Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
1. Assemble State Entity Response Team	p. 5			
1.1. Escalation Manager/Team Lead	p. 5			
1.2. Program Manager (office experiencing the breach)	p. 5			
1.3. Information Security Officer	p. 5			
1.4. Chief Privacy Officer or Coordinator	p. 5			
1.5. Public Information Officer or Communications Officer	p. 5			
1.6. Legal Counsel	p. 5			
1.7. Other	p. 5			
1.8. Chief Information Officer or Technology Specialist	p. 5			
1.9. Personnel Office or Human Resources Manager	p. 5			
2. Escalation/Internal Reporting	p. 5			
2.1. Deputy Director	p. 5			
2.2. Director	p. 5			
2.3. Agency Secretary	p. 5			
2.4. Governor's Office	p. 5			
3. Is an impact assessment/coordination meeting necessary?	p. 5			
3.1. Agency Response Team Members to Attend	p. 5			
3.2. OIS Response Team Member to Attend	p. 5			
3.3. CCIU Response Team Members to Attend	p. 5			
3.4. Sign in Sheet / Attendee roster needed	p. 5			
3.5. Non-disclosure agreement forms needed	p. 5			
4. Security Incident Reporting	p. 5			
4.1. Reported through Cal-CSIRS	p. 5			
4.2. Respond to CHP CCIU response inquiry	p. 5			
4.3. Respond to OIS response inquiry	p. 5			
4.4. Update follow-up report (SIMM 5340-B) through Cal-CSIRS	p.6			
5. Is breach notification required by law (Civil Code Section 1798.29)?	p. 7			
5.1. Was computerized data owned or licensed by the agency involved?	p. 7			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
5.2. Was a computer system, equipment, or peripheral storage device (capable of containing computer data) involved?	p. 7			
5.3. Were notice-triggering data elements involved?				
5.3.1. First name or first initial and the individual's last name, and one or more of the following:	p. 7			
5.3.2. Social Security number.	p. 7			
5.3.3. Driver's License number or California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.	p. 7			
5.3.4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	p. 7			
5.3.5. Medical information (as defined in Civil Code Section 1798.29).	p. 7			
5.3.6. Health insurance information (as defined in Civil Code Section 1798.29).	p. 7			
5.3.7 Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.	p. 7			
5.3.8 Automated License Plate Recognition (ALPR) System information (as defined in Civil Code Section 1798.90.5).	p. 7			
5.3.9 A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.	p. 8			
5.4. Were the notice-triggering data elements encrypted?	p. 8			
5.4.1. Was the encryption product used, a FIPS -140 validated or NIST certified cryptographic module?	p. 8			
5.5. Were notice triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person? ***(Examples only-list is not limited to these***):	p. 8			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
5.5.1. The system, equipment, or information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information.	p. 8			
5.5.2. The information has been downloaded or copied (e.g., any evidence that download or copy activity has occurred).	p. 8			
5.5.3. The attacker deleted security logs or otherwise "covered their tracks".	p. 8			
5.5.4. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting.	p. 8			
5.5.5. The attack vector used is known to seek and collect personal information.	p. 8			
5.5.6. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.	p. 8			
6. Is breach notification required by Information Technology policy	p. 9			
6.1. Was data, of any media type or format (e.g., paper, cassette tape), owned or licensed by the agency involved?	p. 9			
6.2. Were notice-triggering data elements involved?	p. 9			
6.2.1.First name or first initial and the individual's last name, and one or more of the following:	p. 9			
6.2.2. Social Security number.	p. 9			
6.2.3. Driver's License number or California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.	p. 9			
6.2.4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	p. 9			
6.2.5. Medical information (as defined in Civil Code Section 1798.29)	p. 9			
6.2.6. Health insurance information (as defined in Civil Code Section 1798.29)	p. 9			
6.2.7 Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to	p. 9			

authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.				
6.2.8 Automated License Plate Recognition (ALPR) System information (as defined in Civil Code Section 1798.90.5).	p. 9			
6.2.9 A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.	p. 9			
6.3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired? ***(Examples only-list is not limited to these***):	p.9			
6.3.1. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information.	p.9			
6.3.2. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.	p.10			
6.3.3. The information has been shared by an unauthorized person or was used by an unauthorized person, such as instances of sharing the personal information with the media or tabloids, or identity theft reported or fraudulent accounts opened.	p.10			
7. Timeliness of Notification	p.10			
7.1. Notification can be sent within ten (10) days from the date data acquisition has been determined.	p.10			
7.2. Notification may be delayed due to legitimate needs of law enforcement.	p.10			
7.3. Notification may be delayed to determine scope of breach.	p.10			
7.4. Notification may be delayed to restore system to reasonable integrity.	p.10			
7.5. Delay will or may exacerbate the risk of harm to individuals.	p.10			
7.6. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) has authorized the delay of notification.	p.10			
8. Source of Notification	p. 10			
Breach Response Requirement or Element	**SIMM 5340-C Reference**	**Yes**	**No**	**Notes/Comments**

8.1. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) will sign the notice.	p. 10			
8.2. The notice is addressed by the entity in which the recipient has a relationship.	p. 10			
8.3. The notice is addressed by an entity in which the recipient has no direct relationship, but the relationship is explained sufficiently in the notice.	p. 10			
9. Format of Notice	p. 11			
9.1. The notice shall be designed to call attention to the nature and significance of the information it contains, and shall be formatted on official letterhead to include:	p. 11			
9.1.1. No smaller than 10-point Arial font type;	p. 11			
9.1.2. A title "Notice of Data Breach"; and	p. 11			
9.1.3. Contain at a minimum the following headings: • "What Happened"; • What Information Was Involved"; • "What We Are Doing"; • "What You Can Do"; • "Other Important Information"; and • "For More Information ".	p. 11			
10. Content of Notice	p. 11			
10.1. The notice leverages the sample notifications provided by OIS.	Appendices B-I			
10.2. The notice is clear and concise.	p. 11			
10.3. The notice uses easy-to-understand language and does not include technical jargon.	p. 11			
10.4. The notice includes a general description of what happened; including the date of breach if known, or estimated date or date range within which the breach occurred.	p. 11			
10.5. The notice specifically identifies the data elements involved.	p. 11			
10.6. The notice includes the steps the individual can/should take to protect themselves from harm (if any).	p. 12			
10.7. The notice includes an apology.	p. 12			
10.8. The notice includes information about what the agency has done or is doing to investigate the breach, mitigate the losses, and protect against any further breaches.	p. 12			
Breach Response Requirement or Element	**SIMM 5340-C Reference**	**Yes**	**No**	**Notes/Comments**

10.9. The notice includes the name and contact information of an individual contact(s) at the agency with the ability to provide more information about the breach to the affected individuals.	p. 12			
10.10. The notice provides a toll-free number for the agency contact, physical address, e-mail address, and postal address if available. If the agency does not have a toll-free number a local number for the contact is provided.	p. 12			
10.11. The agency has knowledge that affected individuals are not English speaking and has prepared notices in the appropriate languages.	p. 12			
10.12. The agency has given consideration in providing the notification to individuals who are visually or hearing impaired (e.g., establishing a TDD or posting a large-type notice).	p. 12			
11. Approval of the Notice	p. 12			
11.1. Draft notice submitted to OIS for review and approval prior to their release:	p. 12			
11.1.1. Communicated with an OIS security representative by telephone contact, prior to submission.	p. 12			
11.1.2. Submitted breach notification into Cal-CSIRS, selecting "Breach Notification for Review" as the type.	p. 12			
11.1.3. Have allowed at least one full business day for OIS review.	p. 12			
11.2. Final notice submitted to OIS and includes required information.	p. 13			
11.3. The agency has notified and/or sought prior approval for release of notice or the use of reference from other public and private sector agencies that may be impacted by the breach or play a role in mitigating the potential harms (e.g., credit reporting agencies, etc.).	p. 13			
12. Method of Notification	p. 13			
12.1. First-class mail notification will be made.	p. 13			
12.1.1. Addressed to the named individual.	p. 13			
12.1.2. Mailed to the last known address.	p. 13			
12.1.3. Mailed separately from other letters and notices.	p. 13			
12.1.4. Labeled on the outside of the envelope to alert recipient to the importance of its contents (e.g., "Important Information Enclosed"), and as to reduce the possibility that it may be mistaken for advertising mail.	p. 13			
Breach Response Requirement or Element	**SIMM 5340-C Reference**	**Yes**	**No**	**Notes/Comments**

12.1.5. Includes sender or return address information. Special caveats noted here.	p. 13			
12.2. Telephone notification will be made with a concurrent follow-up written by first-class mail.	p. 14			
12.3. E-mail notification will be made as the following criteria are met:	p.14			
12.3.1. Individual has provided agency with an e-mail address.	p.14			
12.3.2. Individual has provided written consent to use e-mail as the primary means of communication.	p.14			
12.3.4. E-mail notification is consistent with the provisions regarding electronic records and signatures set forth in the Federal Electronics Signatures Act (15 U.S. Code 7001).	p.14			
12.4. Substitute notification will be made as the following criteria are met:	p. 14			
12.4.1. Agency has demonstrated that more than 500,000 individuals were affected; or the cost of providing notification would exceed $250,000; or the agency does not have adequate contact information on those affected (no known mailing address is available).	p. 14			
12.4.2. Substitute notification, as required, will include the following collectively: 1) Conspicuous posting on the agency website; 2) Notification to statewide media; and 3) E-mail notification when the agency has an e-mail address to individuals. Here, the requirements of the Federal Electronics Signatures Act **do not** need to be met.	p 14			
12.4.3. Web posting will be made on homepage or a conspicuous link from the homepage.	p.14			
12.4.4. Web posting will also include a link to FAQs.	p.14			
12.4.5. Information in press release will not impede or compromise the investigation or pose other security risks.	p.15			
12.5. Agency has elected to issue press release, as well as first-class notification due to the number of individuals affected.	p.15			
12.5.1. Information in press release will not impede or compromise the investigation or pose other security risks.	p.15			
13. Preparation for Follow-on Inquiries from Noticed Individuals	p.15			
Breach Response Requirement or Element	**SIMM 5340-C Reference**	**Yes**	**No**	**Notes/Comments**

13.1. The agency's public intake areas have been alerted and trained as appropriate to properly direct telephone and in-person inquiries about the breach.	p.15			
13.1.1. Inquiries from the press are to be directed to:	p. 15			
13.1.2. Inquiries from individuals receiving the notice and needing more information are directed to:	p. 15			
13.2. The agency has provisioned for a toll-free call center, staffed with trained personnel.	p. 15			
13.3. The agency has provisioned for documented scripts, and answers to anticipated and frequently asked questions.	p. 15			
13.4. The agency has provisioned for a complaint resolution and/or escalation process.	p. 15			
13.5. The agency has provided early warning and information about the timing of notification to all counterparts, so that they are prepared for the potential surge in inquiries (e.g., credit reporting agencies, etc.).	p. 15			
14. Other Situations When Breach Notification Should be Considered	p. 16			
14.1. The agency has considered the nature of any non-notice triggering personal information involved in this breach and the potential harms it poses or may pose to affected individuals.	p. 16			
14.1.1 The agency has determined the nature of the information does potentially pose one or more of the following potential harms ***(Examples only-list is not limited to these***):	p. 16			
14.1.1.1. Harm to reputation.	p. 16			
14.1.1.2. Potential for harassment.	p. 16			
14.1.1.3. Potential for prejudice, particularly when health or financial benefits information is involved.	p. 16			
14.1.1.4. Financial loss.	p. 16			
14.1.1.5. Embarrassment.	p. 16			
14.1.1.6 Legal problems.	p. 16-18			
14.2. The agency has considered the likelihood that the information has been acquired, or is accessible and usable.	p. 16			
14.2.1. The agency has determined it is known or highly likely the information has been acquired and has the potential for misuse by unauthorized persons due to the following ***(examples only-list is not limited to these***):	p. 16			
14.2.1.1. The information was not encrypted.	p. 16			
Breach Response Requirement or Element	**SIMM 5340-C Reference**	**Yes**	**No**	**Notes/Comments**

14.3.1.2. The list was posted on the Internet for an extended period of time.	p. 16			
14.2.1.3. The encryption product used was not a NIST certified cryptographic module or FIPS-142 validated product.	p. 17			
14.3. The agency determined there is a likelihood that the breach may lead to harm due to the following ***(examples only-list isnot limited to these***):	p. 17			
14.3.1. breach of confidentiality or fiduciary responsibility;	p. 17			
14.3.2. disclosure of address for victims of stalking or abuse; or persons in high risk professions;	p. 17			
14.3.3. legal problems;	p. 17			
14.3.4. harm to reputation;	p. 17			
14.3.5. financial loss;	p. 17			
14.3.6. disclosure of private facts and unwanted exposure; potential for secondary uses of the information which could result in fear or uncertainty;	p. 17			
14.3.7. potential for harassment, blackmail, or prejudice;	p. 17			
14.3.8. the social security number alone can lead to identity theft.	p. 17			
14.4. The ability of the agency to mitigate the risk of harm to individuals.	p.17			
14.4.1. The agency can mitigate further compromise of the system.	p.17			
14.4.2. The agency can monitor systems for misuse of the personal information and patterns of suspicious behavior.	p.17			
14.4.3. The agency has exhausted its ability to mitigate any further risk of harm.	p.18			
14.4.4. The apology and assurance of corrective action may serve as a satisfactory remedy those impacted.	p.18			
14.5. The ability of the noticed individual to mitigate the risk to themselves following notification.	p.18			
15. Other Actions Agencies Can Take to Mitigate Harm	p.18			
15.1. The agency has notified financial institutions if state payroll or bank account information was involved.	p.18			
15.2. The agency has notified other agencies about the potential for benefit fraud as applicable (e.g., disability, unemployment, Medi-Cal)	p.18			
16. Other Considerations When State Employee Data Is Involved				
Breach Response Requirement or Element	**SIMM 5340-C Reference**	**Yes**	**No**	**Notes/Comments**
16.1. Agency has treated affected employees with the same care and	p.18			

concern as any other individual affected by breach.				
16.2. Agency has considered other early warning and notification methods to augment the first-class mail notification (e.g., such as e-mail, Intranet posting, town hall meetings).	p.18			
16.3. Agency has notified managers and supervisors of the affected employees and adequately prepared them to answer questions from employees.	p.18			
16.4. Agency has considered notifying represented employee organizations as may be appropriate.	p.18			
16.5. Agency has considered the use of town hall meetings to respond to employee questions and concerns following notification.	p.18			
17. Other Considerations From a Public Relations Perspective	p.18			
17.1. The agency has considered advanced notification to the media.	p. 18			
17.2. The agency has considered acquiring credit monitoring services for the affected individuals. Note: This should only be considered when the incident involves Social Security number.	p. 19			
18. Notifying Others When Required	p. 19			
18.1. Notifying the California Attorney General and uploading a redacted copy of the notification to their website when the incident requires notification to 500 or more individuals.	p. 19			
18.2. Notifying the Credit Reporting Agencies when notification is made to 10,000 or more individuals.	p. 20			