
- a communication tool to inform users, demand ransom and manage payment.

41 The encryption component seeks out "valuable" file types on the infected system (documents, email, spreadsheets, images, movies, etc.) and encrypts them. As part of this process, each file's extension is modified to reflect encryption; for example, *Doc1.docx* might be renamed *Doc1.docx.wncry.*

42 It is worth noting that most variants make no further attempt to harm infected systems.

43 My investigations have revealed that the consequences of the WannaCry infection to the FDRSCN could potentially have included:

- loss of data;
- damage to equipment and systems;
- loss of operational time; and
- reputational risk to the integrity of the fixed road safety camera Program.

44 One of primary concerns of Victoria Police when news of the virus became widely known was to ensure that no inappropriate infringements be enforced. My preliminary investigation, the results of which were published in my interim report, found that there was no compromise of any infringement data.

45 By way of background, the Office of the Road Safety Camera Commission is set up by an act of Parliament. The office receives administrative support from the Department of Justice and Regulation, without which, under present circumstances, it could not function. That legislation, the *Road Safety Camera Commissioner Act* 2011, has lacunas in relation to investigative powers which were identified early in this office's existence. The functions of the office include overseeing the work and communications of the Department of Justice and Regulation in relation to the road safety camera system. These lacunas had been addressed in part in an exchange between my predecessor, the Hon Gordon Lewis AM, and the Director of IMES, in September 2013, which had included the Director of IMES writing:

> I confirm IMES will continue to cooperate fully with yourself and your office and provide information to assist you to perform your statutory functions.

46 Early in my investigation the Minister for Police, the Hon Lisa Neville, wrote to the Secretary of the Department of Justice and Regulation, Mr Greg Wilson, and asked him to ensure that during the course of my investigation, :

> …all representatives of the Department of Justice and Regulation comply to the fullest extent possible with the requests of the Commissioner, his staff, or representatives, including but not limited to requests for documents, records or other data

47 I had expected this request from the Minister would be understood to mean that every relevant document, fact or item would be handed up and volunteered in a collaborative spirit. However what gradually occurred over the months of this investigation seemed consistent with a widespread culture within the relevant parts of the Department (and in particular IMES) of declining to supply relevant information unless it was specifically nominated. There lies the difficulty in this investigation.

48 In my view this approach is not consistent with the expectations of the Victorian public who rightly expect a transparency in communications and disclosure between DJR and a body overseeing specific activities of DJR. It is also inconsistent with the request from the Minister for Police to the Secretary of the DJR, Mr Greg Wilson.

49 By contrast other contractors and suppliers of services, who, with one exception, gave my investigation full and professional cooperation. For example, one service provider identified that they had an infected computer and gave me information in relation to it. That supplier had conducted its own tests and concluded that it had received the virus from the FDRSCN, not infected it. That supplier had written to IMES but IMES did not supply me with this letter or inform me of this infection. I first learnt of it when meeting with the supplier (and that would have been the first meeting if I had known). Another example is of a supplier who had notified IMES that it had an infected computer (just a few days after I had asked the Director of IMES to look out for such a device). IMES received the information from the supplier that they thought they had an infected computer but IMES did not inform me. The DJR arranged to have that computer delivered to a different consultant, without informing me. It subsequently turned out that this computer was not infected, but that was not known when these steps were actioned, and

without informing this investigation. None of this episode was volunteered at the time. Further, as described below, there were other episodes of DJR declining an opportunity to volunteer significant information to the investigation.

50 Rather than adopting a cooperative approach to identifying and providing me with all relevant information, DJR's approach was limited to providing material that was specifically requested by my office. This meant that I was not necessarily aware of all relevant material. I consider that in the future a more cooperative approach is essential to my capacity to conduct investigations effectively.

51 The many suppliers of services who we met all showed very substantial expertise, a desire for continuous improvement, and a desire for a more collaborative system. Some pointed out that currently there is no format for these suppliers to contribute to the improvement of the system. Multiple numbers of service providers referred to a perceived punitive culture from DJR-IMES which discourages admissions of fault or notification of critical issues.

52 I am also unable to confirm the accuracy of some comments from DJR in relation to the information it provided to the Victorian public from first revelation by Mr Neil Mitchell on 22 June 2017, Listeners to Mr Mitchell's program on that day would have heard statements from DJR's representative which have not been supported by evidence to date, including :

- "55" cameras were affected
- All of the affected cameras were intersection cameras, none were on highways
- IMES was not quite finished patching affected cameras. There were still a dozen or so cameras needing repair
- The infection "came on through an infected file of one of the testers"
- The infection came through a "USB stick"
- The cameras were not linked to each other and could not infect each other
- That IMES first became aware of the infection "at the end of last week"

53 That this apparent absence of corroboration cannot be confirmed with certainty because of the limited investigative powers of this office combined with the limited transparency provided by DJR to this investigation. I have endeavoured to draw conclusions in this report based on the available evidence.

INVESTIGATION

54 This investigation commenced with much media interest. The first that the Minister had heard of the infection came through Mr Neil Mitchell, rather than from her Department. The Minister immediately requested me to conduct an investigation of several key points, the first of which was to identify whether the virus had compromised the integrity of any infringement notice generated by the FDRSCN. My interim report found no such compromise.

55 This investigation continued, looking for more detail to locate the cause of the infection and lessons that should be learnt.

56 At all relevant times, IMES has been the manager of the camera systems and also the manager of the infringement process

57 On 22 June 2017, I commenced requesting information from IMES about the infection. I made various further written requests of the Director of IMES and I had been led to consider that IMES was collaboratively cooperating and assisting the investigation.

58 On 24 June 2017, I made a request to the Director of IMES which, omitting formal and irrelevant parts read:

> *I think that it is important for the investigation for us to not make assumptions, to be cautious of the info we receive and wherever we can to ascertain the facts for ourselves.*
>
> *In that regard we will need to obtain an infected hard drive so that we can analyse it. (We hopefully would copy it and return it promptly). We know there is a process of patching the software, I need one that is still "bad".*
>
> *Can your group help out with this, or point me to who I should be asking please.*

59 I have come to understand that IMES had considerable information that was relevant to my investigation. For example, by 29 June 2017, IMES:

- thought they had an infected computer;
- arranged to collect the suspected infected computer; and
- made arrangements for a consultant to investigate the suspected infected computer,

all without informing this investigation.

60 Despite my request to IMES on 24 June 2017, I was not informed of these matters at the time, nor in a timely or convenient fashion. I first learnt of them when I saw third party emails as part of the "10,000 pages of information" delivered by IMES on 9 October 2017 (referred to below).

61 When later pressed, the Director of IMES confirmed that he had communicated my request of 24 June 2017 to all relevant staff. He says he did so orally, and that there is no written record.

62 On 17 August 2017, my representatives met with Tester 1[1]. We were given a copy of a letter that Tester 1 had sent to IMES on 23 June 2017 but which IMES had not shared with my investigation. A redacted version of this undated letter appears as **Annexure E**.

[1] For the purposes of **de-identification**, the various testers will, as appropriate, be named "Tester1", "Tester 2" and so on. Similarly vendors will be referred as "Vendor1", "Vendor 2" and so on.

63 On 17 August 2017, I concluded that IMES were not producing the information that I needed to complete my investigation. In these circumstances I sent an email to the Director of IMES which, omitting formal and irrelevant parts, read as follows:

> *Our investigation into the "WannaCry" infection is continuing. Today our consultant, Stuart McCormack, attended* (Tester 1)*. .*
>
> (Tester 1) *were perfectly helpful, but they also caused us some concern. They informed us for the first time that* (Tester 1) *had an infected device and that they had communicated with IMES in relation to this.*
>
> *The people at* (Tester 1) *gave to us a copy of an undated letter addressed to* [redacted] *of Camera Operations. For the sake of completeness I* ***enclose*** *a copy of that correspondence.*
>
> *Please confirm if IMES received that letter, and the date of receipt.*
>
> *The concern I feel is that this letter could have been voluntarily supplied by IMES to my office for this investigation, but was not.*
>
> *In these circumstances I request that IMES supplies to my office a detailed timeline of every event of consequence regarding the WannaCry infection, and copies of each and every letter, email, note, memorandum, report, request for report, telephone-call records and memos of call, and every other document which you feel is of consequence to the investigation being carried out by this office. I request this be supplied for the period 31 May 2017 to date. Ideally I would like to receive it by close of business 22 August 2017.*

64 On 5 October 2017, I sent an email to the [redacted] in IMES which omitting formal and irrelevant parts, read as follows:

> *As you know this information was initially requested near two months ago. If there is a substantial reason for IMES being unable to deliver the information promptly then please let me know those reasons; and if appropriate the time that you will need in order to do so. Please prove your response by return.*
>
> *If the information is not supplied without a substantial reason, it will be reported that it was "requested multiple times, but not received".*

65 On 9 October 2017, IMES produced what IMES described as “10,000 pages of documents.” The documents were delivered in a format which made digital searching difficult. Further, the emails supplied by IMES were selective, and had attachments removed. Indeed, every attachment to every email produced to me was removed.

66 As I outline below, part of my investigation involved an attempt to identify the origin of the infection. The IT consultants who I engaged were using all the information that I had been given to reverse-engineer when particular cameras (known as “the Hume sites”) actually were infected. Within the 10,000 pages of documents I received from IMES was evidence that IMES had arranged for Telstra to produce logs from relevant cameras. This information was not given to me and nor was I told that it existed.

67 Overall, I was frustrated with the cooperation that I received from IMES throughout the course of my investigation. Much information that I needed for the purpose of the investigation existed within IMES yet I had to find the information for myself. That was more difficult and slower than would have been the case had IMES been of more assistance. Further, the Department of Justice and Regulation’s own mandatory requirements of *Records Management Policy* and *Records Creation and Capture Procedure* have either not always been adhered to, or some relevant records have not been produced to me. Adherence to the Records Managements Standards and Procedures would result in recording and accessing reliable information in a timely manner.

68 The Public records Office Victoria has produced the *Recordkeeping Responsibilities for Public Sector Employees.* A link to the document is here*:*
https://www.prov.vic.gov.au/sites/default/files/2016-05/1010f2%20v2.0.pdf

69 The DJR *Records Management Policy* states in part:

Digital Records

1. Records should be created, captured and managed digitally throughout their lifecycle whenever possible.
2. The department places emphasis on the integrity of business processes and the authenticity of records they produce over the need to retain records in specific formats.
3. Where hard-copy records are digitised under the department's digitisation plan, the digital records produced hold status of the original and official record of the department. The hard-copy record defaults to the status of access copy and may be disposed of in-line with local business procedures.

Creation and Capture

4. Full and accurate records of department activities, decisions, actions or outcomes are to be systematically created to meet business needs, accountability requirements and community expectations.
5. Records are to be authentic, reliable and created by business processes or systems that focus on the integrity of records created.
6. Special consideration is required for the capture and management of records that hold high-risk, high-value or required for long term (greater than seven years) / permanent retention. This is to ensure the department's valuable records are managed to PROV standards and related legislation over their lifecycle.
7. Records are to be correctly and clearly connected to relevant dates, times, people, systems, process, events and other related records to ensure they are reliable as evidence.

70 Further, DJR's *Records Creation and Capture Procedure* states in part:

What records should be created and captured?

All Department of Justice & Regulation (DJR or the department) staff, contractors and volunteers are responsible for creating and managing records of all decisions, actions, outcomes and business activities in accordance with the department's Records Management Policy, Standards, Procedures and Local Records Management Operating Procedures.

What to consider when creating and capturing records

- Refer to your business unit's Local Records Management Operating Procedures and Record Creation Matrix (RCM) and relevant department procedures.
- Ensure records are created as soon as possible after the event they document e.g. after meetings, phone calls, incidents, transactions, decisions and authorisations.
- Ensure records are a full and accurate record of the event they document e.g. who was involved, what occurred or what was decided, when it occurred, where it took place, why the decision or course of action was taken, any relevant background information and so on.
- What recordkeeping system or business system will be used to manage the record? If it is a business system, is the business system an authorised business system for managing DJR records? (Refer the Managing Records in Business Systems Standard).

Recommendations

71 *DJR, and in particular IMES should review its internal management practices, including record keeping.*

- *IMES should aim for improvement in its compliance with the Victorian Public Service* Code of Conduct *and DJR's mandatory requirements for the administration of its functions, including its* Records Management Policy *and* Records Creation and Capture Procedure.
- *every meeting involving decisions or directions which could impact the Program should be minuted;*
- *where there is a change of course, varying from a previously written direction, then that should be minuted and confirmed by email;*
- *where the RSCC has requested an action, a written confirmation of the distribution of that instruction should be minuted.*

CHRONOLOGY

72 Following my investigation, I have been able to reach a number of conclusions about what happened and when. The following table is a summary of my conclusions.

Date	Event
6 June	The first known infection. Older Windows-based systems (Windows XP and Windows 2000) begin to experience increased downtime.
7 June	Vendor 1 Daily Report details 10 “Red” issues.
7 June	Vendor 1 note unusual downtime issues in morning Review Meeting.
8 June	Camera unit at the intersection of Gilbert Rd & Bell St Preston (Ground-Based Unit) is collided into by a vehicle and knocked out of operation, approx. 3:54 AM. *(The hard drive from this machine eventually provided us with our only "live" sample of the virus, which was the basis for analysis by our consultants Blue Connections Pty Ltd.)*
8 June	Vendor 1 Daily Report details 13 “Red” issues.
9 June	Vendor 1 Daily Report details 10 “Red” issues.
9 June	Vendor 1 email to DJR-IMES confirming the 15 sites with issues that will be unlatched (accessed) in the following three hours. (Six more added one hour later.)
10 June	Vendor 1 Daily Report details 22 “Red” issues.
11 June	Vendor 1 Daily Report details 25 “Red” issues.
12 June	Vendor 1 Daily Report details 24 “Red” issues.
13 June	Vendor 1 Daily Report details 23 “Red” issues.
13 June	Vendor 1 supply DJR-IMES with known details of problem and remediation efforts.
14 June	Vendor 1 Daily Report details 32 “Red” issues.
14 June	Serco inform DJR-IMES that, due to communications issues with Vendor 1 sites, 16 sites are up to 6 days overdue for incident download. (3.4 days on average.)
14 June	DJR-IMES and Vendor 1 meet to discuss downtime issues. It is noted that the problem appears - with a single exception[2] - to affect only older machines.
14 June	Vendor 1 calls DJR-IMES. They suspect that the issue is virus on a Windows 7-based systems. They will confirm ASAP.
15 June	Vendor 1 formally notify DJR-IMES of the WannaCry infection.
15 June	DJR-IMES emergency meeting.

[2] A Windows 7-based Camera Control Unit – King & Hawke Streets, West Melbourne - also appeared to be failing. Investigation proved the issue to be a communications problem and the Windows log files demonstrated that the system was never actually “down”.

Date	Event
15 June	DJR-IMES informs contractors of the infection. Requests immediate checking of associated test & maintenance equipment.
15 June	(Tester 1) computer 31543 is logged off for the first time in several days (see 23 June)
16 June	Email within IMES to inform certification contractors that – due to an exhausted budget – certification processes are cancelled. This is confirmed in meeting Agenda for the same day, but for which no minutes were available. (IMES inform us that despite no paper record to the contrary, this email was “wrong” and that the cancellation of certification was itself “cancelled”)
16 June	Vendor 1 request Work Authority to disinfect & patch all Windows 7-based sites.
16 June	(Tester 1) detect an issue on one of their test laptops. An email sent by (Tester 1) to DJR-IMES identifies that one of their field computers *“is not currently available for use.*" but does not specifically mention infection.
17 June	Vendor 1 inform DJR-IMES that patched test systems have run correctly overnight. *Also, that other, non-Vendor 1 systems on the FDRSC are infected.*
18 June	First site records deactivation due to “Testing Schedule Lapse”. (Princes Highway, Norlane, (Vendor 2) device)
19 June	Vendor 1 request Work Authority to patch Windows XP and Windows 2000 sites.
19 June	DJR-IMES confirm intention to follow up on other infections.
19 June	(Vendor 2) request Work Authority to disinfect & patch all sites.
19 June	DJR-IMES informs (Vendor 2) that three of their sites are infected.
19 June	(Vendor 2) informs DJR-IMES that three sites have now been scanned and infections removed. (Vendor 2) now working through other sites.
21 June	Vendor 1 informs DJR-IMES that Windows 7-based systems are now all disinfected and patched. No signs of further infection attempts.
22 June	Mr Neil Mitchell telephones the Minister for Police and informs her of the information he has received in relation to the virus attack. This is the first that the Minister, or the public, have heard of an infection in the FDRSCN.
22 June	Sites at Main St, Lilydale, (Vendor 2), fail to patch correctly. *(The hard drives from these systems were later examined by Blue Connections, but no remaining ‘live’ virus was found.)*
22 June	DJR-IMES informs Serco that all (Vendor 2) sites are to be "Deactivated" from 14 June 2017. The sites are to remain deactivated until further notice. (*The (Vendor 2) sites were not "reactivated" and produced zero infringements over the 8 days spanning 14 June through 21 June*.)

Date	Event
22 June	DJR-IMES informs contractors that all testing and maintenance is cancelled until further notice.
22 June	DJR-IMES informs Vendors that remote access to sites and daily monitoring can recommence, but that no physical site visits are permitted.
23 June	Vendor 1 Daily Report details 2 “Red” issues. ***Infection over.***
23 June	(Tester 1) inform DJR-IMES that the test laptop 31543 which did not have “up-to-date” virus templates (see 16 June) is infected. In their (Tester 1’s) professional assessment that infection was received on 7 June while working on Hume Highway sites.
24 June	RSCC email to IMES requesting that we need to obtain an infected hard drive for analysis.
29 June	DJR-IMES requests of Vendor 1 that a computer from site B14, Hotham St and Balaclava Road St Kilda East, be removed and set aside for its consultant.
11 July	DJR-IMES email Telstra re FDRSC router *Network segregation is not working correctly.*
18 July	Vendor 3 inform DJR-IMES that two sites are certification expired and that another will expire in the next week. - Geelong Rd & Droop St, Footscray - Doncaster Rd & Victoria St, Doncaster - Fitzroy St & Lakeside Drive, St Kilda
21 July	(Tester 1) note that they would be testing but that "*sign-off of contracts might take a while*".

THE FDRSC INFECTION

73 An important part of my investigation was to attempt to establish when the FDRSC system was first infected by the virus, at what location and by what mechanism.

74 In considering the infection, I was assisted by DJR giving me some access to the SiteTrak database. SiteTrak is a database used by IMES to record Work Authorisations and work done on FDRSC systems. With that data, together with subsequent analysis of some infected hardware, I was able to make an assessment of the likely time and location of infection.

75 During the virus disinfection phase, two (Vendor 2) machines failed to patch correctly and were removed from service. Another (Vendor 2) system was recovered after its roadside cabinet was struck by a vehicle in the early hours of 8 June 2017, camera F34 located at Gilbert Rd & Bell St, Preston (see **Annexure F**). Blue Connections Pty Ltd examined the hard disks of these three camera systems at my direction and found a sample of the virus on F34. This virus sample was then repeatedly run in a virtual environment.

76 Until this step, the only infection timeline data available were the time-stamps of infected files previously recorded by Vendor 1 on their systems. These time-stamps ranged over a period of weeks.

77 Blue Connections noted that the WannaCry infection left data in Windows Event Log files as part of the infection process. I asked Vendor 1 and Vendor 2 to scan their system logs for such tell-tale entries, and at short notice these firms gave full cooperation to my investigation.

78 The resulting data indicate that the virus infection spread much more rapidly than had been previously thought. **The 102 road safety camera systems for which I have log data were all infected within a period of 48 hours commencing at 11:09:55AM on 6 June 2017.**

79 **Annexure B** to this report is a document I received from IMES in response to my request for a list of all the road safety cameras which were infected. It identifies 55 FDRSCs, and was the basis of a post on the camerassavelives website. It was the best guess as at 22 June 2017.

ANALYSIS

80 Initially I had been informed that the infection was first detected in the road safety cameras on the Hume Freeway. All of the Hume cameras are on the FDRSCN subnet F 0.0. The infection spreads sequentially in increasing order. Most F machines are Windows XP and Window 2000 so cannot be infected. Instead, these machines would be affected and would 'reboot'.

81 As time passed the evidence in the Windows logs was overwritten.

82 This table identifies the **first 25** known infections. Infections were often sequential across the subnets (IP addresses beginning with, in this instance, F , G and H). The first found infection on F subnet was less than 8 minutes after the first infection on the G subnet. The chart shows that the addresses were infected sequentially in numerical order but for the F subnet infection.

Site	Vendor	IP Address	Infected	Location
A13	V1	G .2.2	6 Jun 2017 11:09:55	Gordon Street & Barkly Street, Footscray
A12	V1	G .3.2	6 Jun 2017 11:10:24	Elizabeth Street & La Trobe Street, Melbourne
A21	V1	G .9.2	6 Jun 2017 11:14:25	Whitehorse Road & Burke Road, Balwyn
C08	V1	F .12.2	6 Jun 2017 11:17:39	Nicholson Street & Victoria Parade, East Melbourne
B14	V1	G .12.2	6 Jun 2017 11:18:09	Hotham Street & Balaclava Road, St Kilda East
B01	V1	G .16.2	6 Jun 2017 11:22:36	King Street & Hawke Street, West Melbourne
B10	V1	G .17.2	6 Jun 2017 11:24:15	Whitehorse Road & Elgar Road, Box Hill
C02K	V1	G .25.2	6 Jun 2017 11:33:39	Hoddle Street & Victoria Street, Abbotsford
C02M	V1	G .25.6	6 Jun 2017 11:34:08	Hoddle Street & Victoria Street, Abbotsford
C16K	V1	G .34.2	6 Jun 2017 11:42:34	Nepean Highway & Karen Street, Highett
C16M	V1	G .34.6	6 Jun 2017 11:43:25	Nepean Highway & Karen Street, Highett
C19K	V1	G .36.2	6 Jun 2017 11:47:43	Nepean Highway & Warrigal Road, Mentone
C23K	V1	G .38.2	6 Jun 2017 11:48:12	High Street Road & Stud Road, Wantirna South
C19M	V1	G .36.6	6 Jun 2017 11:48:13	Nepean Highway & Warrigal Road, Mentone
C23M	V1	G .38.6	6 Jun 2017 11:49:15	High Street Road & Stud Road, Wantirna South
C26K	V1	G .41.2	6 Jun 2017 11:50:29	Princes Highway & Belgrave Road, Malvern East
C26M	V1	G .41.6	6 Jun 2017 11:50:59	Princes Highway & Belgrave Road, Malvern East
F01	V1	H .100.2	6 Jun 2017 12:19:09	Prospect Hill Road & Burke Road, Camberwell
D08M	V1	G .51.133	6 Jun 2017 21:10:37	Stud Road & Wellington Road, Rowville
A49	V2	H .5.1	7 Jun 2017 01:52:31	High Street & Summerhill Road, Glen Iris

Site	Vendor	IP Address	Infected	Location
C09	V1	F .13.2	7 Jun 2017 02:00:38	Station Street & Thames Street, Box Hill
F48	V2	H .42.1	7 Jun 2017 02:20:55	Princes Highway & Sparks Road, Norlane
M11NA	V2	H .42.68	7 Jun 2017 02:27:51	Monash FWY approx. 290m South of High St, Glen Iris
M11SA	V2	H .42.81	7 Jun 2017 02:28:33	Monash FWY approx. 470m South of High St, Glen Iris
M11SB	V2	H .42.86	7 Jun 2017 02:30:09	Monash FWY approx. 470m South of High St, Glen Iris

Legend: V 1 Vendor 1
V 2 Vendor 2

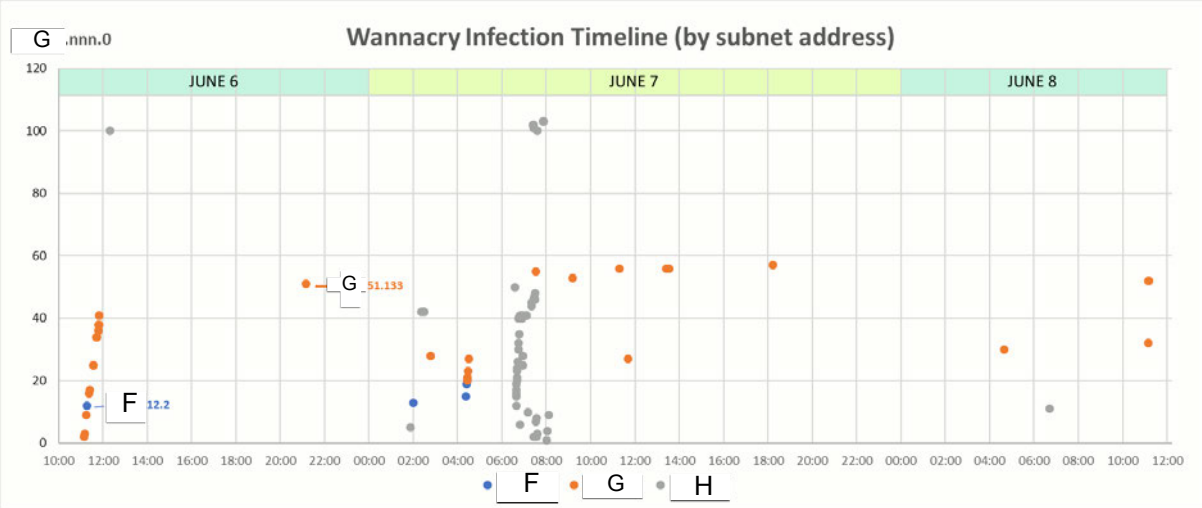

Figure 1 – WannaCry Infection Timeline (by subnet address)

83 Infection Timeline depicted in Figure 1 shows the date and time of the earliest log entry for each **infected** machine on each subnet. It signposts the largely sequential nature of attacks. The vertical address reports the value of the third IP address chunk. For example, the 21:10 infection of G .**51**.133 is plotted in orange with a vertical value of 51.

84 However, not all of the attacks were sequential within a subnet. For example, the 8 June 2017 infection plots might be the result of automatic overwriting of the Windows Event logs rather than a long delay in infection.

85 ByteSmart and Blue Connections were of the view that the data depicts a "long" delay — nine hours — between the infection of the G .41 subnet and the infection of the G .51 subnet. In the 18 infections prior to G .51.**133**, the value of the fourth IP address chunk does not exceed 6. In these circumstances I am of the view (based on the advice I received from ByteSmart and Blue Connections) that it is reasonable to infer that the virus gave up sequential attacks long before it reached a value of 133.

86 ByteSmart and Blue Connections conclude, and I accept, that: the virus mounted systematic sequential address attacks but, when eventually unsuccessful in finding new candidates, reverted to random attacks.

87 Each time the virus attempted to re-infect it left an entry in the Windows log in that computer, so the consultants concluded that the earliest entries were the likely indicator of when the machines were first infected. This is important for two reasons:

- it matches the date and time of first previously known infections, and

- it contradicts an earlier analysis of the spread of the virus which had been based on file time stamps. The previous analysis had considered the infection took two weeks to complete but analysis of the Windows logs showed it took 48 hours.

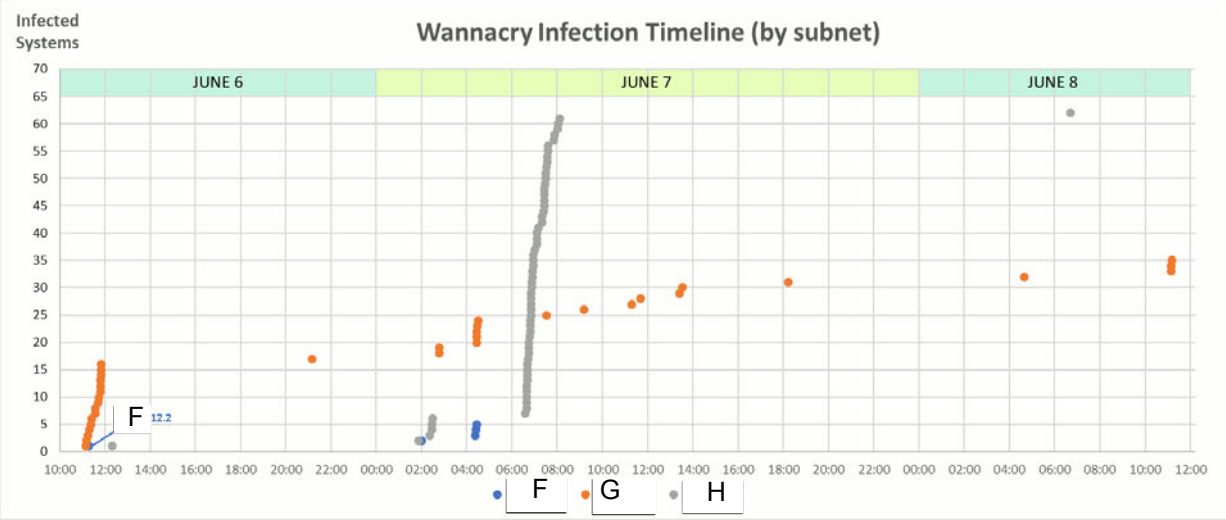

Figure 2 – WannaCry Infection Timeline (by subnet)

88 Figure 2 depicts the date and time of the earliest log entry for each infected machine on each subnet. It demonstrates the speed at which the FDRSC was infected. For example, 55 systems on the H .0.0 subnet were infected in just over 90 minutes.

89 The first 18 known infections on the FDRSC occurred within 70 minutes of each other.

90 The virus appears to have moved from subnet G .0.0 to F .0.0 (C08, labelled in blue in the above graph) in only 8 minutes; ***this is an unexpected and improbable result*** and does not correlate with other recorded subnet "jumps". ByteSmart and Blue Connections considered that there may have been a second infection within 8 minutes but other possibilities were also considered.

91 The infection timeline data imply that the infection attempts to spread by attacking IP addresses in a generally sequential fashion. The spread from the G .0.0 subnet to H .0.0, (site F01 above) for example, appears to have taken 70 minutes and, by this time, at least 18 machines on the FDRSC were infected and were attempting to further spread the virus. However, the spread from G .00 to F .0.0 (site C08 above) occurred very quickly and is a jump ***backwards*** in sequence.

92 There are other "backward" jumps recorded in the infection timeline. For example, the jump from the FDRSC at Prospect Hill Road & Burke Road, Camberwell (F01) (H .100.2) to the FDRSC at High Street & Summerhill Road, Glen Iris (A49) (H .5.1) is a backward jump based on the third set of digits (from 100 back to 5.) Even with at least 20 infected systems on the FDRSC attempting to spread the virus, it required more than thirteen hours to make this jump. ByteSmart and Blue Connections advised me, and I accept their opinions, that:

> *The most likely interpretation of the backward jump from subnet G .0.0 to F .0.0 in only 8 minutes is that the infection **actually began earlier** on the F .0.0 subnet. Also, that the virus found a target on the G .0.0 subnet at Gordon Street & Barkly Street, Footscray (A13) before it found its next candidate system on the F 0.0 subnet at Nicholson Street & Victoria Parade East Melbourne (C08). This interpretation would also explain why affected systems on the Hume Highway – all of which are F .0.0 addresses – were early reported to have been crashing and rebooting.*

93 On this basis, and if the initial infection source was a machine connected to the F .0.0 subnet and was crashing systems on the Hume, there should be evidence in the systems logs. Repeated crashes taking place *earlier than the first known infection* would point to the time, and therefore possible source, of the initial infection.

94 However, by the time I came to this conclusion, system logs for 6 June 2017 on Hume sites had been automatically overwritten so that the histories in the logs were truncated and were no longer available.

95 Instead, I examined the SmartDip records for Hume sites on 6 June 2017. I reasoned that if, at a given time, a number plate was recognised then the system must be operational; otherwise there would be no image and the number plate could not be 'read'.

96 I examined 140,846 Hume events relating to 6 June 2017 traffic in 1,776 files. In particular, I looked at every single minute of 6 June 2017 on the Hume: for every lane, and for every Hume site, I noted if a number plate had been detected during that minute (up until 23:45). I first examined the results by IP Address but soon found the results to be more meaningful when arranged by direction, distance and lane. The results are shown in the following graph (Figure 3):

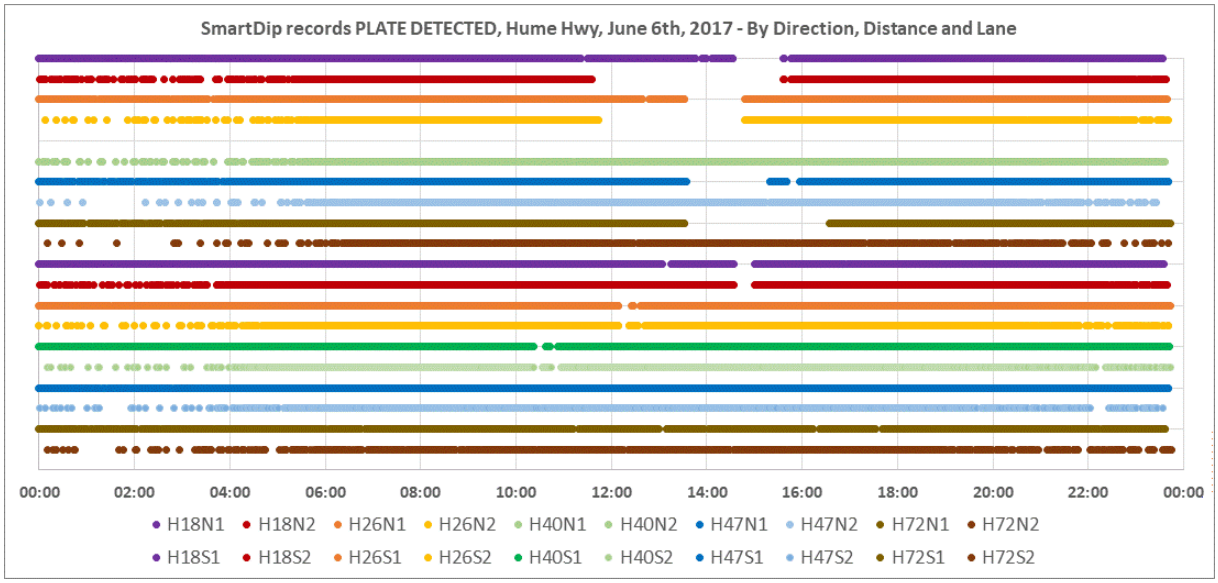

Figure 3 – SmartDip records – Hume Highway – 6 June 2017

97 In Figure 3 each dot represents a minute in which at least one plate was detected and read. From top to bottom the sites are shown first Northbound, then Southbound. H47S2, for example, is Hume Highway, 47 km out, Southbound, Lane 2. H40N1 was not operational on 6 June 2017.

98 Figure 3 shows interruptions in processing, but only H40S records show interruptions prior to the time of the first known infection. (H40S appears down between 10:23 and 10:36, again between 10:44 and 10:56). A similar pattern is displayed at H26S some two hours later.

99 However, the pattern displayed by H40S is not clear evidence of an attack on that site:

- H40S was undergoing testing at the time. The test report states that the cabinet was open between 10:15 and 11:26.

  [Note that it is not a requirement that a system be directly connected to, say, for example, a tester's infected laptop in order to contract the virus. The virus spreads over a *network* and, at the time of infection, there was nothing to stop the virus spreading from and to *any* FDRSC site.]

  The fact that H40S was unavailable during a test process did not compromise the analysis.

- The first known infection on the F .0.0 subnet was Nicholson Street & Victoria Parade East Melbourne, C08, at 11:17 AM. The IP subnet of C08 is F .12.0. For H40 it is F .26.0. This site was non-operational, but the hardware was connected to the network.

ByteSmart and Blue Connections conclude, and I agree, that the attacks on IP addresses were in a sequential fashion. If H40S was the source of C08's infection, then the virus would have to have attacked addresses in reverse order.

100 I assumed that IP address attacks are largely sequential in nature *and* that the F .0.0 subnet was attacked first. I looked at systems on that subnet that might be candidates as the infection source. To be such a candidate, the system's IP address must precede the 12 in C08's third component of F .12.0.

101 There are few such systems, and the investigation proceeded to examine each of them. These were all investigated as the possible infection source. In subnet order, these are:

Site	Location	Subnet
B23	Intersection of Union Road & Mont Albert Road SURREY HILLS	F .4.0
B12	Canterbury Road & Bayswater Road BAYSWATER NORTH	F 5.0
Serco Primary	535 Bourke Street MELBOURNE	F .7.0
Vendor 1	(Vendor 1's business premises)	F .8.0
C01K	Intersection of Flinders Street & William Street MELBOURNE	F .9.0
C01M	Intersection of Flinders Street & William Street MELBOURNE	F .10.0
C03	Intersection of William Street & Flinders Street MELBOURNE	F .11.0

102 In considering the various possible sources, B23 looked a likely source. SiteTrak reports that, on 6 June 2017, B23 was physically examined due to a communications problem. *"Investigated comms to router. Power cycled router. System checked and tested OK."* While possible, ByteSmart and Blue Connections considered it unlikely that a router would be tested without a test device being connected to it. It was conceivable, however unlikely, that such a test would be undertaken by a non-affiliated communications engineer using their own hardware.

103 What the records show, however, is that both the SiteTrak database and Serco's Quarantine Report state that the B23 cabinet was closed at 10:31 AM. Given that B23 is a Windows 2000 machine — and so could not itself be infected — then for a system connected at B23 to be the source of the infection it would have needed to infect a remote Windows 7 system prior to 10:31 AM. There is no evidence of any such infection at any FDRSC site and neither Serco nor Vendor 1 report any infection in their offices.

104 No work was done on C01 or C03 on 6 June 2017.

105 B12 remained a candidate of infection source and is discussed in more detail below.

106 I have examined SiteTrak data for all maintenance, testing and problem resolution efforts undertaken on the FDRSC in the period 3 June through 7 June 2017. I have checked Serco's quarantine rejection times for the same period. (Quarantine rejection times are the times for each site when infringements may not be issued due to work at the site, mostly due to the roadside cabinet being *open* at the time.) I have also reviewed the associated test and maintenance reports, from records delivered to IMES by testers.

107 No one has volunteered to have been the source of the infection, and so this investigation has been an attempt to reverse-engineer various steps. Whilst it might be plausible that the infection of the FDRSC came from an external corporate network (such as, for example, a network to which certain contractors are connected), there is no evidence, nor can I expect ever to have any evidence, that this has been the case. Apart from a single test laptop which was volunteered by (Tester 1) all associated parties deny any relevant infection external to the FDRSC.

108 On the existing evidence:

- the infection was associated with some test or maintenance activity, and
- the earliest infection that I have located was at 11:06 AM on 6 June 2017.

It follows that the source of the infection must be associated with a "connection event" that began before 11:06 AM and finished after this time.

109 On the evidence available the following seven sites were considered the only possible sources for the infection:

Site:	H40 - Intersection of Hume Highway & Mt Fraser Road WALLAN				
Purpose:	Sensor testing. Reports 618920 & 618950				
Subnet:	F .26.0	**Visit ID:**	53931, 53973	**Contractor:**	[redacted]
Open:	10:15	**Close:**	11:26		

H40 was initially considered a strong contender as the infection source. H40 resides on the F subnet and [redacted] later reported an infected test laptop with an infection time-stamp of 7 June 2017.

Although time-stamps often reflect reinfection rather than initial infection times, there is no direct evidence to suggest [redacted] as a more likely candidate than other contractors. It should be noted that, by midday on 7 June 2017, at least 94 FDRSC sites were infected and all were actively seeking other hosts to infect.

Site:	B12 - 334 Bayswater Road (in Canterbury) BAYSWATER NORTH				
Purpose:	Programmed/Routine Quarterly Maintenance				
Subnet:	F .5.0	**Visit ID:**	53883	**Contractor:**	[redacted]
Open:	10:20	**Close:**	12:38		

B12 is a likely infection source; its IP address is sufficiently early, it resides on the F subnet and the cabinet Open and Close times span the times of the first known infections. This evidence, however, is not conclusive.

Site:	B26 - Intersection of Mt Dandenong Road & Dorset Road CROYDON				
Purpose:	Programmed/Routine Quarterly Maintenance				
Subnet:	G .18.0	**Visit ID:**	53879	**Contractor:**	[redacted]
Open:	10:48	**Close:**	12:15		

Possible candidate, but less likely because it is on the G subnet.

Site:	C15 - Intersection of Whitehorse Road & Surrey Road BLACKBURN				
Purpose:	Sensor Evaluation test				
Subnet:	F .17.0	**Visit ID:**	53764	**Contractor:**	[redacted]
Open:	10:13	**Close:**	11:02		

C15 is a likely candidate only if a later 11:08 to 11:19 event was also conducted by [redacted]. However, we understand this second event to be a remote health check by the vendor, [redacted]

Site:	D02K - Intersection of St Kilda Road & Fitzroy Street ST KILDA				
Purpose:	Remote access to check TIRTL operation				
Subnet:	G .51.0	**Visit ID:**	53960	**Contractor:**	[redacted]
Open:	09:53	**Close:**	11:19		

Serco has not recorded any quarantine times for D02 on 6 June 2017

Site:	F39 - Burwood Highway & Stud Road WANTIRNA				
Purpose:	Sensors, Inventory & speed				
Subnet:	G .56.0	**Visit ID:**	53900	**Contractor:**	[redacted]
Open:	09:16	**Close:**	13:39		

Possible candidate.

Site:	F53 - Intersection of Hume Highway & Camp Road CAMPBELLFIELD				
Purpose:	Sensor tests				
Subnet:	G .57.224	**Visit ID:**	53860	**Contractor:**	[redacted]
Open:	09:37	**Close:**	12:30		

Possible candidate.

110 Work undertaken at PL33N — Peninsula Link, Loder's Road — also spanned the times of the first known infections. However, communications at PL33N were unavailable from December 2016 to late 2017.

111 On the available evidence these sites might be candidates for the source of the infection, although they are not necessarily the first infection. This is because, due to the old operating systems, some of these computers could not be infected.

112 The infected (Tester 1) laptop went undetected for at least next nine days. During that period, more than 100 infected FDRSC hosts were attempting to spread the virus to every connected machine. It is highly plausible that there were infections to other test / maintenance devices unless all other hardware was patched with the necessary security software, up-to-date and immune. I have been unable to determine if that was the case or whether other infected hardware was not revealed to me.

113 In order to receive patches, the test hardware most likely would need to be regularly connected to a corporate network, or a wider internet. Such connections currently represent a threat to both the FDRSC and the corporate networks.

Findings

114 Consistent with advice from Vendor 1 to IMES on 15 June 2017, Blue Connections advise, and I accept in full, that the variant of Wannacry was only capable of (a) spreading to Windows 7 machines, without resulting in data encryption, and (b) causing Windows XP machines (and Windows 2000) to crash. It should be noted that this malware only attempts to propagate via a Windows File Sharing (SMB) flaw, and not via other vectors. There is no indication that the malware could propagate by infecting a portable USB drive that was then connected to another system.

115 It has not been possible to identify the source of the infection. The infection could have come from a range of possible sources. No organisation volunteered themselves as a possible source of the infection. This may be because of the risk of a fine for breach of contractual service delivery standards. In my view this approach discourages early reporting of issues of the kind experienced during the WannaCry infection.

Recommendations

116 *There should be a full review of Windows devices on the network to validate the subnet mask configuration on each device.*

117 *That the reporting and fixing of problems requires that IMES establish a collaborative relationship with its contractors.*

THE FDRSC NETWORK DESIGN

118 Currently the network appears to have developed as a result of growth, and historic practices rather than through an overall design plan. This has resulted in linking of camera sites to each other. There is no reason why these sites should be linked in this way. Indeed there are risks with this design, such as vulnerability to spread of a virus.

119 The expert opinion of Blue Connections, which I accept in full, included recommendations for the segmentation of the FDRSC network from all third parties and contractors by leveraging Telstra's IP WAN networking capabilities. They further recommended that FDRSC dedicated centralised firewalls be installed to protect the network. This would result in all communication to the FDRSC network being controlled by firewall policies where full packet inspection and threat prevention profiles will be configured.

Network Activity Monitoring

120 In a corporate network, users can attempt to connect to any internet address; network managers attempt to limit access to dangerous sites.

121 On the FDRSC network, any attempt to reach an unknown site should immediately raise an alarm. And, since the number of *known* (legal) sites is very small, malicious attempted connections will be easy to detect.

122 However, without a dedicated, centralised firewall such monitoring cannot occur.

Patch Management

123 The FDRSC site hardware is not kept up-to-date with the latest security patches. However, the network reconfiguration I have recommended will minimise the need for such measures.

124 A middle-ground approach would be to make patching part of the annual certification process:

- Certification would proceed as normal and demonstrate whether the system has operated correctly in the previous twelve months.
- Camera Control Units and their software are not covered under the act and are often removed by the vendor. Operating System patching could be made a mandatory part of this process.
- The complete system is then reinstalled and retested to demonstrate its correct functioning.

Such a compromise solution is far from ideal.

125 Firstly, it is the Speed Detection devices which are certified. To minimise site downtime during Certification, Vendors often "hot-swap" the current Speed Detection devices with already-certified devices. The Camera Control Unit is not necessarily "down" for an extended period.

126 Secondly, periodic patching can be ineffective in that a system patched, say, three months ago is still at risk from more modern threats. This argument too has merit.

Regular Security Audits

127 Some of the FDRSC contractors require military-standard security on their corporate networks. Others have less stringent requirements.

SiteTrak

128 The SiteTrak database is a collaboration between IMES and Serco to record and report Work Authorisations and all work done on FDRSC systems. Its value is unquestioned.

129 However, in reviewing SiteTrak data I have observed two shortcomings worth reporting:

- SiteTrak does not clearly categorise the reasons for site deactivations. For Red Light systems alone and over an 18 month period, I detected 181 causes for downtime, all grouped under the heading of “Deactivation”. Given that this “Deactivation” downtime comprises around 15% of FDRSC overall availability, this category should be broken down into more meaningful sub-groups.
- SiteTrak does not appear to maintain an objectively accurate historical record. SiteTrak details; for example entries such as Deactivation period start and end times, can be changed retrospectively. The requirement to be able to narrow such times as more information comes to hand is not in dispute. However, standard database practice in such an environment require a complete history of such changes to be retained. My access to SiteTrak is limited, but I have no evidence that such audit trails are retained.

[redacted]

130 [redacted]

Blue Connections' Proposed FDRSC Configuration

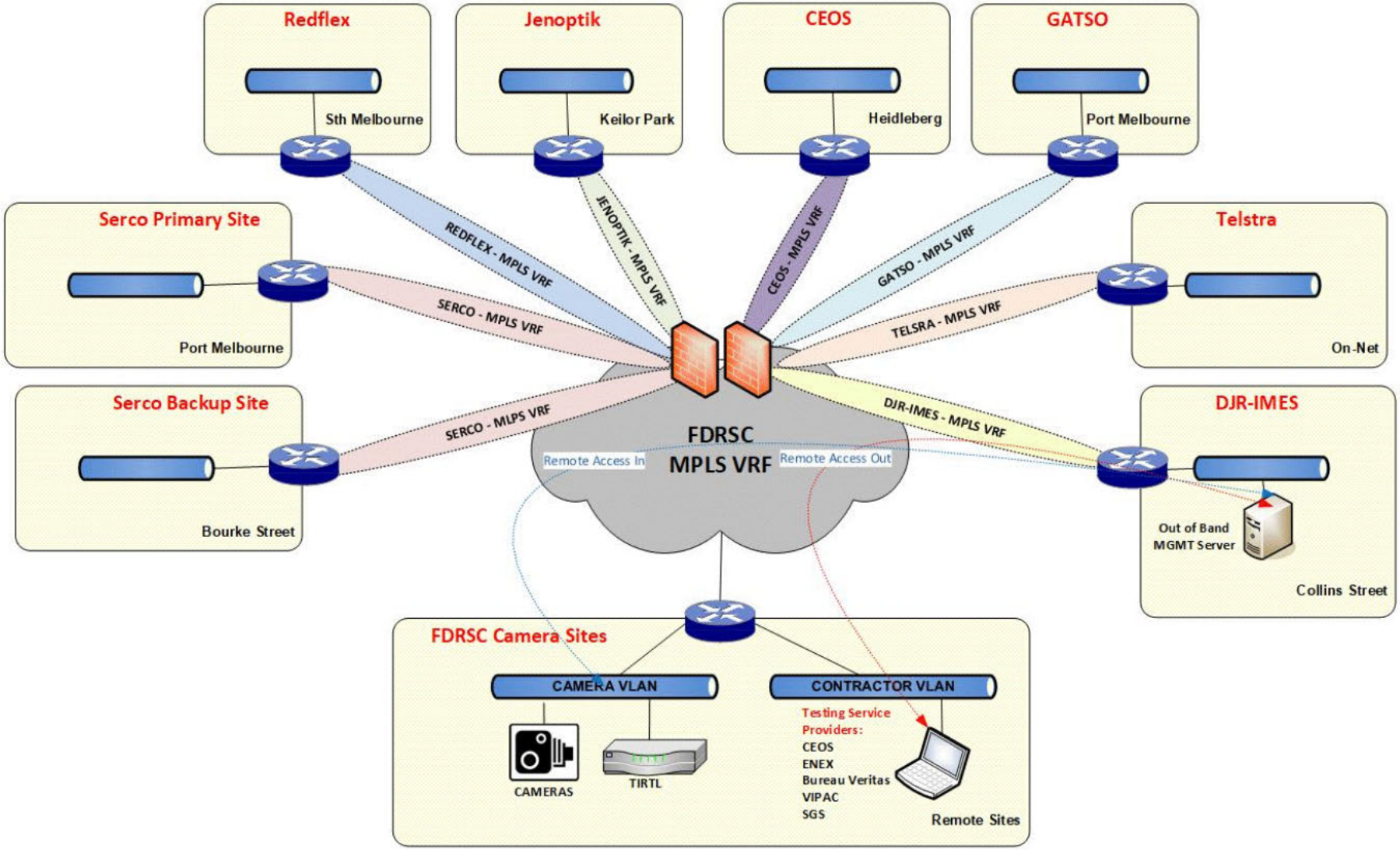

Figure 4

Findings

131 The current design of the FDRSC network lacks appropriate security.

132 Some of the systems were infected with malware due to vulnerable operating systems that did not have critical patches applied. This infection and subsequent spread was assisted by poor Network topology, and security design.

133 The approach to cyber-security of the network was based on the experience to date which was believed to have worked without issues rather than proactively seeking to identify and manage risks.

Recommendations

Network design

134 *I make the following specific recommendations about the FDRSC network design:*

- *there be segmentation of the FDRSC network from all third parties and contractors by leveraging Telstra's IP WAN networking capabilities;*
- *FDRSC dedicated centralised firewalls be applied to protect the network;*
- *all traffic to the FDRSC network will be controlled by firewall policies where full packet inspection and threat prevention profiles will be configured;*
- *all communications traffic is routed through dedicated firewalls;*
- *the firewalls be equipped and maintained with state-of-the-art security features including intrusion prevention, packet inspection, threat detection and Wildfire zero-day threat detection;*
- *all parties — vendors, testers, DJR, Serco, etc — may connect to the FDRSC. That is, no contractors are "air-gapped".*
- *test-related software be maintained on a dedicated OoB server. All testing parties connect to camera sites via and by using software on this server;*
- *out-bound communications from a camera site be strictly limited. A camera site may communicate with its vendor, Serco, IMES and the OoB Server. With possible minor exceptions such as Point-to-Point servers, few other connections are necessary or permissible;*
- *in the event of a future infection, for every infected system, copies of the Windows Event logs be retained (System, Application and Security logs). For each class of infected hardware, a hard drive should be removed and "bagged"; that is, removed from use and maintained in an unmodified state;*
- *there be regular security auditing of IT security of the FDRSC contractors;*
- [redacted]

135 *It is evident that the design of the FDRSC network needs to be updated to modern, high-security standards. Specialist capability separate to IMES should be developed to perform such a task. I have not seen evidence that IMES in its current form could perform this task. However, day-to-day management, monitoring and reporting on the FDRSCN and the ongoing management of the OoB systems should continue to be delivered by IMES.*

136 *I recommend that a specialist organisation oversees the reconfiguration of the FDRSC and then periodically reviews its operation.*

Network Configuration and Out-of-Band Server(s)

137 *All outbound communications from FDRSC camera sites should traverse a central firewall. These connections should be limited to a handful of specific target addresses. Attempts to reach other addresses should trigger an immediate alarm.*

138 *One of these permitted sites might, for example, be a one-way file "DropBox" equivalent. This would allow contractors to recover site data in a highly controlled environment. Serco may be an exception here.*

139 *All network communication incoming at a site must also traverse the central firewall. Most if not all communication would be controlled from virtual sessions via the OoB Servers.*

140 *The proposal is that to reach the FDRSC a party must first "log-in" to the OoB Server. A virtual environment, very much like a remote Citrix login to the DJR, is then constructed. In these circumstances software and connection methods to the FDRSC would be those preconfigured and pretested on the OoB Server.*

141 *Under the suggestion in the previous paragraphs, testers on site and physically connected to the site router would be unable to connect to any other site hardware except via the OoB.*

142 *My office has discussed this concept with some of the testing contractors. Their response was very positive. As well as describing the concept as a more "modern technology", some have pointed out that on-site safety, all-weather testing and out-of-hours maintenance would also improve.*

143 *Additionally, precise incident rejection times (site being accessed) would always be automatically available to SiteTrak.*

GOVERNANCE

144 The Minister for Police, the Honourable Lisa Neville, requested my advice on the adequacy of the management and oversight of the road safety camera Program. She envisaged this would encompass the management and performance of providers contracted to deliver and maintain the Program and also the governance and internal accountabilities within DJR.

145 I arranged for the review of the governance of the FDRSCN. After discussion with consultants, it became clear that the issues would be refined into several parts. Key to these issues would be questions of whether the FDRSCN is being delivered:

- With clear lines of accountability;
- With clear oversight and transparency of the delivery;
- Whether risk and mitigation strategies set in place a model that includes systems for strong proactive identification of risks to ensure detection of issues;
- Whether there are robust measures to mitigate the risks once they have been identified;
- Whether there is stakeholder engagement, to understand the needs of stakeholders;
- Whether the model has feedback loops on Program performance from stakeholders, to ensure continuous improvement;
- Whether personnel have appropriate skills and capabilities to oversee and deliver the Program;
- Whether there is sufficient flexibility to scale up and down as required to meet the needs of the Program;
- Whether the reporting and monitoring processes are in place to report on Key Performance Indicators (KPIs);
- Whether the reporting occurs on a regular basis to monitor performance, risks and outcomes;
- Whether the Program is delivered in a cost-efficient way for government;
- Whether staff are responsive to Ministerial and/or senior executive needs;
- Whether their key activities and transactions are documented and stored appropriately;
- Whether the processes exist to evaluate the quality of the stored documentation;
- Whether financial management systems are in place to manage the delivery of the Program;
- Whether there are processes in place to report on Key Performance Indicators;
- Whether KPI reporting occurs on a regular basis to monitor performance, risks and outcomes.

146 The Victorian Auditor-General's Report *Road Safety Camera Program* (August 2011) stated in part:

> "*While there can be no absolute guarantee over the accuracy of any system, the processes and controls in place provide a particularly high level of confidence in the reliability and integrity of the road safety camera system*."

147 The FDRSCN is one of the key pillars supporting the State Government's commitment to reduce road fatalities, promote road safety and change driver behaviour. In my view, having completed my investigation, the Program is not appropriately structured to ensure ongoing success and support (potential) future growth in fixed road safety cameras across Victoria. Furthermore, in my opinion, the Program does not have the governance framework, systems and processes to effectively and efficiently respond to a crisis, as identified during the WannaCry virus infection incident.

148 IMES are the custodians of and manage the FDRSCN network. KPMG concluded that IMES' business processes for managing the Program are largely manual in nature, reactionary, have excessive delays and are not scalable to accommodate future growth in the Program. IMES has not developed processes to enable its teams to manage the Program by 'exception'. Instead, IMES staff spend significant amounts of time reviewing large volumes of data, for example, to

gather insights into the performance of cameras and determine whether risks in the system have materialised.

149 My investigation has revealed that IMES lacks appropriate governance, processes and resources to effectively discharge its responsibility as a network manager. For example:

- it has a lack of networking tools to proactively monitor activity on the network (the network is not being monitored at all times). This includes a lack of intrusion detection systems and anti-virus or patch management software on the network;
- it is unable to adequately maintain accountability over access to the network. Staff members employed by service providers and testers have generic log-in details as opposed to unique user access profiles; and
- there is a lack of regular monitoring and review over access to the network and anomalies identified across the network. There are no checks performed to ensure user access to the network is current and correct. For example, one stakeholder that I interviewed asserted that there is a router located in the old IMES building that still has access into the FDRSCN network.

150 Improvement of the design of IMES' business processes would assist IMES in proactively managing the Program, from a business as usual perspective and from a critical incidents perspective.

Recommendations

151 *The following matters associated with the governance of the Program need to be considered by Government:*

- *improving the governance structure to direct and give oversight to the Program;*
- *improving the design of systems to manage and monitor the FDRSCN network including (in order that the Program transparently deliver on its objectives in an economic, efficient and effective way):*
  - *a. business processes: to manage the Program on a "business as usual basis";*
  - *b. processes to identify when the Program is not providing business as usual;*
  - *c. processes to respond effectively and efficiently to a crisis (such as a virus attack on IT systems associated with the Program);*
  - *d. Key Performance Indicators (KPIs) to enable objective assessment of whether the Program is achieving its objectives. These should be linked to Towards Zero, Victoria's Road Safety & Action Plan. Some of the KPIs could include:*
    - *community satisfaction of road safety measures;*
    - *camera availability;*
    - *camera achievement against maintenance plan;*
    - *infringements rejected for compliance reasons; and*
    - *the number of collisions or fatalities at key intersections with cameras.*

152 *My investigation has revealed that there are further opportunities for improvement within the Program, such as:*

- *the introduction of governance strategies that encourage and allow contractors to have a greater say and recognition of their ideas within regulatory and legislative boundaries;*
- *enhancing risk management capability Program-wide;*
- *formalising risk monitoring and reporting;*
- *scrutiny over reporting on the Program's performance to the Minister and the RSCC;*
- *incident identification and escalation;*

- *automating and streamlining processes;*
- *workforce capability;*
- *capital and procurement processes;*
- *better alignment the service of contractors, with the objectives of the Program through KPIs with financial penalties should these not be met; and*
- *consideration of whether IMES should continue to be the network operator.*

CULTURE

153 All stakeholders (e.g. DJR, VicPol, VicRoads, as well as third parties) involved with the FDRSCN should have a shared vision in the outcomes of the Program. This calls for greater communication, collaboration and cooperation. At present, the relationship between stakeholders is insular and fragmented. This is limiting the effective and efficient operations of the FDRSCN. In my view, effective risk management and critical incident management for events similar to the WannaCry virus incident is predicated on transparent, clear and timely communication and interaction between all stakeholders involved with the FDRSCN.

154 Cyber incidents such as this WannaCry virus incident are going to be an ongoing threat. It is therefore imperative the FDRSCN is equipped with the requisite prevention and detection tools, as well as the design and architecture, to respond effectively and efficiently to a critical incident. The design of any solutions by DJR to manage cyber incidents / crime needs to consider and align to the State Government's Cyber Security Strategy.

155 The Government has the opportunity to augment the operating model, governance structures, systems and processes for managing the FDRSCN to ensure its ongoing success and to maintain public confidence in the Program.

156 Contractors perceive (not unreasonably) that IMES /DJR are punitive towards any admissions of default or failure (whatever the cause). There is an opportunity to improve the speed and efficiency of dealing with any future issues which would be enhanced by admissions being recognised for their honesty and insight rather than solely for their breach. Governance strategies should support this continuous improvement objective.

Recommendations

157 *The current culture needs to be rapidly addressed to encourage more frank communication between IMES and contractors.*

IMPACT

158 I anticipated that the impact of the virus would be almost completely related to the older, "affected" systems over the 17 days of infection. In fact, the impact was felt over a significantly longer period.

159 Figures 5 – 11 that follow illustrate the operation of FDRSC systems using 18 months of data.

In this section the following terms are defined:

Deactivated	Period when a camera is inactive.
"Rejection" Downtime	Period when a camera is prevented from creating infringements due to, for example, maintenance.
Affected	System downtime *mostly* related to the virus attack.
Uptime	Period when a camera is available and functioning correctly.
Lanes	A camera may relate to multiple lanes. Some or all lanes may be inactive at various times. For example, a Lane's value of 100 on a weekly graph indicates that, during that week, the equivalent of 100 Lanes were inactive for a total of seven days.

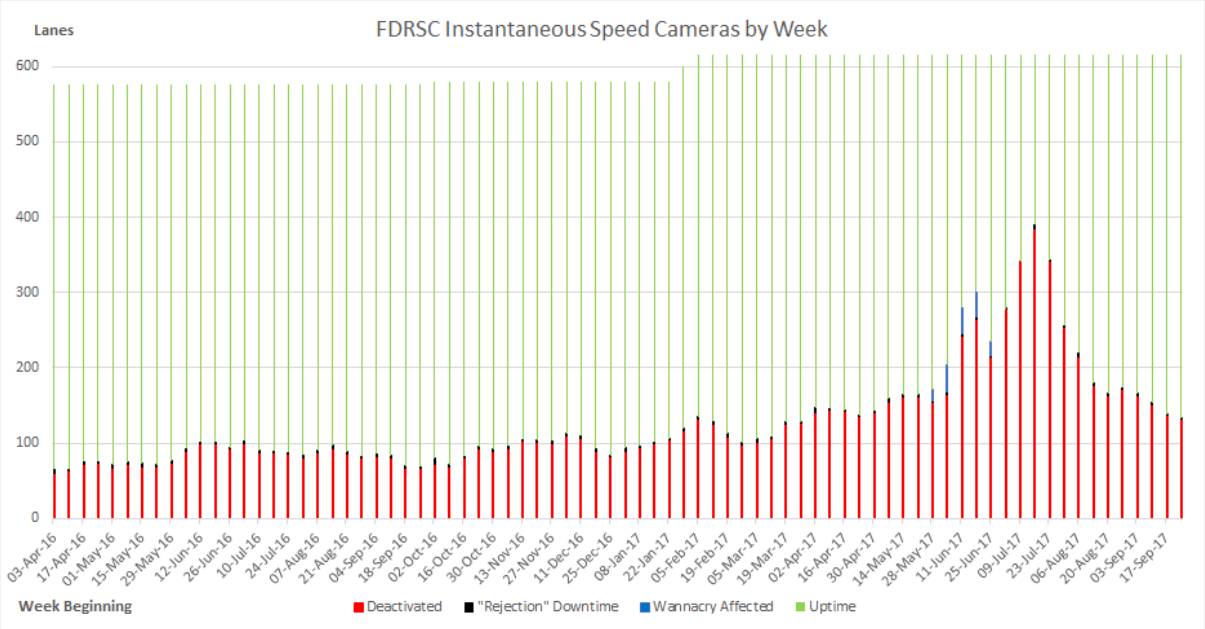

Figure 5

160 Figure 5 shows speed camera uptime and downtime on the FDRSC, by week from 3 April 2016 – 17 September 2017. Vendor 1 provided a breakdown, site-by-site, of downtime minutes experienced by their hardware in the first 28 days of June, 2017. Much, but not all of this downtime, relates to older, affected sites attacked by the virus. For the purpose of this exercise, in circumstances where the precise affected periods are uncertain, downtime for each site has been distributed evenly across the 28 days. If greater detail was available then I would expect higher downtime values in the period 8 June through 19 June. Deactivation periods and Rejection periods often overlap each other. These overlaps have been resolved so as not to "double-count" downtime values. In doing so, priority has been given to Deactivation periods. For example, maintenance time cannot further increase downtime on a system which is already deactivated. Similarly, affected downtime may not be added to a site which is, for example, reporting 100% Deactivation time; downtime on a system that is turned off is meaningless. It follows from the above, the WannaCry Affected values shown are more indicative rather than precise.

161 With the exception of the WannaCry Affected values, downtime data has been recorded with an accuracy granularity of one minute. Approximately 800,000 records cover every lane of every site for each camera type by every day over an 18 month period. It is likely there are some minor inaccuracies in the source data. For example, SiteTrak values are hand transcribed.

162 Figure 5 shows that deactivation downtime increased significantly *after* the period of infection. This was unexpected. A one month "freeze" in camera computer testing and certification resulted in sites' certification lapsing, and the sites classed as "Deactivated" as a result.

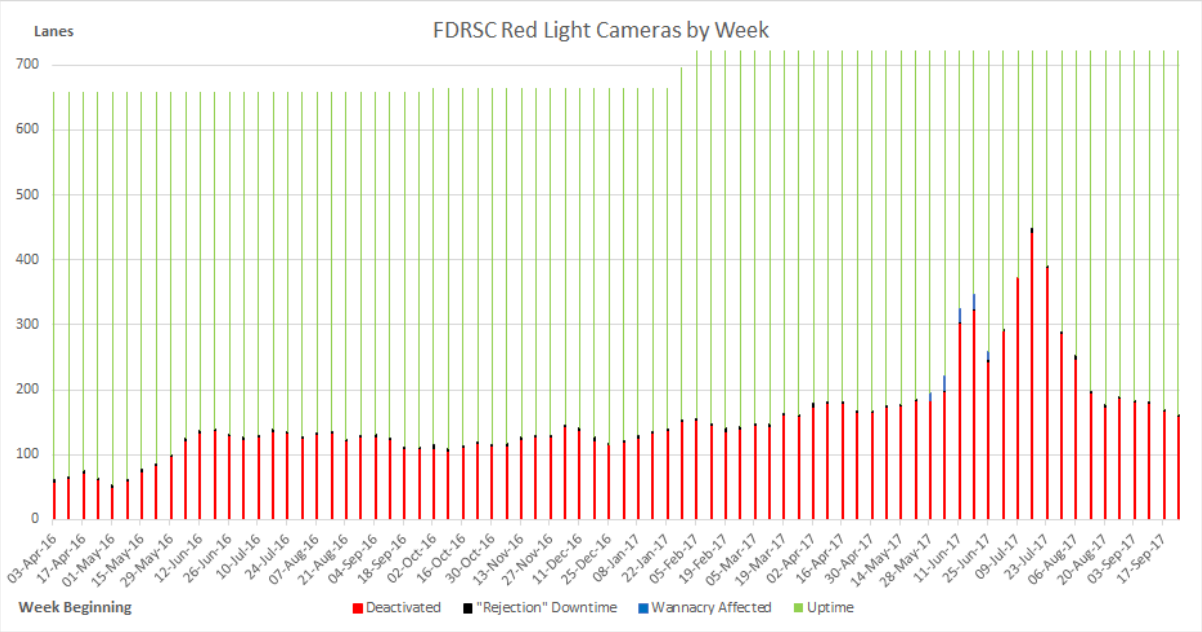

Figure 6

163 Figure 6 is a Red Light camera availability graph. It is similar to Figure 4. However, this is likely because in many instances the same cameras operate both Speed and Red Light detection systems.

164 The Affected values in Figure 6 are relatively muted. This is considered to be because:

- there are overall more Red Light cameras than Speed cameras; and
- more of the Affected systems were highway systems; in particular, Geelong Road, Hume Highway and Peninsula Link.

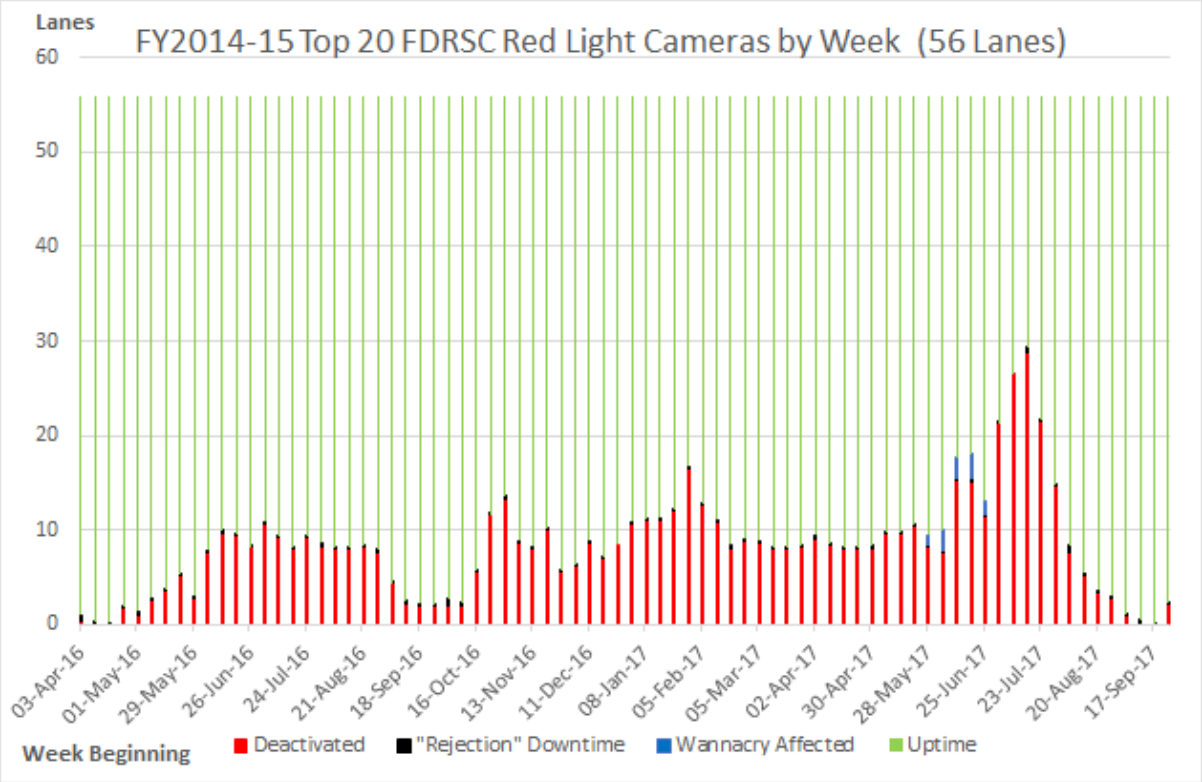

Figure 7-

This figure depicts the downtime activity during the period 27 March 2016 to 24 September 2017 of the top 20 fixed digital red light road safety cameras (of the 2014-15 financial year).

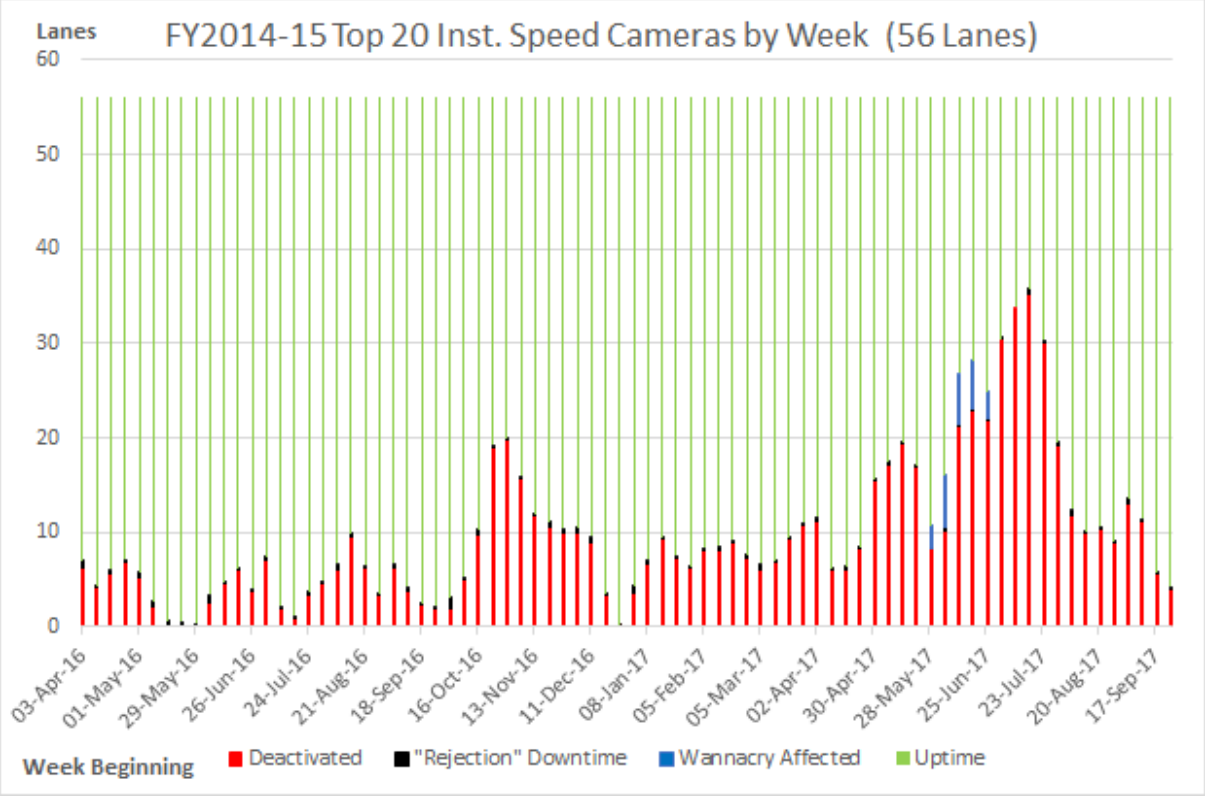

Figure 8

This figure depicts the downtime activity during the period 27 March 2016 to 24 September 2017 of the top 20 fixed digital instantaneous road safety cameras (of the 2014-15 financial year).

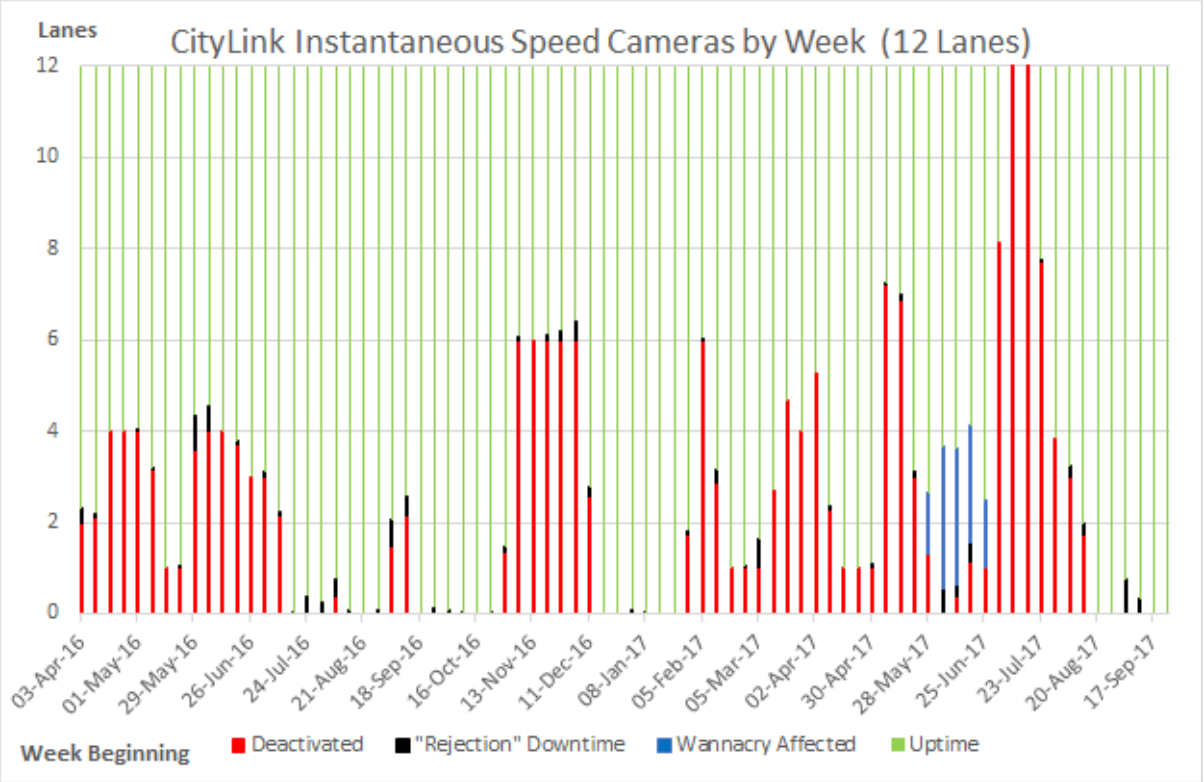

Figure 9

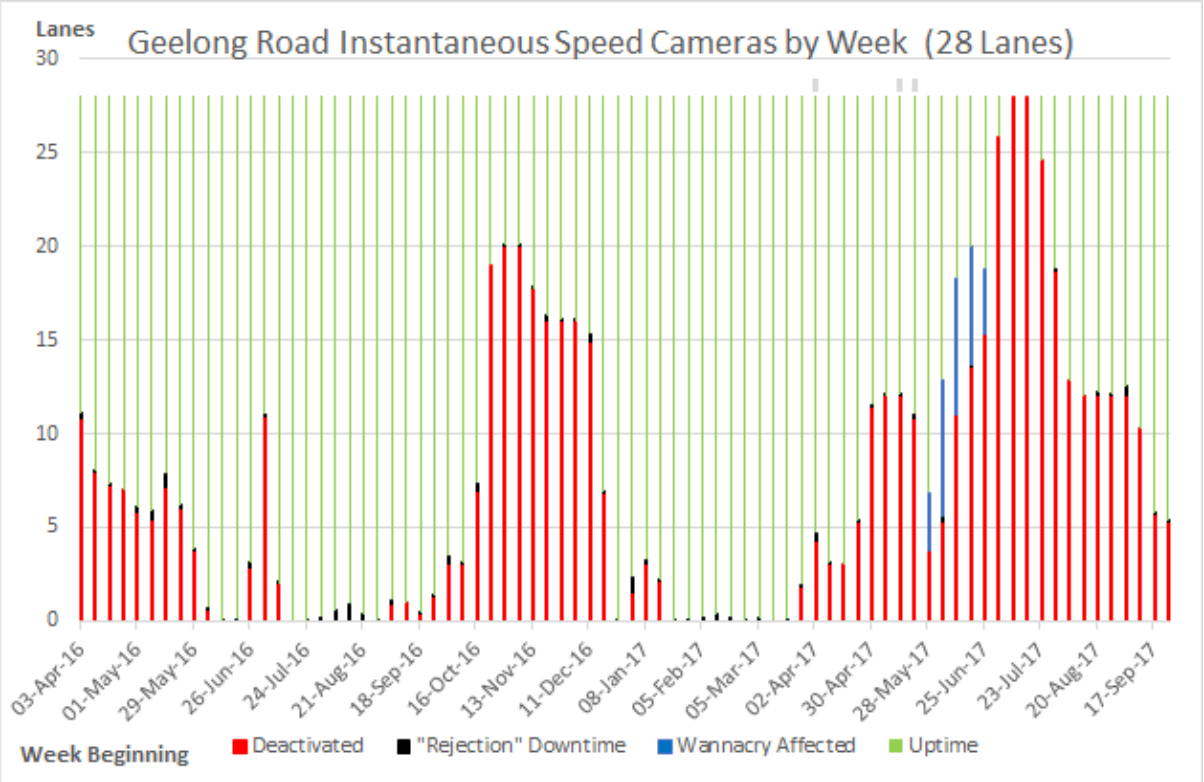

Figure 10

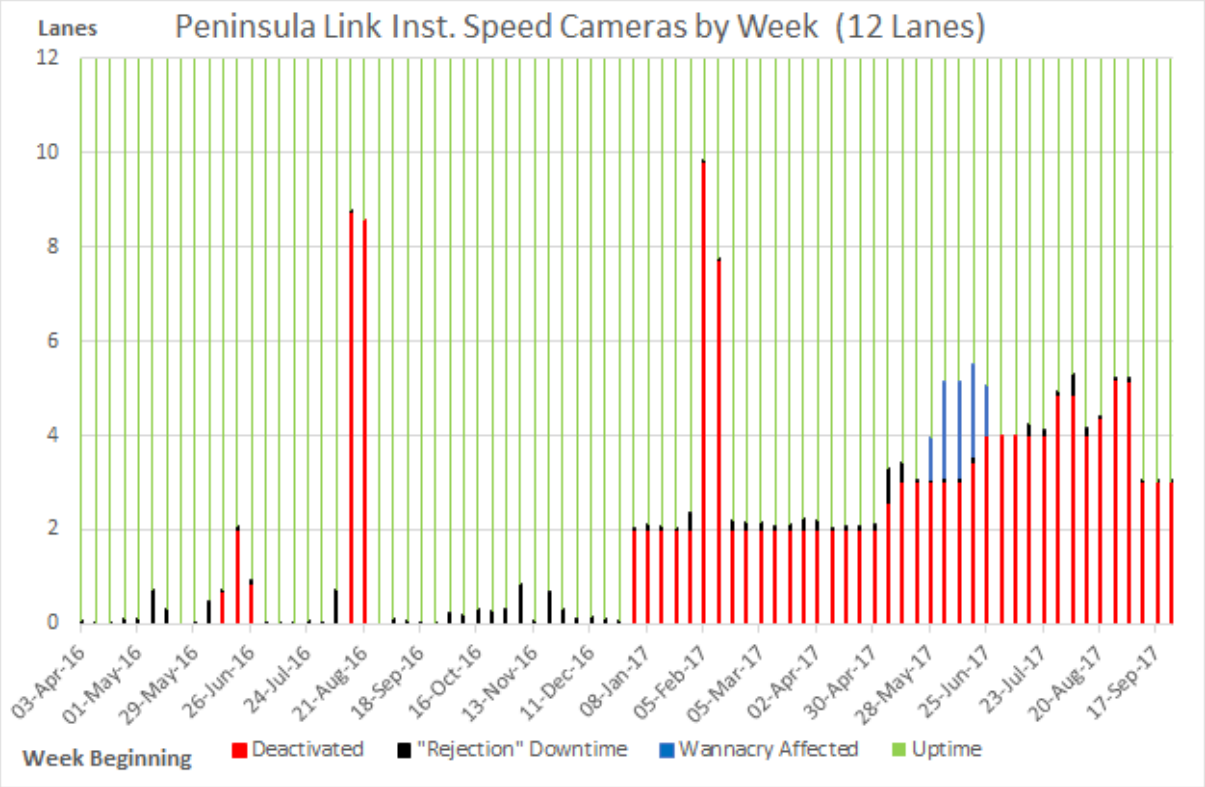

Figure 11

165 The camera downtime caused by the WannaCry virus infection had consequences for road safety and the Towards Zero program objectives. At its most basic this involved infringements that were not detected in the relevant period. Each infringement that was not detected means a reduction in the corrective impact of fines for breaches of road safety laws.

166 A more malignant virus could have caused a much greater reduction in infringements recorded. However, a more malignant virus would likely have been detected almost immediately. Curiously, the subject version of WannaCry resulted in an incident that was not as severe as it might have been, but also was not detected as quickly as might have been, but for the inept virus strain.

167 As at the end of December 2017 there was still incomplete recovery of the FDRSCN from the consequences of the processes involved in the virus. In particular, there was no testing or certification or maintenance between 28 June and 20 July 2017, which had a direct impact on camera uptime as well as detection of incidents. However, the flow-on effect on the testing re-scheduling process, which began on 21 July 2017, continued until at least January 2018.

THE ROAD SAFETY CAMERA COMMISSIONER

168 The office of the Road Safety Camera Commissioner was established by the *Road Safety Camera Commissioner Act 2011* with various functions and powers aimed at enhancing the Victorian public's confidence in the integrity of the road safety camera system. It goes without saying that transparency is essential to the integrity (including perceived integrity) of the fixed road safety camera network.

169 As will become apparent, this investigation has led me to conclude that the powers of investigation of the RSCC need to be clarified.

Findings

170 My powers were inadequate to ensure timely and complete cooperation with my enquiring by both Government and non-Government bodies.

Recommendations

171 *The powers of the RSCC should include the power to compel prompt co-operation from within the Victorian public sector.*

172 *There should be a legislative indemnity for the holder of the office of Road Safety Camera Commissioner in relation to the discharge of its functions.*

CONCLUSIONS

173 My investigation has confirmed that the variant of the virus that infected the FDRSC:

- was incapable of encrypting data. It follows that the performance impact on infected machines was negligible;
- was incapable of infecting machines running older versions of MS Windows (XP & 2000). Such “affected” systems failed (crashed) within minutes of coming under attack;
- was incapable, without human intervention, of propagation via portable USB devices;
- often attacked IP addresses in a sequential fashion;
- spread very quickly when ‘nearby’ IP addresses were detected.

174 I have found no evidence of any malicious intent.

175 I have been unable to conclusively establish the source of the infection. It is plausible that any of a number of sites were the original source of the infection.

176 FDRSC network security relies totally on the professionalism of nine bodies (plus Telstra) external to IMES. While this reliance has proved effective until quite recently, I cannot recommend that such a (non-)system continues.

177 That some vendors and testers have “remote” access to the FDRSC while others do not (i.e. are “air-gapped”) makes no sense. A more modern and defensible network design is required.

178 The FDRSC system requires specialist network redesign. I have not seen evidence that IMES has such capability.

179 In the event of another virus infection, some basic steps need to be undertaken.

180 Consideration should be given to whether or not detection system computers should be continuously patched and upgraded against known malware exploits.

181 In particular in relation to IMES, I have concluded:

a. that there was insufficient attention to prevention strategies;

b. that once a site computer became infected, there was gratuitous spread of the infection;

c. that there was no adequate incident response plan, including levels of escalation / who should be contacted, how to contact key people and service providers; apparently no checklist of processes to follow, or functions to be performed, of notification to staff stakeholders and the public;

d. that there is no evidence of any network security assessment or testing on business critical systems, which could have identified, weighted, and remediated any vulnerabilities;

e. that there was a limited recognition or awareness of the risks, understanding of the risks, assessment of the risks;

f. that there was limited clarity of stated roles and responsibilities, and of education and training;

g. that there was an apparent absence of a plan to identify and prioritise opportunities for improvement;

h. that there was limited communication to stakeholders of the cyber-security risk, steps taken, plans in place, involvement by stakeholders;

i. that the risk mitigation strategy of the FDRSC system appears to have been piecemeal and without an owner.

ANNEXURE A - Minister for Police – Investigation - Terms of Reference

Dear Commissioner,

I am writing to amend my referral of 22/6/2017. On the evening of 23/6/2017 I was made aware of further instances of Victoria's Road Safety Cameras being infected with a virus which has inhibited their operation from 6/6/2017.

In order to ensure all potential issues with the cameras are considered in your investigation, please find amended terms below:

To ensure the public can be confident in the Road Safety Camera System, I ask that you investigate:

- which cameras across the Victorian Road Safety Camera System have been infected with a virus, and how the cameras came to be infected;
- whether there have been any infringements issued across the Victorian Road Safety Camera Network from 6/6/2017 that could be inaccurate as a result of the virus that should be withdrawn;
- whether any damage may have been caused to the data held by any of the Victorian Road Safety Cameras as a result of the virus;
- whether there has been any impact on the accuracy or reliability of the Victorian Road Safety Camera System;
- whether there may be any future impact on the accuracy or reliability of the cameras as a result of the infection;
- whether additional security measures need to be employed in order to protect the Road Safety Camera System in future.

I ask that you investigate these matters in relation to all 280 fixed cameras that operate across the Victorian Road Safety Camera Network.

In addition I ask for your advice on the adequacy of the management and oversight of the road safety camera Program. This work will encompass the management and performance of providers contracted to deliver and maintain the Program but also the governance and internal accountabilities within the Department of Justice and Regulation.

I would appreciate your report at the earliest possible date.

ANNEXURE B - Initial list of infected road safety cameras from IMES

This table was contained in an email dated 23 June 2017 at 12:01:09 pm from Strategic Information Services from IMES and was intended to be identifying 55 infections. This list was published on the Cameras save lives website www.camerassavelives.vic.gov.au

Of note: possible “Ground zero” sites including:

- A13 corner Gordon & Barkly Streets Footscray,
- A12 Elizabeth & LaTrobe Streets Melbourne, and
- the string of cameras on the Hume which had drawn attention to the infection,

were not listed:

Camera Location	At Intersection	Suburb	Site*
Alexandra Parade	Smith Street	Fitzroy North	Kerbside
St Kilda Road	Union Street	Melbourne	Kerbside
Canterbury Road	Bayswater Road	Bayswater North	Kerbside
Canterbury Road	Bayswater Road	Bayswater North	Median strip
Peel Street	Victoria Street	West Melbourne	Median strip
Whitehorse Road	Surrey Road	Blackburn	Kerbside
Blackburn Road	Burwood Highway	Burwood East	Median strip
Bell Street	Plenty Road	Preston	Kerbside
Bell Street	Plenty Road	Preston	Median strip
Ashley Street	Churchill Avenue	Maidstone	Kerbside
St Kilda Road	Fitzroy Street	St Kilda	Kerbside
St Kilda Road	Fitzroy Street	St Kilda	Median strip
Dandenong Road	Chapel Street	St Kilda	Kerbside
Dandenong Road	Chapel Street	St Kilda	Median strip
Princes Highway	Huntingdale Road	Oakleigh East	Median strip
Nepean Highway	Bungower Road	Mornington	Median strip
Nepean Highway	Main Street	Mornington	Median strip
South Gippsland Highway	Lynbrook Boulevard	Lynbrook	Median strip
Hoddle Street	Wellington Parade	East Melbourne	Median strip
Nicholson Street	Princes Street	Carlton	Kerbside
South Gippsland Highway	Thompsons Road	Cranbourne North	Kerbside
South Gippsland Highway	Thompsons Road	Cranbourne North	Median strip
Denmark Street	High Street South	Kew	Kerbside
Sturt Street	Gillies Street	Lake Gardens	Kerbside
Fifteenth Street	San Mateo Avenue	Mildura	Kerbside
Raglan Parade	Mahoneys Road	Warrnambool	Kerbside
Dandenong Road	Warrigal Road	Malvern East	Median strip
Burwood Highway	Springvale Road	Vermont South	Kerbside
Burwood Highway	Springvale Road	Vermont South	Median strip
Princes Highway	Elonera Road	Noble Park North	Kerbside
Kings Road	Melton Highway	Taylors Lakes	Kerbside
Williamsons Road	Doncaster Road	Doncaster	Kerbside
Williamsons Road	Doncaster Road	Doncaster	Median strip
City Road	Montague Street	South Melbourne	Median strip
Mahoneys Road	High Street	Thomastown	Kerbside
Mahoneys Road	High Street	Thomastown	Median strip
Prospect Hill Road	Burke Road	Camberwell	Kerbside
Dandenong Road	Clayton Road	Oakleigh East	Median strip
Springvale Road	Wellington Road	Mulgrave	Kerbside
Springvale Road	Wellington Road	Mulgrave	Median strip
Princes Highway	Gladstone Road	Dandenong	Kerbside
Princes Highway	Gladstone Road	Dandenong	Median strip
Highbury Road	Huntingdale Road	Mount Waverley	Kerbside
Burwood Highway	Stud Road	Wantirna South	Median strip
Alexandra Parade	Brunswick Street	Fitzroy	Kerbside
Alexandra Parade	Brunswick Street	Fitzroy	Kerbside
St Georges Road	Normanby Avenue	Thornbury	Kerbside
Princes Highway	South Gippsland Freeway	Eumemmerring	Median strip
Sydney Road	Mahoneys Road	Campbellfield	Kerbside
Sydney Road	Mahoneys Road	Campbellfield	Median strip
Midland Highway	Level Crossing	Bagshot	Rail crossing westbound traffic
Midland Highway	Level Crossing	Bagshot	Rail crossing eastbound traffic
Loddon Valley Highway	Calder Highway	Ironbark	Kerbside
Royal Parade	Gatehouse Street	Parkville	Median strip
Monash Freeway, approximately 290 metres South of High St		Glen Iris	Kerbside northbound traffic

*Refers to where the camera is situated at the location

ANNEXURE C - Media

AM Radio (1 item)

Mitchell says they broke the news on yesterday's program that the...

- 23 Jun 2017 8:39AM
- AM Radio: 3AW, Melbourne, Mornings, Neil Mitchell

Mitchell says they broke the news on yesterday's program that the speed camera system has potentially been compromised. He says what's happened since is unfair, absurd and sloppy and makes a mockery of the cameras. He says the most important thing about the camera system is integrity. He says they broke the news that a ransomware virus had infected 55 cameras. He says someone tried to deal with the virus quietly rather than telling the Minister and the public. He says Brendan Facey, Sheriff of Victoria claimed yesterday that it only involved metropolitan city cameras but the Dept of Justice says it affects highway cameras as well. He says he's told the problem first emerged on the 8th June but the official version is that it emerged a week ago. He says John Voyage, Road Safety Camera Commissioner wasn't made aware of the problem until yesterday and he's now investigating. He says the Sheriff stated that tickets would be withheld until the inquiry is finished but the message from the government and police is that tickets will be issued and withdrawn if the commissioner finds a problem with the cameras.

- ASR: AUD 6,782
- Country: Australia
- State: VIC
- Duration: 3 mins 20 secs
- Size: 3 mins 20 secs cm²

- Audience:
163,000 All ; 71,000 Male 16+ ; 92,000 Female 16+
- Item ID: M00070826361

Heidi Murphy (@heidimur)

24/6/17, 13:33
The camera-virus-crisis, first revealed by @3AWNeilMitchell worsens.. Details in a presser at 3; but hearing more cameras are infected..

Lisa Neville (@LisanevilleMP)

24/6/17, 16:58
@heidimur @3AWNeilMitchell thanks to Neil for raising it first. Unfortunately Dept failed to. @3AWNeilMitchell led to action

ANNEXURE D - IMES' list of infected Road Safety Cameras

(Provided to RSCC on 02 February 2018)

SPEED AND RED LIGHT CAMERAS							
Site		Vendor 1		**Camera Location**	**At Intersection**	**Suburb**	**Site count**
A00				Alexandra Parade	Smith Street	Fitzroy North	1
A02				Terminal Drive	Centre Road	Melbourne Airport	1
A06K				Boronia Road	Wantirna Road	Wantirna	1
A06M				Boronia Road	Wantirna Road	Wantirna	
A07				Duke Street	Ballarat Road	Braybrook	1
A09				Lonsdale Street	Webster Street	Dandenong	1
A11K				St Kilda Road	Union Street	Melbourne	1
A11M				St Kilda Road	Union Street	Melbourne	
A12				Elizabeth Street	La Trobe Street	Melbourne	1
A13				Gordon Street	Barkly Street	Footscray	1
A16				Princes Highway	Webb Street	Narre Warren	1
A17K				Dandenong Road	Orrong Road	Caulfield North	1
A17M				Dandenong Road	Orrong Road	Caulfield North	
A18				Sussex Street	O'Hea Street	Pascoe Vale South	1
A21				Whitehorse Road	Burke Road	Balwyn	1
A22				Glenferrie Road	Burwood Road	Hawthorn	1
A23				Park Road	Charman Road	Cheltenham	1
A25				Elizabeth Street	Victoria Street	Melbourne	1
B01				King Street	Hawke Street	West Melbourne	1
B02				Flemington Road	Gatehouse Street	Parkville	1
B10				Whitehorse Road	Elgar Road	Box Hill	1
B12K				Canterbury Road	Bayswater Road	Bayswater North	1
B12M				Canterbury Road	Bayswater Road	Bayswater North	
B14				Hotham Street	Balaclava Road	St Kilda East	1
B17K				Springvale Road	High Street Road	Glen Waverley	1
B17M				Springvale Road	High Street Road	Glen Waverley	
B20				Thomas Street	North Road	Brighton East	1
B23				Union Road	Mont Albert Road	Surrey Hills	1
B24				Hawthorn Road	Inkerman Road	Caulfield North	1
B25				Burwood Highway	Brenock Park Drive	Ferntree Gully	1
B26				Mt Dandenong Road	Dorset Road	Croydon	1
C01K				William Street	Flinders Street	Melbourne	1
C01M				William Street	Flinders Street	Melbourne	
C02K				Hoddle Street	Victoria Street	Abbotsford	1
C02M				Hoddle Street	Victoria Street	Abbotsford	
C03				Flinders Street	William Street	Melbourne	1
C04K				Hoddle Street	Victoria Parade	East Melbourne	1
C04M				Hoddle Street	Victoria Parade	East Melbourne	
C05K				Victoria Parade	Nicholson Street	Carlton	1
C05M				Victoria Parade	Nicholson Street	Carlton	
C06				Alexandra Avenue	Church Street	South Yarra	1
C07				Barry Road	King Street	Dallas	1
C08				Nicholson Street	Victoria Parade	East Melbourne	1
C09				Station Street	Thames Street	Box Hill	1
C10				Peel Street	Victoria Street	West Melbourne	1
C13				Nicholson Street	Albert Street	East Melbourne	1
C14				Kings Way	Park Street	South Melbourne	1

C15		Vendor 1		Whitehorse Road	Surrey Road	Blackburn	1
C16K				Nepean Highway	Karen Street	Highett	1
C16M				Nepean Highway	Karen Street	Highett	
C17				Blackburn Road	Burwood Highway	Burwood East	1
C19K				Nepean Highway	Warrigal Road	Mentone	1
C19M				Nepean Highway	Warrigal Road	Mentone	
C20				St Georges Road	Arthurton Road	Northcote	1
C21				LaTrobe Street	Spencer Street	West Melbourne	1
C23				High Street Road	Stud Road	Wantirna South	1
C24K				Bell Street	Plenty Road	Preston	1
C24M				Bell Street	Plenty Road	Preston	
C25				Victoria St	Swanston St	Carlton	1
C26K				Princes Highway	Belgrave Road	Malvern East	1
C26M				Princes Highway	Belgrave Road	Malvern East	
C32				Ringwood Street	Maroondah Highway	Ringwood	1
C34				Princes Street	Rathdowne Street	Carlton	1
C35				Ashley Street	Churchill Avenue	Maidstone	1
D02K				St Kilda Road	Fitzroy Street	St Kilda	1
D02M				St Kilda Road	Fitzroy Street	St Kilda	
D03K				Dandenong Road	Chapel Street	St Kilda	1
D03M				Dandenong Road	Chapel Street	St Kilda	
D04K				Hume Highway	Somerton Road	Campbellfield	1
D04M				Hume Highway	Somerton Road	Campbellfield	
D05				Princes Highway	Huntingdale Road	Oakleigh East	1
D08K				Stud Road	Wellington Road	Rowville	1
D08M				Stud Road	Wellington Road	Rowville	
D09				Nepean Highway	Bungower Road	Mornington	1
D10				Nepean Highway	Main Street	Mornington	1
D11				South Gippsland Highway	Lynbrook Boulevard	Lynbrook	1
D12K				Hoddle Street	Wellington Parade	East Melbourne	1
D12M				Hoddle Street	Wellington Parade	East Melbourne	
D13				Nicholson Street	Princes Street	Carlton	1
D14K				South Gippsland Highway	Thompsons Road	Cranbourne North	1
D14M				South Gippsland Highway	Thompsons Road	Cranbourne North	
D15				Denmark Street	High Street South	Kew	1
D18				Sturt Street	Gillies Street	Lake Gardens	1
D20				Fifteenth Street	San Mateo Avenue	Mildura	1
D21				Raglan Parade	Mahoneys Road	Warrnambool	1
D23K				Nepean Highway	Davey Street	Frankston	1
D23M				Nepean Highway	Davey Street	Frankston	
D24K				Dandenong Road	Warrigal Road	Malvern East	1
D24M				Dandenong Road	Warrigal Road	Malvern East	
D25K				Burwood Highway	Springvale Road	Vermont South	1
D25M				Burwood Highway	Springvale Road	Vermont South	
D27				Canterbury Road	Colchester Road	Kilsyth South	1
D30				Princes Highway	Elonera Road	Noble Park North	1
D32				Kings Road	Melton Highway	Taylors Lakes	1
D33				Centre Road	Huntingdale Road	Oakleigh South	1
D34K				Williamsons Road	Doncaster Road	Doncaster	1
D34M				Williamsons Road	Doncaster Road	Doncaster	

D35		Vendor 1		City Road	Montague Street	South Melbourne	1
D37				Hall Road	Dandenong-Frankston Road	Carrum Downs	1
D38				Pascoe Vale Road	Reservoir Drive	Coolaroo	1
D39K				Mahoneys Road	High Street	Thomastown	1
D39M				Mahoneys Road	High Street	Thomastown	
D49				King Street	Latrobe Street	Melbourne	1
F01				Prospect Hill Road	Burke Road	Camberwell	1
F13				Punt Road	High Street	Prahran	1
F14				Dandenong Road	Clayton Road	Oakleigh East	1
F28				Denmark Street	Barkers Road	Kew	1
F31				Princes Highway	Pioneer Road	Grovedale	1
F33K				Springvale Road	Wellington Road	Mulgrave	1
F33M				Springvale Road	Wellington Road	Mulgrave	
F36K				Dorset Road	Canterbury Road	Bayswater North	1
F36M				Dorset Road	Canterbury Road	Bayswater North	
F37K				Princes Highway	Gladstone Road	Dandenong	1
F37M				Princes Highway	Gladstone Road	Dandenong	
F38				Highbury Road	Huntingdale Road	Mount Waverley	1
F39K				Burwood Highway	Stud Road	Wantirna South	1
F39M				Burwood Highway	Stud Road	Wantirna South	
F40				Stud Road	Heatherton Road	Dandenong	1
F41K				Alexandra Parade	Brunswick Street	Fitzroy	1
F41M				Alexandra Parade	Brunswick Street	Fitzroy	
F42				Ballarat Road	Ashley Street	Maidstone	1
F43				St Georges Road	Normanby Avenue	Thornbury	1
F46				Seymour Grove	Camberwell Road	Camberwell	1
F49				Princes Highway	South Gippsland Freeway	Eumemmerring	1
F51				Scoresby Road	Mountain Highway	Bayswater	1
F53K				Sydney Road	Mahoneys Road	Campbellfield	1
F53M				Sydney Road	Mahoneys Road	Campbellfield	
X01E				Midland Highway	Level Crossing	Bagshot	1
X01W				Midland Highway	Level Crossing	Bagshot	
							98
A03		Vendor 2		Alexandra Parade	George Street	Fitzroy North	1
A28				Harp Road	Burke Road	Kew East	1
A37				Somerville Road	Geelong Road	Yarraville	1
A39				Centre Road	Springs Road	Clayton South	1
A41				Middleborough Road	Eastern Freeway	Box Hill North	1
A42				Elgar Road	Arnold Street	Box Hill	1
A45				Glen Eira Road	Kooyong Road	Caulfield	1
A46				Gladstone Road	Heatherton Road	Dandenong North	1
A47				Heatherton Road	Corrigan Road	Noble Park	1
A49				High Street	Summerhill Road	Glen Iris	1
A50				Johnston Street	Wellington Street	Collingwood	1
A51				Manningham Road	Macedon Road	Templestowe Lower	1
A55				The Boulevard	Melbourne Road	Norlane	1
A56				Mont Albert Road	Union Road	Surrey Hills	1
A57				Mountain Highway	Wantirna Road	Wantirna	1
A59				Ogilvie Avenue	High Street	Echuca	1
A60K1				Dandenong Road	Kooyong Road	Armadale	1

A60K2		Vendor 2		Dandenong Road	Kooyong Road	Armadale	
A66				Shannon Avenue	Noble Street	Newtown	1
A75				Burke Rd	Old Burke Road	Kew East	1
A76				Toorak Road	Glen Iris Road	Camberwell	1
A81				Loddon Valley Highway	Calder Highway	Ironbark	1
A83				Centre Road	Buckland Street	Clayton	1
A84				Lightwood Road	Corrigan Road	Noble Park	1
A85				Doncaster Road	Gardenia Road	Balwyn North	1
A86K				Stud Road	Ferntree Gully Road	Scoresby	1
A86M				Stud Road	Ferntree Gully Road	Scoresby	
A89				High Street	Verene Avenue	Templestowe Lower	1
A91K				Sydney Road	Barry Road	Campbellfield	1
A91M				Sydney Road	Barry Road	Campbellfield	
A92				Latrobe Terrace	Fyans Street	South Geelong	1
B22				Alma Road	Chapel Street	St Kilda	1
D16				Hallam Road	Fordholm Road	Hampton Park	1
D17				Princes Highway	Fitzgerald Road	Hallam	1
D19				Lincoln Causeway	Hume Highway Ramp	Wodonga	1
D22				York Street	MacArthur Street	Sale	1
D26E				Heatherton Road	Monash Freeway	Endeavour Hills	1
D26W				Heatherton Road	Monash Freeway	Doveton	1
D28				Swan Street	Batman Avenue	Melbourne	1
D29				Exhibition Street	Victoria Street	Melbourne	1
D31				Gaffney Street	Sydney Road	Coburg	1
D36SE				Frankston Freeway Off Ramp	Dandenong-Frankston Road	Seaford	1
D36SW				Dandenong-Frankston Road	Skye Road	Frankston	1
D40				Macaulay Road	Stubbs Street	Kensington	1
D41				Wells Road	Palm Grove Boulevard	Aspendale Gardens	1
D42				Wells Road	Nurten Parade	Aspendale Gardens	1
D43N				Greensborough Highway	Grimshaw Street	Watsonia	1
D43S				Greensborough Highway	Grimshaw Street	Greensborough	1
F04				Canterbury Road	Station Street	Box Hill	1
F09				Centre Road	Warrigal Road	Bentleigh East	1
F17				Grimshaw Street	Macorna Street	Watsonia North	1
F22				Geelong Street	Geelong Road	Kingsville	1
F25				Barkly Street	Carlisle Street	St Kilda	1
F27				Warrigal Road	Centre Dandenong Road	Cheltenham	1
F32M1				Royal Parade	Gatehouse Street	Parkville	1
F32M2				Royal Parade	Gatehouse Street	Parkville	
F34				Gilbert Road	Bell Street	Preston	1
F35				Punt Road	Toorak Road	South Yarra	1
F44				Nepean Highway	Highett Rd	Highett	1
F45				Waverley Road	Blackburn Road	Mount Waverley	1
F47				High Street	Don Street	Bendigo	1
F48				Princes Highway	Sparks Road	Norlane	1
F52				High Street Road	Huntingdale Road	Mount Waverley	1
P01E				Maroondah Highway	Approx. 100 metres West of Hutchinson Street	Lilydale	1
P01W				Maroondah Highway	Approx. 100 metres West of Hutchinson Street	Lilydale	
							60
D01		Vendor 3		Wyndham Street	High Street	Shepparton	1

D06M1		Vendor 3		St Kilda Road	Kings Way	Melbourne	1
D06M2				St Kilda Road	Kings Way	Melbourne	
D07				Punt Road	Commercial Road	Melbourne	1
D44K				Springvale Road	Canterbury Road	Forest Hill	1
D44M				Springvale Road	Canterbury Road	Forest Hill	
D45N				Narre Warren North Road	Ernst Wanke Road	Narre Warren	1
D45S				Narre Warren North Road	Ernst Wanke Road	Narre Warren North	1
D46NK				Maroondah Highway	Ringwood Bypass	Ringwood	1
D46NM				Maroondah Highway	Ringwood Bypass	Ringwood	
D46SK				Maroondah Highway	Mount Dandenong Road	Ringwood	1
D46SM				Maroondah Highway	Mount Dandenong Road	Ringwood	
D47N				Plenty Road	Dunne Street	Kingsbury	1
D47S				Plenty Road	Kingsbury Drive	Bundoora	1
D48K				Canterbury Road	Mitcham Road	Vermont	1
D48M				Canterbury Road	Mitcham Road	Vermont	
F02K				Maroondah Highway	Springvale Road	Nunawading	1
F02M				Maroondah Highway	Springvale Road	Nunawading	
F03K				Cemetery Road West	Royal Parade	Parkville	1
F03M				Cemetery Road West	Royal Parade	Parkville	
F05				Bell Street	St Georges Road	Preston	1
F06K				Warrigal Road	North Road	Oakleigh	1
F06M				Warrigal Road	North Road	Oakleigh	
F07				Albert Street	Gower Street	Preston	1
F08				Williamstown Road	Somerville Road	Yarraville	1
F10				Ballarat Road	Churchill Avenue	Maidstone	1
F11				Spencer Street	Dudley Street	West Melbourne	1
F12K				Hoddle Street	Johnston Street	Collingwood	1
F12M				Hoddle Street	Johnston Street	Collingwood	
F15K				Springvale Road	Lower Dandenong Road	Braeside	1
F15M				Springvale Road	Lower Dandenong Road	Braeside	
F16				Maribyrnong Road	Mt Alexander Road	Moonee Ponds	1
F18				Foster Street	McCrae Street	Dandenong	1
F19				Geelong Road	Droop Street	Footscray	1
F20				Munro Street	Sydney Road	Coburg	1
F21				Blackshaws Road	Millers Road	Altona North	1
F23				Fitzroy Street	Lakeside Drive	St Kilda	1
F24				Victoria Street	Doncaster Road	Doncaster	1
F26				Warrigal Road	Batesford Road	Chadstone	1
F29				Nicholson Street	Elgin Street	Carlton	1
F30				Epsom Road	Smithfield Road	Kensington	1
F54M1				Brighton Road	Glen Eira Road	Ripponlea	1
F54M2				Brighton Road	Glen Eira Road	Ripponlea	
F55K				North Road	Clayton Road	Oakleigh East	1
F55M				North Road	Clayton Road	Oakleigh East	
F56K				Nepean Highway	Centre Road	Brighton East	1
F56M				Nepean Highway	Centre Road	Brighton East	
F57				Barkers Road	Glenferrie Road	Hawthorn	1
F58				Murray Road	Elizabeth Street	Coburg	1
F59				Pascoe Vale Road	Peck Avenue	Strathmore	1
F60				Thompson Road	Separation Street	Bell Park	1

F61		Vendor 3		Princes Highway	Station Street	Corio	1
F62				Settlement Road	Torquay Road	Belmont	1
F63				Moorabool Street	Fyans Street	South Geelong	1
F64E				Francis Street	Wembley Avenue	Yarraville	1
F64W				Francis Street	Wembley Avenue	Yarraville	1
F65				McIvor Road	Reservoir Road	Strathdale	1
AR062				Royal Parade	Cemetery Road	North Carlton	1
AR150				Johnston Street	Hoddle Street	Collingwood	1
BR025				Fitzroy Street	Princes Street	St Kilda	1
JR022				Blackshaws Road	Millers Road	North Altona	1
							48
SRL TOTAL							**206**

HIGHWAY CAMERA SYSTEMS					
System	**Site No.**		Vendor 1	**Camera Location**	**Site count**
Geelong Road	GA			Westgate Fwy, Geelong Bound, Millers Rd Gantry	1
Geelong Road	GB			Princes Fwy, Geelong Bound, Forsyth Rd overpass	1
Geelong Road	GC			Princes Fwy, Geelong Bound, Pt Wilson Rd overpass	1
Geelong Road	GD			Princes Fwy, Geelong Bound, Avalon Rd overpass	1
Geelong Road	GE			Princes Fwy, Melbourne Bound, Pt Wilson Rd overpass	1
Geelong Road	GF			Princes Fwy, Melbourne Bound, Avalon Rd overpass	1
Geelong Road	GG			Princes Fwy, Melbourne Bound, Forsyth Rd overpass	1
Geelong Road	GH			Westgate Fwy, Melbourne Bound, Grieve Pde overpass	1
CityLink	CBA			Burnley Tunnel, Southbank, approximately 430 metres after the eastbound entrance	1
CityLink	CBC			Burnley Tunnel, Cremorne, approximately 2140 metres after the tunnel entrance.	1
CityLink	CDA			Domain Tunnel, Melbourne, approximately 725 metres after the tunnel entrance.	1
CityLink	CDB			Domain Tunnel, Southbank, approximately 1195 metres after the westbound entrance	1
Hume Highway	H18N			O'Herns Road, Epping	1
Hume Highway	H26N			Amaroo Rd, Craigieburn	1
Hume Highway	H40N			Mount Fraser, Beveridge	1
Hume Highway	H47N			Station St, Wallan East	1
Hume Highway	H72N			Broadford-Flowerdale Rd, Broadford	1
Hume Highway	H72S			Broadford-Flowerdale Rd, Broadford	1
Hume Highway	H47S			Station St, Wallan East	1
Hume Highway	H40S			Mount Fraser, Beveridge	1
Hume Highway	H26S			Amaroo Rd, Craigieburn	1
Hume Highway	H18S			OHerns Rd, Epping	1
Peninsula Link	PL17N			Skye Road, Frankston	1
Peninsula Link	PL27N			Eramosa Road, Moorooduc	1
Peninsula Link	PL33N			Loders Road, Moorooduc	1
Peninsula Link	PL17S			Skye Road, Frankston	1
Peninsula Link	PL27S			Eramosa Road, Moorooduc	1
Peninsula Link	PL31S			Mornington-Tyabb Road, Moorooduc	1
					28
Monash Freeway	M11NA		Vendor 2	Approximately 290 metres South of High Street, Glen Iris	1
Monash Freeway	M11NB			Approximately 290 metres South of High Street, Glen Iris	
Monash Freeway	M11SA			Approximately 470 metres South of High Street, Glen Iris	1
Monash Freeway	M11SB			Approximately 470 metres South of High Street, Glen Iris	
					2
Western Ring Rd	WA		Vendor 3	Glenroy, Westbound, approximately 600 metres West of Sydney Road	1
Western Ring Rd	WBA			Keilor Park, Southbound, Fullarton Road Bridge	1
Western Ring Rd	WBB			Keilor Park, Southbound, Fullarton Road Bridge	
Western Ring Rd	WC			Ardeer, Southbound, approximately 560 metres North of Ballarat Road	1
Western Ring Rd	WD			Southbound, Boundary Road North Side Gantry	1
Western Ring Rd	WE			Broadmeadows, Eastbound, approximately 1600 metres West of Sydney Road	1
Western Ring Rd	WF			Keilor East, Northbound, Keilor Park Drive Bridge	1
Western Ring Rd	WG			Deer Park, Northbound, approximately 650 metres South of Ballarat Road	1
Western Ring Rd	WH			Laverton North, Northbound, Boundary Road South Side Gantry	1
Eastlink	EA			Mullum Mullum Tunnel, Donvale, approx. 600m prior to Tunnel Exit	1
Eastlink	EB			Rowville, Southbound, Wellington Road Bridge	1
Eastlink	EC			Keysborough, Southbound, Dandenong Bypass Bridge	1
Eastlink	EF			Melba Tunnel, Donvale, approx. 500m prior to Tunnel Exit	1
Eastlink	EG			Rowville, Northbound, Wellington Road Bridge	1
Eastlink	EH			Keysborough, Northbound, Dandenong Bypass Bridge	1
					14
TOTAL					**44**

ANNEXURE E – (Tester 1) letter to IMES – undated

Infringement Management and Enforcement Services
Level 22, 80 Collins Street,
Melbourne VIC 3000

Re: Access to DJR network for standalone laptops

Dear [redacted]

Further to our recent phone call and your email of the 15th June, I have conducted an investigation to determine the root cause from a [redacted] perspective of the introduction of the "Wannacry" virus to your network.

We have not detected the virus on any computer on any date before the 15th June despite the fact that virus templates and patches from Microsoft and Sophos were installed and active from the date of their release in May.

[redacted] has a mature data security and antivirus strategy, and this is described in a document published to all staff. Each staff member has to sign and accept this policy before being granted access to our network for any reason, and at every logon they must acknowledge the policy.

The aims of the network data security policy are to ensure that there is no data theft internally, that there is no unauthorised or un-sanitised external access to our network, and that any data received or sent from our network is screened for viruses.
Within our national network at each external connection, there is a firewall and a virus scanner. Each of these servers are updating both virus templates/software and operating system patches in real time.

The deployment of these updates is enforced by the network and is beyond the control of a user. Should the deployment fail then it will be noted and the IT team is automatically notified of the failure. This is detailed in both a local and central Log File. The individual is unable to change these configurations as only the IT Security Manager has administrative rights to the computer. The user does not have read or write access to the configuration directories including the root directory.

Every computer connected to our network for security reasons is rebooted or re-logged on every day so as to ensure that any software update is made active and any virus introduced and made active is sanitised.
The highest risk of any of these systems failing to be effective is with a field computer. To counteract this threat, we have employed several measures. All external USB storage devices are made read-only, all Optical drives are made read-only, and every file access and connection to the device is logged with a security program called Lumension.

Therefore, in normal circumstances if there was a breach of security (including a virus) the breach would be dealt with instantly and the whole event logged. The latest time that the IT Security Manager (and management) would be notified is within 12 hours of the event occurring.

Investigation of the virus event that you discussed with me on the 15th June detailing the introduction of a virus into the DJR network on the 6th June on the Hume highway revealed the following:

- The patches provided by Microsoft were applied via enforced script to every computer in May.
- The Sophos virus logs on every computer as at June 16th revealed that there was no presence of the "Wannacry" virus or any variants, nor had the virus been cleaned on any computer.

The inference [redacted] draws from this is that if the virus had been presented to our network then it would have been prevented "at the gate" (firewall).

Other methods of introducing the virus to our network would be Cameras, USB sticks, and mobile phones (classified by Lumension as a Storage Device) and foreign computers.

- Cameras - if a virus was presented to our network from a camera it would be sanitised at the first point of contact by our security systems. Our computers are unable to write to a camera.
- USB sticks - if a virus was presented to our network from a USB stick it would be sanitised at the first point of contact by our security systems. Our computers are unable to write to a USB stick, except via a special procedure controlled by the IT Security Manager.
- Mobile Phones - if a virus was presented to our network from a mobile phone it would be sanitised at the first point of contact by our security systems. Our computers are unable to write to a mobile phone. All company phones have antivirus software installed by policy and private email and file-sharing sites are blocked from our network. The risk with phones and connection with a field computer is mitigated by setting the USB ports to read-only. This prevents a phone from making a synced connection to a computer that may provide unauthorised internet access or the transfer of email from another email source. WIFI and Bluetooth ports are also restricted.
- Foreign computer- these are prevented from accessing our network by using static IP addresses. Every computer (and device) has been allocated a static IP reserved address and the DHCP range has been closed to accommodate this preventing any computer from connecting to our network except with the specific intervention of the IT Security Manager.

Importantly, [redacted] was testing on the Hume highway sites on the 6th and 7th June. However, on the 6th June, the day that the virus was introduced to your network, we did not connect a computer to your network. On the 6th June we were conducting sensor evaluation tests that do not require connection to your network. On the 7th June [redacted] was conducting repeatability tests on the Hume highway, at which time [redacted] connected to the DJR network.

Given the fact that this virus has not presented itself on our network, it is extremely unlikely that we were in a position to transmit this virus at any time.

All the computers that are used by the [redacted] traffic team, including the particular computer that was used on the Hume Highway on the 7th June, were subsequently interrogated on the 15th/16th June and the logs were interrogated by our IT Security Manager.

The findings revealed that none of the six computers had transmitted any files in either direction by USB or CD at any time. Five of these computers were found to have "up-to-date" virus templates/software and "up-to-date" Operating System patches.
A single computer, 31543, did not have "up-to-date" virus templates. This computer was used on the Hume on the 7th June.
This computer had not been logged off for several days prior to the 15th June. It was not until the 15th June that this computer was rebooted by our IT Security Manager and the virus was made active, at which time it was detected and immediately sanitised.

It is our professional assessment that [redacted] did not transmit the virus but simply received it from the camera system on the Hume highway, and all our evidence supports this.

[redacted] has had significant experience in the past in this area and as a result has developed a data security policy that has adapted to the ever-changing threat. Our policies always take on board changing scenarios and as such, are constantly improved to enhance their robustness. As a result of this review, we have taken subsequent actions with regard to findings, most of which are procedural, but they involve a series of additional custody sign-offs and security measures by each individual user and for each computer. In addition, all communication ports including wireless, and excluding the Ethernet Port, which were previously read-only, have now been completely disabled.

From a data security point of view, we have sufficient logging and preventative measures in place to ensure that any breach of security is detected and managed, and that any breach will be sufficiently documented to allow us to be able to reconstruct (as we have in this case) the particular scenario and take further action as appropriate.

Again, it is our professional assessment that [redacted] did not transmit the virus but simply received it from the camera system on the Hume highway.

Yours sincerely,

ANNEXURE F - Blue Connections Scan Results of (Vendor 2) hard drives

Disk	MalwareBytes	Windows Defender	Kaspersky	Bitdefender
KSA0609450	No threats found	No threats found	No threats found	No threats found
KSA0609448	No threats found	No threats found	No threats found	No threats found
KSA1680913	No threats found	WannaCrypt	WannaCryptor.H	WannaCryptor.H

Note: While KSA0609448 had no malware installed, there were clear indications (from the stored event logs) that the disk had previously been infected by WannaCry on 7-Jun-2017 07:27am. Disk KSA0609450's event logs did not go back as far as early June, so there is no evidence as to whether the disk was previously infected or not.

ANNEXURE G – BITRE estimated social cost of road crashes

T7.1 Estimated social costs of road crashes in Australia by cost element, 2006

Cost element	Human related costs			Property damage and general costs ($millions)	Total crash cost ($millions)	Proportion (per cent)
	Fatalities ($millions)	Hospitalised injuries ($millions)	Non-hospitalised injuries ($millions)			
Workplace and household losses	3007.2	2 573.9	108.9	na	5 690.0	31.9
Repair costs	na	na	na	4 227.5	4 227.5	23.7
Disability-related costs a	na	1 863.9	na	na	1 863.9	10.4
Non-economic or non-pecuniary costs	728.3	1 039.7	na	na	1 768.0	9.9
Insurance administration	13.2	256.5	na	1 421.3	1 691.0	9.5
Medical and related costs	3.4	511.4	349.5	na	864.2	4.8
Travel delay and vehicle operating costs	na	na	na	839.7	839.7	4.7
Legal costs	36.5	231.3	na	na	267.9	1.5
Vehicle unavailability costs	na	na	na	214.1	214.1	1.2
Emergency and police services cost	7.6	62.6	na	72.9	143.1	0.8
Work place disruption	10.3	77.7	na	na	88.0	0.5
Ambulance	3.6	59.9	na	na	63.5	0.4
Health cost of crash-induced pollution	na	na	na	53.4	53.4	0.3
Street furniture damage cost	na	na	na	40.2	40.2	0.2
Correctional services	15.3	na	na	na	15.3	0.1
Recruitment and re-training	6.6	2.5	na	na	9.2	0.1
Premature funeral cost	7.2	na	na	na	7.2	0.0
Coronial costs	3.1	na	na	na	3.1	0.0
Total	3 842.4	6 679.5	458.3	6 869.1	17 849.3	100.00

Note: Components may not add to totals due to rounding.

na not applicable.

a Disability-related costs include the costs of future care, specialist accommodation, therapy and specialist services, day programs, specialist equipment and alterations to houses.

Source: BITRE estimates.