Office of the Inspector-General of Intelligence and Security

Review of NZSIS holding and use of, and access to, information collected for security vetting purposes (Part two)

Public Report

Cheryl Gwyn
Inspector-General of Intelligence and Security

3 May 2017

I INTRODUCTION

1. I am required to regularly review the effectiveness and appropriateness of intelligence and security agency compliance systems concerning operational activity.[1] As part of that review function, in January 2015 I began an examination of the New Zealand Security Intelligence Service (NZSIS) systems for storing, using and controlling access to information that it compiles for the purpose of assessment (vetting) of candidates for New Zealand government security clearances.

2. I have reported on this review in two parts. The part one report concerned the physical storage of information and the controls on its use. This second part concerns the security compliance and the adequacy of access controls for the electronic record-keeping systems used by the NZSIS for security clearance information.

3. As a systemic review, the report assesses the NZSIS's compliance with applicable security requirements and standards. Where necessary it identifies steps needed to bring about compliance. It does not address individual responsibility or fault.

Content of this public report

4. Under ss 13, 25(8) and 25A of IGIS Act, I may not disclose information that would endanger any person or prejudice national security, the sharing of information by other governments or the intelligence and security agencies' capacity to discharge their functions.

5. I am satisfied that it is necessary to withhold some specific details of ICT systems and of aspects of the security of those systems, where disclosure would likely prejudice the national security interests recognised in the IGIS Act.[2] Further, to the extent that this report refers to necessary work by the NZSIS and the GCSB to resolve a number of compliance issues and previous potential vulnerabilities in these systems, it is not possible to report publicly on such work.

6. Those details have been included in the classified report that has been provided to the responsible Minister and the two Directors. I have also provided a classified report to key security-cleared personnel in the government agencies most affected by security clearance vetting, as with my part one report.

---

1 Inspector-General of Intelligence and Security Act 1996 (IGIS Act), s 11(1)(d)(ii).

2 As required by s 25(8) of the Act, I have consulted the Director of the NZSIS. Further, because the Government Communications Security Bureau (GCSB) is responsible for information security, including issuing the New Zealand Information Security Manual (*NZISM*) and accrediting certain systems, I consulted the Director of the GCSB on the content and national security aspects of this report.

II FINDINGS AND RECOMMENDATIONS

7. This report addresses the two remaining aspects of this review:

   7.1. Whether the four NZSIS electronic record-keeping systems used for security clearance information met New Zealand government requirements for the storage of national security information and, if not, the extent to which such information has or may have been compromised or has been at risk of compromise; and

   7.2. Whether logging of user access to electronic records indicated, and was able to indicate, unauthorised access.

Compliance with government requirements

8. The NZSIS currently holds security clearance vetting information on four ICT systems. They are described in this report as follows:

   8.1. OVR is an internet-connected system used to receive vetting information from security clearance candidates and referees. It was introduced in 2009.

   8.2. "System B" is a specialised internal NZSIS system used for vetting information. It was introduced in 2009.

   8.3. The document management system (DMS) and "System D" are internal NZSIS systems each used for a wide range of information. The DMS is used for a significant quantity of vetting information. More limited information is held on System D. Both were introduced in 2013.

9. Mandatory New Zealand government security standards applied to all four systems. Throughout the relevant time, the central requirements under those standards were, and are, that:

   9.1. Each ICT system must be formally certified – that is, the responsible agency, in this case the NZSIS, must undertake a comprehensive assessment of each system against information security standards; identify potential security vulnerabilities; and set out all necessary mitigations to reduce such risks to an acceptable standard, taking account of the sensitivity of the information held; and

   9.2. Each ICT system must be accredited, which requires an independent review of that certification. For highly classified systems – here, at least the DMS, System B and System D – accreditation must in practice be obtained from the GCSB. For less classified systems, accreditation can be provided by the Agency head or formal delegate as accreditation authority after an internal review, provided that the review is independent of the accreditation process.

10. I have found that, as at the date of this report, all four systems comply with the obligations set out in paragraphs 34 to 36 below. The certification and accreditation programme conducted by the NZSIS from June 2015 to July 2016, together with several significant security improvements made around the same time, provides a significant assurance of the security of each system as it now stands.

11. Until that certification and accreditation programme, however, the NZSIS instituted and operated all four systems without certification or accreditation, in breach of those security standards. OVR and System B were operated without accreditation from 2009-2016; the DMS from 2013-2015; and System D from 2013-2016.

Whether undue risk to security of information held

12. The NZSIS has now largely completed steps to address the shortcomings, some in conjunction with the GCSB. The NZSIS also took steps to identify and address security vulnerabilities at the time of adopting each of the four systems. Notably:

    12.1. Two of the four systems used software already used by partner intelligence agencies, so the NZSIS relied on security work already undertaken by those agencies; and

    12.2. The three internal systems were operated within a standalone secured network, which afforded significant assurance against external compromise.

13. These and other steps undoubtedly lessened security vulnerabilities, though they did not afford the comprehensive assessment and assurance that was required. In particular, certification is concerned both with each ICT system and with its particular installation and environment, not with particular software or wider systems. Overall, there was no systematic and comprehensive identification, management and mitigation of risk, or external verification of that assessment.

14. Subsequent system-wide measures adopted over the past two years have also materially reduced potential risks and formed part of the accreditation of the four systems.

15. However:

    15.1. Other steps were commenced but not completed. In particular, an NZSIS programme to secure comprehensive accreditation began in 2010 on an urgent basis but was then downgraded to “business as usual” and ultimately closed in 2014, without securing any accreditations. Similarly, an external review conducted for the NZSIS at the time that the DMS and System D were introduced in 2013 specifically recommended accreditation, but that recommendation was not followed.

15.2. It appears that there were potential security vulnerabilities that were not adequately addressed at the time. For example, the GCSB had specifically identified what it regarded as a risk of compromise in one system before its entry into operation. The NZSIS and the GCSB have since, through a number of measures, undertaken further work to address potential vulnerabilities.

Remedial steps undertaken and further work underway or recommended by this review

16. The NZSIS has undertaken some investigation of the potential for past compromise of these systems and that has not given any indication of compromise during their periods of non-certification/accreditation.

17. While retrospective investigation of these systems is difficult, I have recommended that the NZSIS, with GCSB assistance, carry out such further investigations as are feasible. While certification and accreditation provide a substantial assurance of the security of relevant systems as now in place, it does not involve an assessment of whether systems were compliant in the past, particularly when those systems have been upgraded and supplemented over time, as here. Such further work as can be done is needed in order to provide greater assurance about these systems.

ICT access controls

18. In addition to our review of compliance of the four systems, we undertook testing of available logged access data. Only limited data was available and only for one of the four systems. Our analysis of that data indicated:

18.1. There was no unauthorised access, so far as could be ascertained from the available data. There were instances of access to and, more often, management of records by non-vetting staff but these were justifiable.

18.2. Current user access controls do not meet the need-to-know standard.[3] As noted in the part one report, ICT access controls give access rights to the approximately 60 NZSIS personnel with vetting responsibilities to most people's security vetting files, whether or not those files are needed by that user and whether the files are active or not.[4] The NZSIS currently relies upon users to comply with an access agreement and I acknowledge that users take that agreement seriously, but data protection

[3] See, for example, *Protective Security Requirements ("PSR")* "The need-to-know principle" (staff to have access only to information that they need, rather than for convenience) and see also *Review of NZSIS holding and use of, and access to, information collected for security vetting purposes (Part one)* (April 2016, accessible at http://www.igis.govt.nz), 6 at n 5.

[4] See *Review*, above n 3, 8. As a step towards implementing the recommendations in the part one report, the NZSIS has reviewed the groups of authorised users to identify and remove users who do not require access.

standards also require ICT controls. Such controls will ensure that each staff member may access only those files that he or she actually needs.

18.1. Controls over access privileges are inadequate. The analysis of logged access data indicated, for example, that individuals' vetting documents could mistakenly be assigned access privileges that would allow almost any NZSIS staff member to come across them. The controls around access privileges do not necessarily identify such mistakes. Access audit measures were also inadequate at the time of our review. They are now being improved, along with training and other measures.

Recommendations

19. I make the following recommendations as a result of this review:

R1: The NZSIS, with GCSB assistance, should continue to pursue whatever testing or other steps are practicable to assess and if need be address any past or existing vulnerabilities or compromise in the four systems. Where further work is required to address identified vulnerabilities, it should occur with appropriate priority. The NZSIS should report on that work to my office.

R2: In the event that the NZSIS considers it necessary to institute new systems without full certification or accreditation, it should follow the procedure prescribed in the NZISM. In particular, if the NZSIS seeks to accredit without certification, it must do so only so far as permitted by, and consistently with, the NZISM.

R3: In addition to bringing ICT access controls into compliance with the need-to-know standard, as set out in the part one report, the NZSIS should strengthen ICT safeguards against inadvertent or unauthorised access to vetting-related files and ensure that:

R3.1: Incorrect access permissions cannot be assigned;

R3.2: If access permissions are incorrectly assigned, they are more readily identified and removed;

R3.3: Personal/local file areas are never used for vetting-related documents; and

R3.4: Access records are routinely audited, in addition to any general system auditing.

20. The Director of Security has accepted the recommendations made in this report.

III REVIEW PROCESS

Overall process

21. The overall process followed in this review is set out in the part one report.[5] In addition to the steps set out there, my office has also obtained a range of information and documents from the GCSB, because the GCSB has been involved both in some of the events described and in much of the remedial work recommended here.

22. The completion of this part of the review report took longer than I had anticipated, principally for two reasons:

    22.1. I decided in late 2015 to wait on the completion of the NZSIS remedial work that began during this review, so as to be able to assess it in this report.

    22.2. Some relevant information proved difficult to access and comprehensive records of some events were not available. In particular, the NZSIS advised towards the end of the review process that some further relevant information might be known only to key officers who had since left the organisation and/or might be held on retired ICT systems that are now inaccessible.

23. This report was provided in draft to the Director of the NZSIS to ensure its completeness and accuracy; to give an opportunity for response on conclusions and recommendations critical of the NZSIS; and for consultation on security classification matters.[6] I have taken into account comments provided by the Director. I also provided a draft for comment to the GCSB, because of its involvement as outlined above, and have as appropriate incorporated the GCSB's comments.

Whether inquiry necessary

24. On occasions, a regular review of compliance under s 11(1)(d) of the IGIS Act might raise matters that necessitate an inquiry under ss 11(1)(a) and 19-24. An inquiry is a more formal process, involving for example the taking of sworn evidence under summons from relevant individuals, with independent legal representation.

25. As this review progressed and the NZSIS's non-compliance with mandatory standards became apparent, I considered whether to institute a formal inquiry into the decisions made by the NZSIS and any question of responsibility for those decisions.

26. I decided not to proceed from this review to such an inquiry for two reasons. The first is that, I believe, the principal additional benefit of any further inquiry beyond this review has already been secured:

---

5 *Review*, above n 3, 6.

6 IGIS Act, s 25(8).

26.1. The Director of the NZSIS has accepted responsibility for the Service's non-compliance, which is now remedied. The Director further advised that, while she accepted that the decisions were in breach of mandatory government requirements, they were made by the NZSIS as a whole and, from her perspective, were made in good faith.

26.2. The Director has agreed that I can provide a classified report of this review to key security-cleared personnel of those government agencies most significantly affected by security clearance practices. That affords those agency representatives a complete account of what has and has not been done to protect the data of their personnel and provides additional external accountability.

26.3. The Director has also, in accepting the recommendations of this review, made a commitment to complete such further work as is needed.

27. I also concluded that it would be very difficult to undertake a further inquiry in a rigorous and fair way:

27.1. It is difficult at this point to reconstruct the detail of the NZSIS's decisions and the reasons for those decisions. As I noted above, the NZSIS advised during the review process that there may be further information that is no longer practically accessible. I note that the NZSIS has, following an earlier inquiry by my office, instituted much better record-keeping practices.

27.2. There are difficulties in evaluating the decisions made by the NZSIS and its personnel at the relevant times. The available records indicate that concerns were raised within the NZSIS, as well as by the GCSB, over potential security non-compliance and vulnerabilities and remedial steps were proposed, though these did not proceed. More widely, perceptions of information security risks have changed significantly since many of these decisions, as reflected in reactions to the Snowden insider disclosures and the OPM data breach.[7]

28. I consider that this review and recommendations made here are an adequate and proper response.

[7] See paragraph 31 below.

IV RELEVANT SECURITY STANDARDS FOR ELECTRONIC RECORD-KEEPING SYSTEMS

29. The review has assessed the compliance of the four systems used by the NZSIS to hold security clearance information with applicable New Zealand government information security requirements for holding classified national security information, both at present and since the systems' entry into operation.

Background and purpose of this part of the review

30. As I explained in part one of this report, the compilation, analysis and retention of personal information by the NZSIS for security clearance purposes is significant because of:

    30.1. The breadth and depth of that information, which relates to thousands of people, including many in sensitive employment;

    30.2. The importance of security clearance work to the NZSIS, both as a key safeguard for information security and as a substantial and highly visible component of its work; and

    30.3. The need for clarity and trust on the part of the people who provide sensitive information to the NZSIS, both for security clearance holders who must disclose sensitive information to obtain and retain their jobs and for referees who agree to provide information.[8]

31. The significance of the security of electronic recordkeeping systems and the risk to such systems is demonstrated by the revelation of successive breaches of security clearance applicant data at the United States Office of Personnel Management (OPM) in 2014-2015. These involved loss of data for more than 22 million people, with consequent risks to those people and to national security that I noted in the part one report.[9]

32. Subsequent reporting of those breaches, both in the media and in a September 2016 United States congressional staff report, has provided further detail. In particular, it has indicated that OPM had operated just over half of its key systems without current authorisations to operate, which are the United States equivalent of certification and accreditation. OPM had declined to follow oversight recommendations that these systems cease operation while authorisations to operate were secured, so as not to disrupt its operations.[10]

---

8 *Review*, above n 3, 4.

9 *Review*, above n 3, 5.

10 United States House of Representatives Committee on Oversight and Government Reform *The OPM Data Breach: How the Government Jeopardised our National Security for More than Generation* (2016), 21-22 & 48.

New Zealand government information systems security requirements

33. Information system security requirements apply to all New Zealand government agencies that hold classified information in electronic form. During the period relevant to this review, these requirements were set out by:

    33.1. *Security in the Government Sector* (*SIGS*), which applied from 2002-2014, was formulated and issued on the authority of the Prime Minister through the Interdepartmental Committee on Security. *SIGS* was expressed to be mandatory for all government departments and other agencies, including the NZSIS;[11]

    33.2. The *Protective Security Requirements* (*PSR*), which replaced *SIGS* in December 2014 and is again expressed to "set out the government's mandatory requirements";[12] and

    33.3. The *NZISM*, which details specific security standards and was in effect throughout the period. Compliance with *NZISM* was mandated both under *SIGS* and then under *PSR*.[13]

Certification and accreditation

34. The central requirement for systems that handle classified information under *SIGS*, *PSR* and *NZISM* is certification and accreditation. *NZISM* describes certification and accreditation as:[14]

> "… the fundamental governance process by which the risk owners and agency head [derive] assurance over the design, implementation and management of information systems …"

35. Certification is based on a comprehensive evaluation or systems audit and is evidence that due consideration has been paid to risk and security[15]. Certification of any given IT system is "confirmation that it meets all security requirements" and "involves confirmation by the system developers or administrators that the documentation is correct and complete and that the document security architectures, mechanisms and processes have been implemented".

36. Accreditation is "the process of verifying the system's security and formally authorising the system for operation", involving an independent review of whether the security measures meet the required level of security; inspections to ensure that security has been implemented; and ultimate determination of whether the system has approval to operate.

---

11 *SIGS,* 8.

12 *PSR*, "Information Security Management Protocol: Mandatory requirements".

13 *NZISM*, [6.1]-[6.2].

14 *NZISM*, [1.1.17].

15 *NZISM* 4.1.11 & 4.1.12.

For all highly classified information, the GCSB was and remains the accreditation authority. Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged, including the acceptance of any residual risk.[16]

Wider purposes of information security standards

37. The relevant standards indicate two wider purposes:

37.1. The first is public assurance. While the contents and details of secure information systems will often be sensitive, transparent compliance of those systems with government standards is critical to public accountability:[17]

> "The environment conducive to good security is not necessarily secret. In fact, the decision-making process must be as transparent as possible. This will ensure accountability to the New Zealand public."

37.2. The second is to ensure whole-of-government management of risks, as reflected in the *NZISM*:[18]

> "[Mandatory c]ontrols for classified systems … cannot be *individually* risk managed by agencies without jeopardising their own, multi-agency or all of government information assurance."

Findings on NZSIS compliance with information security standards

Absence of accreditation until 2015/2016

38. The NZSIS instituted each of the four information systems used for vetting information without certification or accreditation.

39. All continued in operation without certification or accreditation until an urgent accreditation programme undertaken from June 2015 to July 2016.

40. Prior to that:

40.1. The NZSIS discussed certification and accreditation of OVR and System B with the GCSB in 2009. The GCSB raised a broad range of security concerns, including at Director to Director level. The NZSIS did address some of those concerns but put the two systems into operation without certification or accreditation.

---

16 *NZISM,* 4.1.17.
17 *SIGS***,** ch [1-2].
18 *NZISM*, [1.1.61.R.01] (emphasis in the original).

40.2. The NZSIS did not seek to certify the DMS or System D or seek GCSB accreditation before it put them into operation. Some preliminary certification work began but did not proceed. An external review of the two systems shortly after their implementation recommended that accreditation be secured but that recommendation was not acted upon.

40.3. The NZSIS has noted some security steps taken around each system. Those steps may, to varying degrees, have lessened potential security risks, but the NZSIS accepts that there was no comprehensive or systematic process to identify and seek to mitigate security vulnerabilities over these respective periods.

41. These actions breached a number of mandatory information security requirements under *SIGS/PSR* and *NZISM*, including the following:

41.1. The NZSIS was required to secure accreditation for all four systems before their entry into operation, their connection to any other system, and during their continued operation;[19]

41.2. In the absence of accreditation, the NZSIS was required to get dispensations from the GCSB and to review non-compliant systems at least every year;[20] and

41.3. The NZSIS was required to ensure that information security monitoring, logging and auditing was conducted on all accredited systems.[21]

NZSIS initiatives since the start of this review

42. In the course of this review, the NZSIS commenced three further initiatives:

42.1. The first, which occurred from late May to mid-August 2015, was the signature by senior NZSIS staff of "system certification waivers".

42.2. The second, which began in June 2015, was an urgent programme of certification and accreditation. That programme secured accreditation of the DMS in September 2015, OVR in March 2016 and the remaining two systems in July 2016.

42.3. The NZSIS has undertaken some limited testing of one of the four systems in 2015 and is currently pursuing further testing. It has also consulted with the GCSB.

Use of "System Certification Waivers"

43. In June-August 2015 the NZSIS drafted documents titled "System Certification Waivers" (SCW) for each of the four systems. These were intended to provide a pragmatic means of

---

19 *NZISM,* 4.4.5.C.01; C.02; C.03.

20 *NZISM,* 1.1.61.C.01 and 1.1.65.C.01.

21 *NZISM,* 4.4.5.C.04.

deciding whether to continue to operate each system pending certification and accreditation work.

44. The signature of the four SCWs marked acceptance by senior NZSIS personnel of the NZSIS non-compliance and of a prescribed timeframe to address that non-compliance. However:

    44.1. Under the *NZISM*, the NZSIS could proceed to accreditation without certification only for systems that were not highly classified: for any highly classified system, only the GCSB could make that decision. The *NZISM* does provide for emergency use of unaccredited systems and for provisional accreditation.

    44.2. While SCWs were expressed to balance the risks of operating without certification and accreditation against the operational impact of ceasing use of the systems, two of the SCWs did not include security risk information. While I understand that some evaluation did nonetheless occur, there was limited or no recorded assessment. The SCWs were also intended to provide a basis for seeking provisional accreditation from the GCSB but were inadequate for that purpose.

45. I have therefore recommended that the *NZISM* procedure should be followed in future.

2015/2016 certification/accreditation

46. The certification and accreditation programme conducted by the NZSIS from June 2015 to July 2016 has brought the NZSIS into compliance with its *NZISM* and *PSR* obligations. Some indication of the scale and technical significance of the certification and accreditation process is given by the time required, which ranged from three months to more than a year, against initial estimates of approximately three months. I acknowledge that the NZSIS undertook this work alongside other security initiatives that required significant resources.

47. In addition to ensuring current compliance, the certification and accreditation programme gives a significant indication of the security of each system as it stands.

48. However, certification and accreditation does not assess the potential for past vulnerability or past compromise. Additional security measures were added to each of the four systems during the periods between their introduction in 2009/2013 and their accreditation between two and seven years later and some of these were expressly relied upon in the certification and accreditation assessment.

Security testing to date

49. The NZSIS undertook some limited testing of one system in 2015 and is currently undertaking further testing. At the time of concluding this report, the NZSIS and the GCSB were also working towards further investigations. The NZSIS has accepted my recommendation to pursue such assessment as far as practically feasible.

V ANALYSIS OF LOGGED ACCESS TO VETTING RECORDS

50. The part one report found that:

    50.1. There was not adequate logging or audit of access to vetting records; and

    50.2. System access controls to electronically held vetting records allowed access to most vetting records for all staff with vetting responsibilities, regardless of whether that access was needed. The part one report recommended significant narrowing of access controls so as to meet the "need to know" standard.

51. In this second part of the review, we sought to compile and analyse available data for access to records held in each system. The aim was to ascertain:

    51.1. So far as possible, if the logged data indicated any unauthorised or inappropriate access to vetting records; and

    51.2. The extent to which data logging indicated adequate controls within these systems against unauthorised access.

52. Our analysis identified two basic limits in pursuing these questions:

    52.1. Useable logged access data was available for only one of the four systems. Two systems did not generate significant log data and, while it was technically possible to retrieve data from a third, that would have required significant staff work that could not be done at the time. During the course of this review, a wider access logging and audit system has been developed and extends to some of the four systems.

    52.2. For the fourth system, the access controls permitted all staff with vetting responsibilities – approximately 60 NZSIS personnel – to access most vetting records and there is no recording of reasons for access to individual records, as noted in the part one report. As such, the available logged data would not identify anomalous access by vetting staff. The logged data could identify instances of access to vetting records by non-vetting staff.

53. This part of the review further clarified the findings made in the part one report that while there is some logging and some audit, these would detect only some forms of unauthorised access.

54. I acknowledge that NZSIS staff sign, and are subject to, a detailed user access agreement and that staff take that agreement seriously. However, such agreement alone is

inadequate; there must also be systemic controls to ensure "need to know" access and to detect and prevent unauthorised access, whether intentional or inadvertent.[22]

55. Our limited analysis of logged access indicated that while vetting files were occasionally accessed by non-vetting staff and, more often, files dealt with without viewing their content, those instances did not indicate improper access.

56. Some of these instances did, however, reflect deficiencies at a systemic level:

    56.1. Some of the instances of administrative or other management file actions indicated that staff were able to deal with vetting files not only through administrator accounts, which is appropriate, but in some instances through individual accounts, which is not.

    56.2. Some instances also indicated that some vetting files had been stored in users' local or shared drives, rather than on record systems. They were therefore not subject to systemic access controls, logging or – in some cases – backup/archiving. NZSIS policy directs staff not to use such drives but there is no ICT control to prevent that occurring.

    56.3. Our analysis also indicated that access permissions could be incorrectly assigned and such errors were not automatically or regularly detected and fixed. For example, in one instance identified by our review, a complete vetting record was incorrectly assigned access permissions that would have permitted access by virtually all NZSIS staff.

57. The NZSIS advised that the system does not prevent human error in assigning access controls to each record. The NZSIS explained that in recognition of incorrect application of access privileges, the system administrator regularly runs scripts across all vetting files to update the access privileges applied to some vetting records, though it later clarified that the scripts must be initiated manually and that there was no schedule for running scripts.

Conclusions on access controls

58. Access privileges afford a potentially effective means of protecting data, consistent with the need-to-know standard, which is required both for information security and for privacy of personal information.[23]

59. My report on part one of this review found, however, that the vetting-related access privileges were so wide that most vetting-related files could be accessed by all of the approximately 60 NZSIS staff with vetting-related responsibilities, and so did not meet the need-to-know standard. The NZSIS has accepted a recommendation to reform its use of

[22] *Review,* above n 3, 7.
[23] *Review,* above n 3, 7.

access privileges accordingly.[24] That fault in the system, and the need for change, is emphasised here: because the access privileges were so wide, it was not possible to determine from logged data if vetting-related staff had or had not undertaken unauthorised access to vetting-related files. Even if the NZSIS had audited logged data, auditing would almost certainly not have identified such access.

60. This analysis identified other gaps in access controls. I acknowledge that some system-wide security measures that are being incrementally introduced have improved logging and, over time, will improve audit of access, but more is required to meet data protection standards.

61. I have made recommendations to address these inadequacies.

[24] See n 4 above.

CHRONOLOGY[25]

2008-2009	NZSIS and contractors develop OVR and System B to streamline security clearance vetting process.
	NZSIS consults GCSB over security and accreditation. GCSB identifies significant security vulnerabilities, some of which are addressed by NZSIS.
	NZSIS undertakes some preliminary certification work in pursuit of GCSB accreditation but does not proceed further.
2009	NZSIS commences operation of OVR and System B without certification or accreditation.
2010	NZSIS commences urgent comprehensive certification and accreditation programme. Programme later downgraded to business as usual.
2011-2013	NZSIS works to develop its document management system (DMS) and System D. NZSIS does not undertake certification and does not seek accreditation from GCSB. Security assessment work undertaken, which includes recommendations to undertake certification/accreditation, but recommendation not pursued.
2013	NZSIS commences operation of the DMS and System D without certification or accreditation.
	NZSIS canvasses possible redevelopment for one system, including for the purpose of enabling certification and accreditation. Redevelopment does not proceed.
2014	NZSIS implements additional security steps for one system.
	NZSIS and GCSB begin introduction of wider security measures for two systems.
January 2015	OIGIS review of holding of security vetting information commenced.
June 2015	NZSIS begins urgent programme to address certification and accreditation of all four systems.
September 2015	DMS accredited.
Late 2015	NZSIS and GCSB implement significant new security steps for one system.
March 2016	OVR accredited.
July 2016	System B and System D accredited.
November 2016	NZSIS and GCSB commence additional security review for one system.

[25] While this review has found a large volume of NZSIS and GCSB records, the NZSIS has indicated that there may be further relevant records held in systems that are now not practically accessible: see paragraph 22.2 above. For that reason, it has been necessary to give only approximate dates for some events.