Information Security and Privacy Incident Response Plan

Revision History

Date	Revision	Last Updated By	Change
02/05/2018	0.1	Mike Arakji	Initial Draft
03/26/2018	0.2	Mike Arakji	Added the following to Appendix I Incident Scenarios: Paragraph 2; a section for “General Scenario Questions”; and a section for “Scenarios”.
01/09/2019	1.0	Mike Arakji	Redacted Version
02/19/2021	1.1	Mike Arakji	Updated Appendix B

Table of Contents

1. Introduction

This is a security and privacy incident response plan for the Department of General Service (DGS) to effectively manage information security and privacy incidents and meet federal, state, and industry legal compliance requirements. The plan consists of several components, including federal and state policy directives and procedures as well as forms, samples, checklists, and instructions that are essential for effective security and privacy incident management. Incident scenarios will be added to the plan, in Appendix I, as part of testing to improve readiness. Implementation of the plan will enhance the department's Information Technology (IT) risk management capabilities and process maturity. When an information security or privacy incident is declared, DGS will follow the protocols detailed in this document.

2. Purpose

The more specific goal of the DGS Information Security and Privacy Incident Response Plan is to detect and react to IT security incidents, determine their scope and risk, respond to incidents, communicate the results and risk(s) involved to all stakeholders, and reduce the likelihood of incident recurrence.

3. Scope

The plan applies to all IT assets owned by, or in the custody of, DGS – including information systems, networks, information, and any person or device that gains access to DGS information systems, networks, and information.

4. Audience

This document has been created for authorized members of the DGS Security Incident Response Team (SIRT), the Chief Information Officer (CIO), the Chief Information Security and Privacy Officer (CISO/CPO), Privacy Coordinator, IT Management, Program Management, System and Network Administrators, security and privacy staff, technical support staff, and others who are responsible for responding to and managing security or privacy incidents.

5. Authority

The DGS Security Operations Center (SOC) is charged with executing this plan by virtue of its charter and various security and privacy policies mandated by federal and state laws, and policies (see Appendix A: References).

6. Maintenance

The DGS Chief Information Security and Privacy Officer (CISO/CPO) is responsible for the maintenance and revision of this document.

7. Expectations

It is expected that the Security Incident Response Team (SIRT), led by the Incident Commander (usually the CISO/CPO), will follow the guidance provided in this document to ensure they successfully manage, document, and close a security or privacy incident while minimizing the impact to DGS business operations, its employees, and any external entities that interact with DGS. In the case that a member of the SIRT is a person of interest in an incident, the CISO/CPO will assign another incident handler. In the case the CISO/CPO is a person of interest in an incident, the person with a higher rank and authority within DGS will delegate someone other than the CISO/CPO to act as the Incident Commander and recuse the CISO/CPO from all roles and responsibilities pertinent to the incident.

The SIRT is expected to follow the steps to be taken when managing a security or privacy incident, primarily:

- The phases and corresponding actions for managing an incident;
- How to document incident response efforts;
- How to communicate incident response status;
- How to handle incidents involving personal information; and
- How to report security incidents to the California Information Security Office (CISO) and California Highway patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC).

An outcome of implementing this plan should be a uniform, results-oriented approach to achieve an incident response maturity level that support the department's risk management continuous improvement efforts.

8. Escalation

The Incident Commander and Incident Communication Coordinator may find it necessary to escalate any issues regarding an incident response process or an actual incident. When that happens, they will consult with the DGS CISO/CPO, CIO, and Legal Counsel. An incident that requires notifications to the media should also involve DGS Public Information Officer and other department public officials. Escalation to external authorities will follow existing DGS escalation policy and process.

9. Testing and Training

The plan will be tested with a series of tabletop exercises throughout the year based on common and known scenarios involving sensitive departmental information and personal information (including notice-triggering PII/PHI/FTI) in order to identify the necessary improvements in the incident response plan itself and its implementation. Testing will also occur when significant changes are introduced to the department's IT infrastructure including decommissioning and replacement of mission critical business systems as well as security tools. Theoretical and practical testing will also serve as a means to sharpen the skills of incident handlers (the SIRT) and improve their response time in actual incidents. Tabletop exercises will at a minimum include the eleven (11) Incident Handling Scenarios detailed in NIST SP 800-61 (revision 2) Computer Security Incident Handling Guide (pages 52-57).

New SIRT members will be trained annually and upon hire on all technical and administrative aspects and developments in the field of security and privacy incident management. It is highly recommended for each SIRT member who is a permanent state worker to include security and privacy incident handling training in their annual Individual Development Plan (IDP) and equally recommended for managers to allocate appropriate funding for training in order to ensure successful and sustainable

implementation of the incident response plan. Additionally, the technical members of SIRT should include in their training building use cases based on legal compliance requirements and by viewing DGS environment from an attacker's perspective. Incident response readiness begins with understanding of legal compliance requirement, taking inventory of which assets to protect, and how best to protect them. But the best way to protect DGS assets is by identifying our weaknesses, thinking how they can be exploited, then building defenses accordingly. At a minimum the following use cases must be considered by the technical members of SIRT:

- Repeat attack from a single source.
- Repeat attack on a single ID.
- SMTP traffic from an unauthorized host.
- Antivirus failed to clean.
- Excessive SMTP traffic outbound.
- Excessive web or email traffic outbound.
- Excessive traffic inbound (streaming, web, etc.).
- Excessive access to a malicious website from a single internal source.
- Excessive connections to multiple hosts from a single host.
- Excessive exploit traffic from a single source.
- Excessive exploit traffic to a single destination.
- Excessive port blocking attempts from antivirus or other monitoring systems.
- Excessive scan timeouts from antivirus.
- Accessing a malicious website from multiple internal sources.
- Service account access to the Internet.
- Service account access to an unauthorized device.
- Scanning or probing by an unauthorized host.
- Scanning or probing during an unauthorized time window.
- Anomaly in DoS baselines.
- Anomaly in recon baselines.
- Anomaly in malware baselines.
- Anomaly in suspicious activity baselines.
- Anomaly in user access and authentication baselines.

- Anomaly in exploit baselines.
- Anomaly in network baselines.
- Anomaly in application baselines.
- Multiple logins from different locations.
- Multiple changes from administrative accounts.
- Multiple infected hosts detected on a subnet.
- Unauthorized user access to confidential data.
- Unauthorized subnet access to confidential data.
- Unauthorized user on the network.
- Unauthorized device on the network.
- Unauthorized server connection to the Internet.
- Suspicious traffic to known vulnerable host.
- Logging source stopped logging.
- Logs deleted from source.
- Device out of compliance (antivirus, patching, etc.).

10. Definitions

Information Security

The protection of information assets from a wide range of threats in order to provide for their confidentiality, integrity, and availability. Information security supports business continuity, minimizes business risk, and maximizes return on investments and business opportunities.

Privacy

The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Incident Response Plan

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber attacks against an organization’s information assets.

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that violates any DGS computing policy, standard, or code of conduct. Also, an incident includes any action that threatens the confidentiality, integrity, or availability of DGS information and/or information systems. DGS network or system/application vulnerabilities regardless of criticality may not be deemed as incidents if not yet exploited by a threat actor (they are merely risks that the DGS Chief Information Security Officer works to mitigate outside the SIRT).

Security Incident

An occurrence that actually or potentially jeopardizes the security objectives (i.e., the confidentiality, integrity, or availability) of an information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Privacy Incident

An incident involving the potential disclosure or non-consensual sharing of personal information such as a natural person's name, home address, email address, social security number, and phone number.

Breach

A privacy breach occurs when there is unauthorized access, collection, use or disclosure of personal information, particularly health information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation such as Health Insurance Portability and Accountability Act (HIPAA) of 1996. California Information Practices Act of 1977 (Civil Code Section 1798.82) defines a breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business". 45 C.F.R. Section 164.400 et seq. (HIPAA) defines a breach as the "acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which comprises the security or privacy of the PHI.

Not a Breach

1) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.

2) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed.

3) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

4) An unauthorized acquisition, access, use, or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Confidential

Information maintained by state agencies that are exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265)

or has restrictions on disclosure in accordance with other applicable state or federal laws.

Need-To-Know

A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

Personally Identifiable Information (PII)

PII is any information about an individual that could cause harm to such individual, such as medical, financial, employment or criminal records or other information, together with information that can be used to identify or trace an individual's identity, including any other personal information that is linked or linkable to that individual. PII includes any portion of a natural person's name, social security number, physical and email addresses, phone/fax numbers, financial information, and any other unique characteristic that identifies the individual (see Appendix B for a larger List of Personal Information Identifiers). Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Individually Identifiable Health Information (IIHI)

IIHI is information collected from an individual that is created or received by a health care provider, employer, plan, or clearinghouse and relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and identifies the individual, or can reasonably be used to identify the individual.

Protected Health Information (PHI)

PHI is Individually Identifiable Health Information that is transmitted or maintained in any form or medium by a covered entity or Business Associate. Protected Health Information **excludes** individually identifiable health information when found:

(i) In education records covered by the Family Education Rights and Privacy Act (FERPA) (however, such information is considered confidential PII);

(ii) In employment records held by a covered entity in its role as employer (however, such information is considered confidential PII); and

(iii) Regarding a person who has been deceased for more than 50 years.

Notice Triggering Information

Specific items or personal information (name plus Social Security Number, driver's license/California identification card number, financial account number, medical information or health information) that may trigger a requirement to notify individuals if it is reasonably believed to have been acquired by an unauthorized person (details in CA Civil Code Section 1798.29) or information that is protected under the Family Educational Rights and Privacy Act (FERPA) which requires the agency or institution to maintain a record, with the other educational records of that individual, of each disclosure of PII from an educational record. 34 CFR 99.32(a)(1).

Unsecured Health Information

Health information not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the U.S. Department of Health and Human Services (HHS) in guidance.
Only encryption and destruction consistent with National Institute of Standards and Technology (NIST) guidelines renders health information unusable, unreadable, or indecipherable to unauthorized persons, in which case notification is not required in the event of a breach. [source: 45 C.F.R. §§ 164.400 – 160.414]

Process

A high-level sequence of activities and tasks to complete a function.

Procedure

A more detailed, step-by-step sequence of activities and tasks to complete a function. It is a specific series of actions that must be taken to implement policies or apply standards that helps the organization to meet its business and legal obligations such as becoming cost-effective, risk managed, and maintaining compliance with federal and state information security and privacy regulations.

Criminal Activity

Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. This includes unauthorized access, tampering, or damage to, and interference with, state owned or licensed physical and virtual IT assets (details in CA Penal Code Section 502).

11. Incident Management Lifecycle

The DGS information security and privacy incident management program consists of five (5) distinct phases with corresponding actions for managing an incident. An Incident Management Workflow (Appendix C) depicts a high level process of the SIRT activities throughout these phases.

11.1 Phase 1: Identification

The Identification phase of the incident management lifecycle is all about the detection and determination of whether an event of interest or abnormal activity is an actual security or privacy incident. It usually begins when someone internal or external to DGS reports the suspected activity or when DGS audit or monitoring efforts uncover unapproved deviation from normal data processing and/or normal behavior of information systems. This phase encompasses the following activities:

- Activate SIRT, establish incident command center, and designate incident commander. If two persons hold the title of Chief Information Security Officer and Chief Privacy Officer at the same time, both become incident co-commanders. In addition, at least two incident handlers must be available to handle an incident so that one can be the primary to identify and assess the incident while the other can help to gather evidence. Communication and coordination among members of the SIRT is critical specially where the scope of the incident involves a significant impact on business operations in terms of confidentiality, integrity, and availability of information and information systems. In his/her role as the central point of contact for all incident communications to SIRT members and all impacted parties, the Information Security & Privacy Incident Communications Commander (ICC) starts to communicate security or privacy incident details and instructions among the SIRT members.

- SIRT members start documenting all actions and relevant data points associated with their activities, i.e., everything that they are doing. Documents should be able to answer the Who, What, Where, Why, and How questions in case the documentation is to be used to prosecute the perpetrator(s) in court.
- Analyze alarms, error messages, log files, triggers, intrusion detection systems and firewalls for indicators of compromise on systems suspected of compromise, Identity and Access Management systems, and any other security systems.
- Determine incident type using the STRIDE Threat Model which identifies six threat categories: **S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege (refer to applying STRIDE methodology).
- SIRT members identify and classify incidents whether they are level 1, 2, or 3 (refer to Appendix E- Incident Identification and Classification for details of each classification level).
- Determine if notice triggering information is involved with incident (refer to section 19.3 of this document to assist in identifying notice triggering information and how to manage an incident that involves notice triggering information).
- CISO/CPO and ICC officially declare an incident once it has been determined that there was loss, damage, or misuse of information assets; or improper dissemination of DGS and/or State information.
- Initiate incident communication protocol outlined in the Incident Communication Plan, section 14 of this document.
- Identify any additional software, tools, and/or services necessary to complete investigation and/or analysis.
- Gather forensics evidence.
- Establish the Chain of Custody for forensics evidence preservation and protection.
- Notify the following entities in this order: DGS leadership, CHP ENTAC, and California Office of Information Security (OIS).
- If notice triggering data was compromised, work with privacy officer to initiate breach notification process.

- If a DGS employee or contractor is suspected of wrongdoing, work with DGS OHR and OBAS to address employee/contractor related issues.
- If criminal activity is suspected, contact CHP Emergency Notification and Tactical Alert Center (ENTAC) to address criminal aspect of incident response.

11.2 Phase 2: Containment

The purpose of this phase is to contain the damage and prevent it from spreading and making the situation worse. It is imperative for the SIRT to work with impacted program area stakeholders to develop an agreeable containment strategy and containment options which includes the timing and method of announcing system(s) shutdown or reduction/halt of operations. The Containment phase involves the following activities:

1) Short-term Containment – limit the damage as soon as possible. This could be any of the following non-long-term solutions or containment actions:
   - Isolate a network segment of infected nodes.
   - Turn off hacked production servers and routing traffic to failover servers.
   - Disable affected accounts or reset passwords.
   - Force firewall/IPS rules to prevent future infection or compromise.
2) System Back-up – It is critical that this step is done as follows:
   - First, take a forensic image of the affected system(s) with DGS approved forensic tools to capture the current state of the infected system(s).
   - Preserve and secure the forensic image to serve as: a) the means to provide the SIRT, during the Lessons Learned phase, a valuable insight into how the system(s) were compromised; b) evidence in case needed for disciplinary action against negligent or malicious employees; or c) evidence in criminal prosecution or civil liability litigation cases.
   - Then proceed to reimage or wipe clean any compromised system.
3) Long-term Containment –
   - Remove accounts and/or backdoors left by attackers on affected systems.
   - Install security patches on both affected and neighboring systems.
   - Limit any further escalation of the incident while allowing normal business operations to continue.

11.3 Phase 3: Eradication

The primary objective for this phase is to remove the threat or whatever caused a security or privacy incident (e.g., remove malicious or other illicit content from the affected systems with approved sanitization tools, remove the malicious intruder's access, terminate the insider threat's access, etc.). At a minimum, the following SIRT activities must take place:

- Scan affected systems and/or files with anti-malware software to ensure any latent malware is removed.
- Scan the Windows registry for keys that may initiate any latent malware.
- Remediate any vulnerabilities that were exploited.
- Remediate any account/privileges related issues or areas of concern.
- Remove malware, inappropriate materials, and other destructive/invasive components from **all** affected components.
- Determine if any system/data backups were made of compromised system(s) and then perform clean-up of such compromised system/data.
- Reconfigure security technical controls as needed to prevent recurrence.
- Rebuild systems from scratch if necessary.
- If reimaging system hard drives, use the most recent gold image or the original disk images that were created prior to system deployment into production to restore the system, then install the tested and approved patches that will bring the system up-to-date.
- Disable unused services to further harden the system against further attacks.

11.4 Phase 4: Recovery

The primary objective of this phase is to return the affected systems or environments to their normal state as before the incident took place, while making certain the recovery efforts will not lead to another incident. The SIRT is to prevent another incident from taking place due to the same problems that caused the one they just resolved. This phase involves the following activities:

- SIRT develops recovery options with a recommended recovery approach to provide to the stakeholders. Depending on the severity of compromise of the confidentiality, integrity, and/or availability of information and/or information systems, the recovery options may include activating the DGS Technical Recovery Plan (TRP) or specific sections of the TRP.
- SIRT leads or coordinates the recovery option authorized by the decision makers such as the Incident Commander, Chief Information Officer, top management of impacted program area(s), legal counsel(s).
- Restore any affected business operations. Examples include restoring to a known good state from known good backups, rebuild systems to known good state, and replace systems suspected of Root level infection (aka RootKit).
- Identify and document any additional steps necessary to complete the recovery effort after incident has been resolved; if required, submit change tickets to schedule work required to complete the recovery phase.
- Notify all stakeholders and affected parties that recovery has been completed and business can return to normal operations.
- Incident Commander declares incident as resolved and completes Incident Report to submit it via CalCISR (or manually to CHP ENTAC and CISO should the online CalCISR system be down).
- ICC communicates the incident resolution to affected parties and stakeholders.

11.5 Phase 5: Lessons Learned

This is the last and most important phase in the incident response lifecycle because it is serves not only to measure the incident response effectiveness and inform management but also to leverage the lessons learned as input for the continuous improvement of the DGS risk, security, privacy, and compliance management programs. Documentation of the lessons learned will serve to benefit the department as training materials for new SIRT members, as reference materials in the event of a similar incident, and a benchmark to compare to future crises. At a minimum, the following activities must take place:

- SIRT, stakeholders, and affected parties meet within two weeks after the incident to discuss what worked and what areas need improvement (including response time, quality, and cost).
- SIRT develops a PowerPoint presentation summarizing:
    - When and by whom the problem was first detected,
    - The nature and scope of the incident,
    - How it was contained and eradicated,
    - What high-level steps were taken during recovery?
    - Areas of success and areas flagged for improvement.
- Incident Commander develops a “confidential” Plan of Action with Milestones (POAM) to implement the lessons learned.
- ICC publishes a “confidential” report in an executive summary format for DGS risk, security, privacy, and compliance managers.
- Information Security and Privacy officers will merge the incident response POAM items with their current POAMs due for periodic reporting to agencies of control such as CDT and CalOHII as well as other impacted BA or CEs (if any).

12. Incident Handlers Checklist

The following is a checklist of a series of questions for the SIRT to methodically perform their incident response roles and responsibilities.

1. Preparation

a. Are all members aware of the security policies of the department?

b. Do all members of the Computer Incident Response Team know whom to contact?

c. Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?

d. Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?

2. Identification

a. Where did the incident occur?

b. Who reported or discovered the incident?

c. How was it discovered?

d. Are there any other areas that have been compromised by the incident? If so what are

they and when were they discovered?

e. What is the scope of the impact?

f. What is the business impact?

g. Have the source(s) of the incident been located? If so, where, when, and what are they?

3. Containment

a. Short-term containment

i. Can the problem be isolated?

1. If so, then proceed to isolate the affected systems.
2. If not, then work with system owners and/or managers to determine further action necessary to contain the problem.

ii. Are all affected systems isolated from non-affected systems?

1. If so, then continue to the next step.
2. If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.

b. System-backup

i. Have forensic copies of affected systems been created for further analysis?

ii. Have all commands and other documentation since the incident has occurred been kept up to date so far?

1. If not, document all actions taken as soon as possible to ensure all evidence is retained for either prosecution and/or lessons learned.
2. Are the forensic copies stored in a secure location?

a. If so, then continue onto the next step.

b. If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.

c. Long-term containment

i. If the system can be taken offline, then proceed to the Eradication phase.

ii. If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

4. Eradication

a. If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?

i. If not, then please state why?

b. Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?

i. If not, then please explain why?

5. Recovery

a. Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?

b. What day and time would be feasible to restore the affected systems back into production?

c. What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?

d. How long are you planning to monitor the restored systems and what are you going to look for?

e. Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

6. Lessons Learned

a. Has all necessary documentation from the incident been written?

i. If so, then generate the incident response report for the lessons learned meeting.

ii. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.

b. Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?

c. Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?

i. If not, then please explain why and when is the next convenient time to hold it?

d. Lessons Learned Meeting

i. Review the incident response process of the incident that had occurred with all SIRT members.

ii. Did the meeting discuss any mistake or areas where the response process could have been handled better?

1. If no such conversations occurred, then please explain why?

13. Incident Management Documentation

Documentation is critical in that it may be needed as evidence for prosecuting criminal acts and bring suspect(s) to justice. Documentation is also necessary for lessons learned for the SIRT and the entire department. The following information is required for the documentation of all incidents.

- How was the security event/incident identified?
- Type of incident:
    - Spoofing
    - Tampering
    - Repudiation
    - Information disclosure
    - Denial of service
    - Elevation of privilege
- Who identified the event/incident?
- What time was the event/incident identified?
- When was the ISO notified?
- How was the ISO notified? (ticket, call, in person, email, text, etc.)
- Who participated in the SIRT?
- When and how the notification was made to CHP ENTAC?
- Was notice triggering information involved in the incident?
    - If so, what type of notice triggering data?
    - How many records?
- ID(s)/IP(s) of compromised/infected/affected system(s).
- ID(s)/IP(s) of suspected or confirmed source of incident (i.e. what system is causing the incident).

- What authorized accounts were used as part of the incident response?
- What actions taken, approximate times actions were taken as part of the incident response?
- Start and completion demarcations for phase transitions (e.g. transition from containment to eradication phase).
- Quantification of the incident's impact.
- When was the incident resolved?
- Estimated outage time frames for any affected systems and/or user.
- Retain evidence and chain of custody.

14. Incident Communications Plan

Any oral and written communication about a security or privacy incident throughout all phases of the incident management lifecycle is confidential and the minimum information necessary is shared on a need to know basis as determined by the Incident Commander, except among the SIRT members involved in responding to the current incident. Only the Incident Commander and the Incident Communication Coordinator are allowed to speak for the SIRT to any others within DGS. Any communication to parties external to DGS must not take place before the specific communication is reviewed and approved by representatives of the DGS executives, including legal counsel(s). Timely and accurate communication of incident response status is imperative for successfully managing a security incident. The Incident Communication Coordinator is responsible for managing the incident status communications to all affected parties and/or stakeholders. The Incident Communication Coordinator will be designated by the Incident Commander when the SIRT is convened to perform incident response. Communications will be consistent throughout all phases of the incident to ensure everyone has a baseline understanding of the incident and related activities.

Communication Source: The primary authoritative source for incident response communication activities is the SIRT's Incident Communication Coordinator. However, when this person is unavailable, such responsibility reverts back to the person ultimately

responsible, i.e., DGS Chief Information Security and Privacy Officer (CISO/CPO) acting as the Incident Commander.

Communication Audience: Incident response related communications will be distributed to SIRT members, affected parties, and decision makers. The Incident Communication Coordinator acts as the hub for the flow of information among the SIRT, but he/she is the primary communication channel outside the SIRT. The Incident Commander can play the role of the Incident Communication Coordinator is he/she chooses or when the latter is absent.

Communication Method(s): Email is the primary communication method for any incident response related communications. When appropriate the Incident Communication Coordinator will call or conduct face to face meetings with incident response participants, affected parties, and/or decision makers. Any phone or face to face based communications will be captured in the incident notes and when appropriate the content of those conversations will be captured in the general, email based incident status communications. If email is unavailable or potentially compromised the SIRT will leverage land line telephones, mobile phones, conference bridges, and/or SMS text messaging. The Incident Commander will make the decision if and when to discontinue the use of email and use an alternate communication medium for incident response related communications. The Incident Commander will instruct the SIRT on what communication medium should be used as part of the incident response effort. Only dgs.ca.gov domain is allowed for email communications (no copying anyone on their personal email accounts such as gmail, yahoo, and other non-DGS ISP. Only DGS issued or approved computing devices (laptops, smart phones, tablets, encrypted USB/flash drives, etc.) are allowed for any communications about the incident at hand. Any deviation from DGS Data Security policy and standards must be pre-approved by the DGS Chief Information Security Officer (no exceptions). All paper/electronic based written communications must bear a confidentiality disclaimer. All verbal communications must not begin before a verbal confidentiality disclaimer is agreed to by

the parties receiving confidential information. No discussions of any incident shall occur in hallways, elevators, or within ear shot of those not involved in the incident response.

Communication Timing: The Incident Communication Coordinator will distribute incident response status communications via email every hour at the top of the hour. Even if there is nothing new to report, communications will be sent stating there is no new information. When warranted, the Incident Communication Coordinator will distribute additional communications but at a minimum SIRT members, affected parties, and decision makers will be updated on an hourly basis. The communication timing for reporting incident information outside DGS depends on variable requirements depending on the type and size of incident described in subsequent sections of this document.

15. Security Incident Response Team

The SIRT is a cross functional group that varies based on the severity of the incident as well as the phase of the incident. The cross functional team listed in Table 1 represents the core SIRT. Depending on the severity of the incident and/or the phase, some SIRT members may not participate in some or all of the phases. Any designated SIRT member must provide an alternate to contact should they be unavailable when DGS is responding to an incident. The SIRT team is identified in Section 16, Table 1 – SIRT Contact List and in Section 17.1, Table 2 – Incident Handling Roles and Responsibilities.

DGS Chief Information Security and Privacy Officer (CISO/CPO) will be the default Incident Commander and central point of contact for the management and reporting of all incident handling activities. As the Incident Commander, the CISO/CPO will conduct a preliminary investigation of the incidents and takes steps to activate the SIRT. He/she is ultimately responsible for the appropriate and timely notification to the appropriate persons when responding to an incident; however, he/she may designate a member of the SIRT to act as an Incident Communication Coordinator to assist with large scale incidents or breaches involving numerous reporting compliance requirements. The

Technical members of the SIRT should be selected with the following knowledge, skills, and abilities in mind:

- O/S proficiency
- Network protocols
- Platforms
- Directories
- Routers/switches/firewalls
- IPS/IDS
- Databases
- Applications
- Policies
- Investigative processes
- Chain of custody
- Forensics
- Attacks
- Ethics
- Programming
- Extreme curiosity
- Abstract thinking
- Critical thinking
- Correlate events, incidents, and alerts in real time
- Communicate to various groups that have different requirements
- Respond well to frustrating situations

16. SIRT Contact List

Contact information are reviewed for necessary updates on a quarterly basis. Physical and electronic contact lists will be distributed to everyone on the list in the following table upon each review that results in an update. Please note that the SIRT list in publication at the time of reporting an incident will be used as an attachment to the incident report for DGS stakeholders (per RACI chart) to serve as a documentation of who was involved in the incident response and to report on effectiveness of response per NIST SP 800-53 Rev.4 Control SE-2: Privacy Incident Response. Hence, each incident

report may not reflect an updated SIRT Contact List, which serves purposes of internal controls and future audits or investigations.

Table 1: SIRT Contact List **<This is a sample table; It must be modified to suit C2C>**

DGS Division / Office	Title	Contact	Main Phone No. / Alternate Phone No.	Backup	Phone
ADMIN / ETS	Information Security & Privacy Officer (ISO/PO)				
ADMIN / ETS	Chief Information Officer (CIO)				
ADMIN / ETS	Privacy Coordinator				
EXEC / OPA	Public Information Officer				
EXEC / OLS	Legal Counsel				
ADMIN / OHR	Human Resources				
ADMIN / ETS	Forensic Evidence Collection				
ADMIN / ETS	Infrastructure Representative				
ADMIN / ETS	Platform Representative				
ADMIN / ETS	Application Representative				
RESD / AMB	Physical Security				
ADMIN / OBAS	Integration Partner/Contractor or Procurement Officer				
ADMIN / ETS	Incident Communications Coordinator (ICC)				

17. Response Actions for Information Security or Privacy Incidents

In this section we prescribe actions for certain roles in incident response efforts. These actions are not meant to be overly specific but instead provide the high level objective/task and it is expected the person with the designated role will possess sufficient skills and experience to fill in blanks as required.

17.1 Table 2: Incident handling roles and responsibilities <Must modify for C2C>

Organization	Title/Role	Responsibility
DGS ETS	Information Security and Privacy Officer (ISO/PO)	• Acts as the Incident Commander. When the ISO/PO is no longer the same person, both of the Chief Information Security Officer and Privacy Officer will act as co-commanders for privacy incidents. For merely security incidents, the Chief Information Security and Privacy Officer will act as the Incident Commander in charge of the SIRT. • Initiates security incident response process by contacting all SIRT members, assigning action items, and establishing status update and communications protocols • Officially declares an incident once it has been determined that there was loss, damage, or misuse of information assets; or improper dissemination of DGS and/or State information • Creates and owns the containment plan • Assigns an incident scribe to document the incident management actions • Assigns Incident Communications Coordinator • Leveraging SIMM 5340-C as a guide, works with DGS Legal Team to determine/declare if the incident is standard, "notice triggering," or a privacy breach. • Works with affected parties and stakeholders to determine the frequency and timing of incident status communications • Manages the incident through closure

Organization	Title/Role	Responsibility
DGS	Privacy Officer or Designee	• Works with CISO/CPO to determine if the breach includes notice triggering information • If notice triggering data is breached, he/she is accountable for managing the breach notifications to affected parties • Works with CISO/CPO and Legal team to prepare and deliver breach notifications • Serves as the back up and representative of CISO/CPO before DGS executive management team
DGS ETS	Privacy Coordinator	• Assists the CISO/CPO with all aspects of privacy related incident handling.
DGS ETS	Incident Communication Coordinator (ICC)	• Communicates security/privacy incident details and instructions among the SIRT and impacted parties throughout the lifecycle of the incident.
DGS ETS	Technology Team	• Analyzes health, security, and audit log information to estimate size and scope of breach • Assigns SMEs to participate in tactical incident response; SMEs may be needed for some or all of the following areas: o Networking (LAN/WAN/WLAN) o Operating Systems (Windows, Linux, Unix) o Application Development and Support (Enterprise & LOB applications) o Database o End Points/Workstation Support • State Technology Managers are responsible for managing and communicating with any external service providers that are under their management that may be required to participate in the incident response
DGS ETS	Chief Information Officer (CIO)	• Participates in status communications as warranted • Reviews and approves the security incident report prior to being release to external entities (State OIS and CHP ENTAC)

Organization	Title/Role	Responsibility
		• Facilitates communications to local, state, or federal partners
DGS Other	Impacted Program Manager	• Participates in incident response activities as warranted
DGS	Public Information Officer or Communications Officer	• Responsible for managing any/all communications to external entities affected by the breach • If applicable, responsible for responding to public demands for information and status
DGS	Legal Counsel	• If notice triggering/protected data is potentially involved, initiate process for breach disclosure/notification • Assists in preparing breach notification
DGS	Personnel Officer or Human Resource Manager	• Addresses any employee discipline issues if employee wrong doing is discovered
DGS	Forensic Evidence Collection SME	• Determines if SIRT possess all tools and technology required to appropriate obtain and preserve forensic evidence
DGS	Physical Security/Building-Facility Management	• Participates in response activities if required
ETS	Technology Team	• Under the direction of CISO/CPO, Incident Commander, or DGS technology managers, provides data as requested • Reviews systems under ETS management for Indicators of Compromise and report to the DGS ISO or Incident Commander • Assists in incident identification, containment, eradication, and restoration activities as directed by DGS ISO, Incident Commander, or technology managers

18. Incident Reporting for Lost or Misused IT Assets

In addition to responding to exposure of sensitive information, whether personal or not, the SIRT will report, within 24 hours of discovery, a loss or misuse of IT assets such as laptop computers and other computing devices to CHP, using Report of Crime on State Property, STD. 99 (see Appendix H). The SIRT may also need to complete Property Survey Report, STD. 152.

These criteria for reporting such incidents include one or more of the following:

- When there is a violation of law (see Penal Code Section 502, subsection (c));
- Any incident that results in a loss costing more than $5,000.00;
- Any incidents involving the accessing or storing of inappropriate material.

The SIRT Incident Commander or Incident Communication Coordinator will also report such incidents to CHP and the California Office of Information Security (OIS), using the Cal-CSIRS system at https://calcsirs.rsam.com/. Reporting must not be delayed until all information is gathered and it must include as much information as possible at the time of becoming aware of incidents. The following information will be needed before filing a report in CalCSIRS:

- Name and address of the reporting entity.
- Name, address, e-mail address, and phone number(s) of the reporting person (Incident Commander or Incident Communication Coordinator).
- Name, address, e-mail address, and phone number(s) of the DGS CISO/CPO.
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate CISO/CPO, system administrator, etc.).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Any actions at and following the time of discovery that were taken prior to reporting incident on Cal-CSIRS.

The Incident Commander or Communication Coordinator should attempt to gather the following additional information before reporting incident about incidents involving computer-related theft or crime:

- Make / model of the affected computer(s).
- Serial and state asset identification numbers of affected devices.
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating system of the affected computer(s).
- Location of the affected computer(s).

19. Incident Reporting for non-Personally Identifiable Information

Beyond communicating incident impact and status to stakeholders and SIRT members, DGS CISO/CPO is responsible for reporting the incident to CHP ENTAC even if it does not involve Personally Identifiable information (PII). Security and privacy incidents must be reported using the California Compliance and Security Incident Reporting System (Cal-CSIRS). As required in SIMM 5340-C (March 2017), a report made to CHP, other law enforcement agencies, or the California Office of Information Security (OIS) outside of the Cal-CSIRS notification process by email or other means is NOT an acceptable substitute for the required report through Cal- CSIRS.

In the case that the Cal-CSIRS system is offline during normal business hours, contact CISO directly by phone at (916) 445-5239 or by e-mail at security@state.ca.gov for assistance. If the Cal-CSIRS system is offline outside of normal business hours and you require immediate law enforcement assistance, contact CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will forward that information to Computer Crimes Investigations Unit (CCIU) for immediate assistance. In the situation that notification is made outside of
normal business hours through CHP, it is the state entity’s responsibility to notify OIS of incident the next business day.

The report will outline the details of the incident and corrective actions taken, or to be taken, to address the root cause of the incident. The report will be completed through Cal-CSIRS within 10 business days following creation of the incident. If corrective actions cannot be completed immediately, DGS will follow the instructions outlined in SIMM 5305-B to submit a Plan of Actions and Milestones (SIMM 5305-C) that identifies all corrective actions along with timelines indicating when these corrective actions will be completed. If the state entity currently has a POAM on file, you will need to update the existing POAM and resubmit.

Additionally, the SIRT will monitor changes made by the California Department of Technology OIS on its website https://cdt.ca.gov/security/ to ensure continued compliance with all updated requirements for incident management.

20. Security and Privacy Incident/Breach Reporting

All DGS Intranet and Internet web pages will include a link for reporting any suspicious security or privacy events or incidents. The form ISO-02 Security/Privacy Incident Report Form is currently located at http://documents.dgs.ca.gov/ISPO/forms/ISO-02%20Security%20and%20Privacy%20Incident%20Report%20Form.pdf but will also be located within a new non-confidential Security and Privacy Incident Response Plan that consists of a summary of this detailed confidential plan intended for the SIRT. When an incident does not involve personal information, that is, it involves sensitive information, as defined in SIMM 5305-A, that pertain to confidential records of state entity financial transactions and regulatory actions, the SIRT at DGS will be activated to follow the processes and actions outlined earlier in the five phases of the Incident Management Lifecycle, Incident Management Documentation, and Incident Communication Plan. An example of sensitive non-personal information is a Budget Change Proposal (BCP) of a state entity until the annual budget is signed by the state Governor and released to the public.

For incidents involving personal information (PII, Notice Triggering PII/PHI, and FTI), state and federal laws have specific requirements for managing them. The Incident

Commander will work with the SIRT comprised of Security and/ or Privacy teams to determine if the information associated with the breach is in fact standard PII, notice triggering PII/PHI or FTI. The incident management process will follow accordingly.

20.1 Requirements for Breach Notification

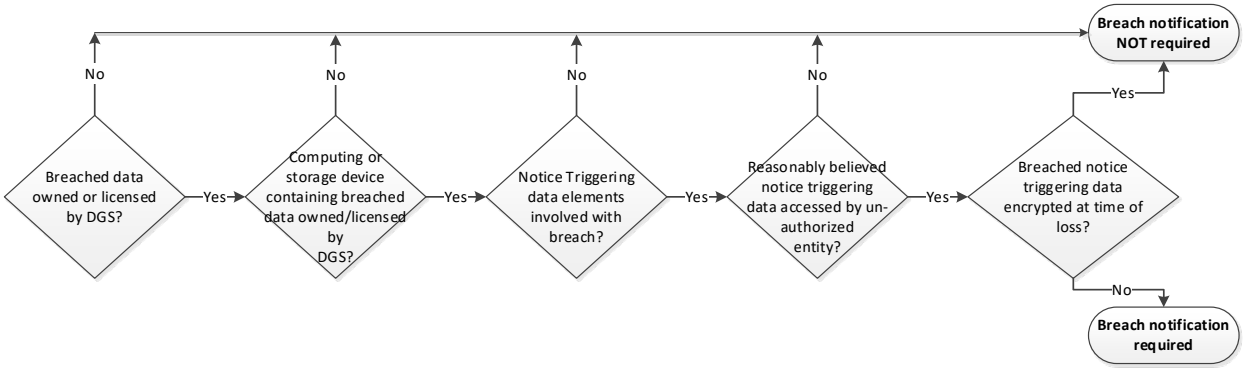
When determining whether or not an unauthorized acquisition of information has actually or is reasonably believed to have occurred, the Incident Commander -- working with the SIRT members -- will consider the following indicators:

a. 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. This includes, but is not limited to, documents containing notice-triggering data elements which have been addressed and mailed to an unauthorized person, transmitted by facsimile to an unauthorized person, or information containing notice-triggering data elements which is otherwise conveyed, such as by word-of-mouth, to unauthorized persons.

b. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.

c. 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.

The following decision tree helps to determine if breach notification is required.



20.2 Incidents involving Standard PII

Both the state and federal governments have specific requirements for notifying individuals affected by a breach of personal information, aka Personally Identifiable Information (PII), depending on the type of personal information and the magnitude of the breach. The federal HIPAA Privacy Rule and the state Information Practices Act (California's Civil Code Sections 1798.29 and 1798.82) require breach notifications to be provided to certain parties, within specific time frames, in a specific format, and include certain content. In addition, the Family Educational Rights and Privacy Act (FERPA) requires the agency or institution to maintain a record, with the other educational records of that individual, of each disclosure of PII from an educational record. 34 CFR 99.32(a)(1). The reporting procedures in this plan conform to these requirements and any others outlined in SAM 5340.4 Incident Reporting, SIMM 5340-A Incident Reporting and Response Instructions.

For suspected or confirmed incidents involving standard PII (non-notice triggering), the SIRT Incident Commander or Incident Communications Coordinator will notify OIS using the secure online reporting at https://calcsirs.rsam.com/default.aspx (aka Cal-CSIRS) within 10 days of incident discovery date.

20.3 Incidents Involving Notice Triggering PII

The SIRT will follow the same process for reporting suspected or confirmed notice-triggering PII incidents as non-notice triggering PII incidents; however, confirmed incidents warrant additional steps because federal and state laws require notifications to the affected individuals and/or the maintenance of a record, with the other educational records of that individual, of each disclosure of PII from an educational record. 34 CFR 99.32(a)(1). When the SIRT determines a notice should be made to individuals affected by a breach of their personal information and/or the maintenance of a record of the unauthorized disclosure in the individual's file, as in an instance of breach of unencrypted notice-triggering PII, the SIRT Incident commander and Incident Communication Coordinator will collaborate with the DGS Legal Counsel permanent member of the SIRT to draft a breach notice and upload it to the incident report through Cal-CSIRS for the California Office of Information Security (OIS) Program Manager to

review and approve. No breach notification shall be released to affected individuals or maintained in the file relating to the individual before the review and approval of the OIS (refer to SIMM 5340-C).

It is important to recognize that Notice-triggering PII may include PHI, whenever the PII is related or associated with a past or present medical transaction or health condition.

Notice Triggering information is defined in Civil Code Section 1798.29 as an individual's first name or first initial and last name in combination with **any one or more** of the following personal information identifiers:

- Social Security Number.
- California Driver's License Number or California ID Number.
- Credit or Debit Card Number in combination with any Security Code, PIN/Access Code, or Password that would allow access to an individual person's financial account.
- Past or present physical or mental health condition of an individual.
- Medical Record Number or health insurance plan identification number.
- Any other Individually Identifiable Health Information (IIHI).

Also, a user name or email address, in combination with a password or security question and answer that would permit access to an online account may trigger a requirement to notify individuals if it is reasonably believed to have been acquired by an unauthorized person user or a process acting on behalf of a person user.

20.4 Incidents/breaches involving PHI

The following are incident response policy directives and procedures requirements that align with the DGS Incident Management Lifecycle (Section 11 of this document) but contain additional or more specific incident response and reporting instructions for the SIRT to follow based on State Health Information Policy Manual (SHIPM). When an incident involving PHI is suspected or reported to the SIRT, the SIRT will be activated to investigate if the personal information identifiers involved are PHI and whether the incident qualifies as a 'Breach' or "Not a Breach". If a suspicion or claim of a breach incident is confirmed, the SIRT will mitigate and report on it expeditiously. The SIRT is

required to notify affected individuals, document corrective actions, and submit reports to oversight entities specified in this section.

What is covered:

PHI or individually-identifiable health information that is transmitted or maintained in electronic media or any other form or media. It includes any information, oral or recorded in any form or medium, relating to the current or past physical or mental health or condition of an individual, the health care provided, or payment for health care provided (except for persons deceased for more than 50 years). It is the unencrypted computerized data containing an individual's first name or first initial and last name in combination with:

1. Social Security Number (SSN);
2. Driver's license number or California identification card number;
3. Account number, 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;
4. Medical information; or
5. Health insurance information, including health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Exceptions:

I. Good faith acquisition of personal information by an employee or agent for business purposes is not a breach if no further use/disclosure (Civil Code Section 1798.82). Also a breach does not include the following per HIPAA Privacy Rule:

1. Unintentional acquisition, access, or use of PHI by authorized person if made in good faith within scope of authority and no further use/disclosure in a manner not permitted by Privacy Rule.

2. Inadvertent disclosure by authorized person to another authorized person at same covered entity (CE) or business associate (BA) or organized health care arrangement, and no further use/ disclosure in a manner not permitted by Privacy Rule.

3. Disclosure where CE or BA has good faith belief that the recipient would not reasonably have been able to retain the information.

4. The "incidental disclosure," defined as: a use/disclosure "incident to" an otherwise permissible use/disclosure that occurs despite reasonable safeguards and proper minimum necessary procedures. (See Appendix G: Incidental Uses and Disclosures 45 C.F.R. Section 164.502(a)(1)(iii).)

II. An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is a reportable breach, unless the covered entity demonstrates a low probability that the PHI has been compromised based on a risk assessment of the following four factors, plus any other relevant factors:

1. The nature/extent of the PHI involved, including types of identifiers and the likelihood of re-identification.

2. The unauthorized person who used the PHI or to whom the disclosure was made.

3. Whether the PHI was actually acquired or viewed.

4. The extent to which the risk to the PHI was mitigated.

Who must be notified:

Civil Code Section 1798.29 (e) requires any state entity that is required to issue a security breach notification to more than 500 California residents, as a result of a single breach, to electronically submit a sample copy of the breach notification, excluding any personally identifiable information, to the Attorney General. The SIRT's Incident Commander or the Incident Communication Coordinator will upload notification to the AG, using www.oag.ca.gov/ecrime/databreach/report-a-breach.

HIPAA Privacy Rule requires notification to patients, the U.S. Department of Health and Human Services (DHHS), and the media if more than 500 residents of a state or

jurisdiction were affected. HIPAA Privacy Rule also requires that for breaches by a business associate or a subcontractor of a business associate, the subcontractor must notify the business associate, and the business associate must notify the covered entity of any breach. Once the covered entity is aware of the breach, it must report the breach as explained above. The covered entity is permitted, however, to coordinate with its business associate as to who will make the notification to patients. As a result, the business associate may make the patient notification, as agreed upon by the covered entity.

The SIRT's Incident Commander or the Incident Communication Coordinator will also report incidents involving Protected Health Information to the California Office of Health Information Integrity (CalOHII) at ohicomments@ohi.ca.gov and again annually to CalOHII, using the Annual Breach Reporting Form.

Time frame for notification:

In accordance with California Civil Code 1798.82, notification will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system. When notification to the individual subject of PHI breach is required, the SIRT Incident Commander or Incident Communication Coordinator will submit a draft notice to the OIS using CalCSIRS for review and approval prior to any release. The SIRT must meet the HIPAA notification time frame requirement without unreasonable delay and in no case later than 60 calendar days after discovery.

The same time frame holds true for reporting to U.S. DHHS if more than 500 patients affected. Smaller breaches will be submitted to U.S. DHHS via annual log each March 1 (February 29 in leap years). When notification to the media is required (i.e., where a single breach affect more than 500 California residents, the state budget allows, and the OIS Program Manager approves), the SIRT Incident Commander or Incident Communication Coordinator will make the notification via press release without

unreasonable delay and in no case later than 60 calendar days after discovery. Notification may be delayed or interrupted upon request from law enforcement.

Delays beyond the ten (10) business days required to report confirmed breaches (unauthorized access to notice-triggering PII) are allowed due to: 1) Legitimate needs of law enforcement, when notification would impede or compromise a criminal investigation, or pose other security concerns (refer to Civil Code Section 1798.29 (c)); and 2) DGS SIRT taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system, so that the harm of the initial incident is not compounded by premature announcement. For example, if a data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident (refer to Civil Code Section 1798.29 (a)). However, any decision to delay notification should be made by the Director of DGS, or the senior- level individual designated in writing by the Director of DGS as having authority to act on his/her behalf, and any delay should not exacerbate the risk of harm to any affected individual(s) (refer to SIMM 5340-C).

Medium of notice:

The SIRT will implement any of the following Civil Code Section1798.82 options for communicating a breach notice:

- Written notice (on paper) by first class U.S. mail to the last known address of the affected individual;
- Electronic notice in conformity with the federal E-SIGN Act; or

Substitute notice if the costs of providing notice will exceed $250,000 or if more than 500,000 consumers are affected, or if the business does not have sufficient contact information. Substitute notice consists of: E-mail notice with prior consent;

- Conspicuous posting on the website; and any other procedure in accordance with policy.

The format of notice per HIPAA requirement for notification to individual subjects of PHI breach is as follows:

- Written notice via first class U.S. Mail, or substitute notice, to affected individual or legal representative, or to next of kin if the individual is deceased for less than 50 years.
- May notify by phone if urgent (i.e., the SIRT suspects possible imminent misuse of breached PHI), but also need written notice. Substitute notice applies where there is insufficient or out-of-date contact information for affected individual(s). If fewer than 10 individuals in this category, the SIRT will use alternative form of written notice, phone, or other means. If more than 10 individuals, a website or media notice for 90 days will be published. The notice will include toll-free phone number for 90 days.
- A notice to U.S. DHHS Office for Civil Rights will be sent via website www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html .
- To media: Press release to prominent media outlets serving the state or jurisdiction where affected patients reside.

Content of notice:

As prescribed in California Civil Code Section 1798.82 and the U.S. HIPAA Privacy Rule, the content of the notification shall be written in plain language and translated as required under other applicable laws. The overall format of the notice shall call attention to the nature and significance of the information, titles and headings will be clear and conspicuously displayed as well the text of the notice must not be smaller than 10-point type. The notice shall include all of the following, to the extent possible, using the prescribed headings:

1. The notice must be on DGS approved letterhead and have a date.

2. The notice should be titled "**Notice of Data Breach**".

3. Using the title "**What Happened**", provide a brief description of what happened, including the date of the breach and the date of the discovery of the breach. If the date of the breach is unknown, use an estimated date or a date range within which the

breach occurred. It is essential to include whether the notification was delayed as a result of a law enforcement investigation.

4. Using the title "**What Information Was Involved**", provide a description of the types of unencrypted/unsecured health information involved in the breach (e.g., full name, SSN, date of birth, California driver's license or ID number, home address, diagnosis, disability code, account number, etc.).

5. Using the title "**What You Can Do**", provide advice on any steps individuals should take to protect themselves from potential harm resulting from the breach. Also, provide the toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a name and social security number, driver's license, or California identification card number.

6. Using the title "**What We Are Doing**", provide a brief description of what DGS is doing to investigate the breach, to mitigate harm to the patients/individuals, and to protect against further breaches.

7. Using the title "**Other Important Information**", provide additional information, such as the contact procedures for individuals to ask questions, or learn additional information, which shall include a toll-free telephone number, an email address, website, or street address.

20.5 Incidents involving FTI

The following are incident response policy directives and procedures requirements that align with the DGS Incident Management Lifecycle (Section 11 of this document) but contain additional or more specific incident response and reporting instructions for the SIRT to follow based on IRS Pub 1075 Section 10.0 Reporting Improper Inspections or Disclosures.

19.5.1 Incident Response Procedures

When the SIRT is activated, it conducts an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the SIRT must contact the U.S. Treasury Inspector General for Tax Administration (TIGTA) https://www.treasury.gov/tigta and the IRS Office of

Safeguards immediately (see 19.5.3 below). Incident response policies and procedures required in *IRS Pub 1075 Section 9.3.8, Incident Response* (Appendix F: IRS Defined NIST SP 800-53 Security Controls IR-1 through IR-9), must be used when responding to an identified unauthorized disclosure or data breach incident. The Incident Commander will coordinate appropriate follow-up actions required to be taken by DGS entities to ensure continued protection of FTI.

Once the incident has been addressed, SIRT will conduct a post-incident review as part of the Lessons Learned phase of incident management lifecycle to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors and data center employees, immediately.

19.5.2 Incident Response Notification to Impacted Individuals

Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon DGS' internal incident response policy since the FTI is within DGS' possession or control. However, DGS CISO/CPO (in case the Incident Commander is someone other than the CISO/CPO) must be informed of notification activities before considering release to impacted individuals and before pending media releases. CISO/CPO will decide if a threshold has been met for breach notification of FTI to impacted individuals, then work with SIRT legal member(s) to draft a notice of breach to upload to OIS via Cal-CSIRS for OIS Program Manager's review and approval. Note, as the ultimate authority, OIS may decide for DGS not to issue a notice of breach. Should this be the case, the IRS Notification Process will not be triggered.

19.5.3 IRS Notification Process

1) Immediately, but no later than 24 hours after identification of a possible issue involving FTI, notify TIGTA, first at the Local Field Division Office in San Francisco, phone number (213) 576-4147, asking for the special agent-in-charge. If unable to contact the local TIGTA Field Division, contact the Hotline Number (800) 589-3718.

2) Concurrent to notifying TIGTA, the Incident Communications Coordinator or the Incident Commander (if ICC is unavailable) at DGS must notify the Office of Safeguards by email to safeguardreports@irs.gov.

3) To notify the Office of Safeguards, DGS must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time the incident occurred
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)

4) Reports must be sent electronically and encrypted via IRS-approved encryption techniques. The following is an IRS approved protocol for transmitting electronic documentation:

- Compress files in .zip or .zipx formats.
- Encrypt the compressed file using Advanced Encryption Standard (AES).
- Use a strong 256-bit encryption key string.
- Ensure a strong password or pass phrase is generated to encrypt the file.

- Communicate the password or pass phrase with the Safeguards Office through a SEPARATE email or via a telephone call to your IRS contact person. Do NOT provide the password or pass phrase in the same email containing the encrypted attachment!
- Refer to DGS specific file compression software user guide for instructions on how to compress and encrypt files. Known products compatible with IRS include, but are not limited, to WinZip and SecureZip.
- Do Not include in the email message any sensitive information because only the attachment is encrypted.

5) Use the term data incident report in the subject line of the email.

6) Do not include any FTI in the data Incident report.

Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

DGS SIRT must cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

21. Notification to Credit Bureaus

The SIRT Incident Commander or Incident Communication Coordinator will contact all major credit bureaus before sending breach notification letters involving a breach of notice-triggering PII such as Social Security numbers, Dates of Birth, and/or California Driver's License/Identification numbers only in cases involving a large number of individuals - 10,000 or more. Breaches of a single account number or of medical or health insurance information alone do not necessitate notifying credit reporting agencies. The Incident Commander or Incident Communication Coordinator will begin to make arrangements with credit bureaus as follows:

• Experian: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.
• Equifax: Send an e-mail to businessrecordsecurity@equifax.com.
• TransUnion: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

22. Credit Monitoring

In response to a notice-triggering breach involving only Social Security numbers or California Driver’s License numbers or California Identification Card numbers, the SIRT will offer credit monitoring services to affected individuals regardless of the number of individuals, where the compromised information presents a risk of identity theft to commit financial crimes. DGS Chief Information Officer will work with the SIRT member from OBAS to make arrangements for procuring credit monitoring services. If a “free” mitigation product is offered, DGS will make sure the affected individuals are not automatically enrolled for a renewal at their own cost.

23. Notification to US-CERT

Per CalOHII SHIPM 3.1.2, covered entities should also report to the United States Computer Emergency Readiness Team (US-CERT) any suspicious activity, including cybersecurity incidents, cyber threat indicators and defensive measures, phishing incidents, malware, and software vulnerabilities (https://www.us-cert.gov/report).

24. Documentation Retention

DGS will retain breach policies and procedures documentation, as well as documentation related to any incident or breach investigations, including all work papers, notes, response forms, meeting minutes, risk assessments and results, notifications, reports made, and other items relevant to incident or breach investigations for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is later (refer to SHIPM 2.4.1 and 3.1.2 or 45 C.F.R. § 164.414(b), § 164.530(j), and 164.316(b)(2)(iii)).

25. Further Information

Further information on the DGS Information Security and Privacy Incident Response Plan and associated policies and procedures can be obtained from the DGS Security Operations Center dgsinfosec@dgs.ca.gov (916) 376-3940 707 Third Street, 3rd Floor, West Sacramento, CA 95605.

Appendix A: References

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA Omnibus Rule of 2012

HIPAA Security Rule

- 164.308 (a)(6) Incident Procedures,
- 164.308 (a)(1) Security Management Process Reg Review/ Risk Analysis,

HIPAA Privacy Rule

- 45 CFR Section 164.400
- 45 CFR Sec 164.410 Breach and Breach Notification
- 45 CFR Sec 164.414

NIST SP 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

- Incident Response (IR)
  - IR-1 Incident Response Policy and Procedures
  - IR-2 Incident Response Training
  - IR-3 Incident Response Testing
  - IR-4 Incident Handling
  - IR-5 Incident Monitoring
  - IR-6 Incident Reporting
  - IR-7 Incident Response Assistance
  - IR-8 Incident Response Plan
- Security (SE)
  - SE-2 Privacy Incident Response

NIST SP 800-61 Revision 2 Computer Security Incident Handling Guide

Internal Revenue Service (IRS) Publication 1075 Tax Information Security Guidelines for Federal, State, and Local Agencies – Safeguards for Protecting Federal Tax Returns and Return Information

- Section 9.3.8 Incident Response
- Section 10.3 Incident Response Procedures
- Section 10.4 Incident Response Notification to Impacted Individuals

IRS Publication 1075 *Tax Information Security Guidelines For Federal, State and Local Agencies* http://www.irs.gov/pub/irs-pdf/p1075.pdf

IRS Office of Safeguards Website https://www.irs.gov/privacy-disclosure/safeguards-program

California Information Practices Act of 1977 (Civil Code Sections 1798 et seq)

- 1798.21
- 1978.29
- 1798.82

State Administrative Manual (SAM) 5305 Information Security Program

SAM 5340 Information Security Incident Management

- SAM 5340.1 Incident Response Training
- SAM 5340.2 Incident Response Testing
- SAM 5340.3 Incident Handling
- SAM 5340.4 Incident Reporting

SIMM 5305-B Plan of Action and Milestones Instructions

SIMM 5305-C Plan of Action and Milestones Worksheet (XLSX)

SIMM 5340-A Incident Reporting and Response Instructions

SIMM 5340-C Requirements to Respond to Incidents Involving a Breach of Personal Information

Statewide Health Information Policy Manual (SHIPM) 2.4.1 Breach and Breach Notification

Statewide Health Information Policy Manual (SHIPM) (PDF version 6/2017)

SHIPM 2.4.1 Breach and Breach Notification

SHIPM 3.1.2 Incident Procedures

Appendix B: List of Personal Information Identifiers

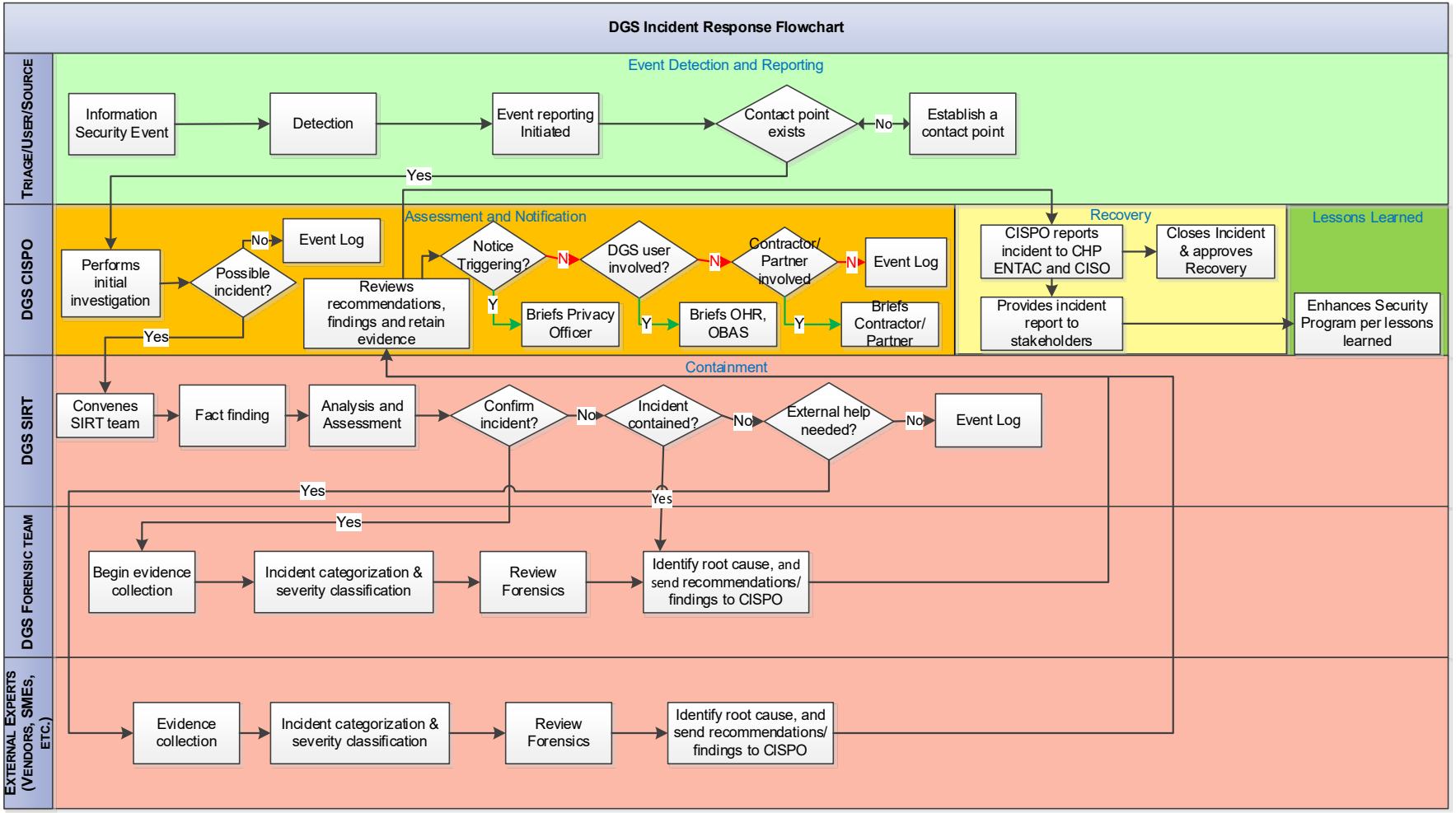
	List of Personal Information Identifiers	Notice Triggering	Comments
1	Full (or any combination of) Social Security Number (SSN)	Yes	When linked to either a name (or portion of a name) or a medical transaction. It is Federal Tax Information (FTI) if it comes directly from U.S. IRS.
2	Full date of birth (mm/dd/yyyy) or year of birth (yyyy)	Yes	When linked to a medical transaction and in combination of a first name, or first initial, and last name
3	Medical history	Yes	When in combination of a first name, or first initial, and last name
4	Past or current Physical health condition(s)	Yes	When in combination of a first name, or first initial, and last name
5	Past or current mental health condition(s)	Yes	When in combination of a first name, or first initial, and last name
6	Medical diagnostic codes	Yes	When in combination of a first name, or first initial, and last name
7	DNA sequence	Yes	When in combination of a first name, or first initial, and last name
8	Medical Record Number (MRN)	Yes	When in combination of a first name, or first initial, and last name
9	Health Plan Beneficiary Number	Yes	When in combination of a first name, or first initial, and last name
10	Full Name (or any combination of first, middle/middle initial, and Last)	Yes	When linked to a medical transaction and in combination of a first name, or first initial, and last name
11	Home phone number	Yes	When linked to a medical transaction and in combination of a first name, or first initial, and last name
12	Home fax number	Yes	When linked to a medical transaction and in combination of a first name, or first initial, and last name
13	Satellite phone number	Yes	When linked to a medical transaction and in combination of a first name, or first initial, and last name
14	Full home address	Yes	When linked to a medical transaction and in combination of a first name, or first initial, and last name
15	Banking account information (checking, saving, money market, other investment)	Yes	When linked to first name or initial plus last name and in combination with any required security code or password that would permit access to the individual's account
16	Credit/debit Primary Account Number (PAN)	Yes	When linked to first name or initial plus last name and in combination with any required security code or password that would permit access to the individual's account
17	Password for any online personal, financial, business, or social media accounts	Yes	When linked to first name or initial plus last name and in combination with any required security code or password that would permit access to the individual's account
18	Credit/debit card security verification number and expiration dates	Yes	When linked to first name or initial plus last name and in combination with any required security code or password that would permit access to the individual's account
19	Banking Personal Identification Number (PIN)	Yes	When linked to first name or initial plus last name and in combination with any required security code or password that would permit access to the individual's account

	List of Personal Information Identifiers	Notice Triggering	Comments
20	Security questions for access to personal, financial, business, or social media accounts	Yes	When linked to first name or initial plus last name and in combination with any required security code or password that would permit access to the individual's account
21	Driver's license or California identification card number	Yes	When in combination of a first name, or first initial, and last name
22	Email address when in combination with a password or security question and answer that would permit access to the account	Yes	When in combination of a first name, or first initial, and last name
23	Personal income tax information	Yes	FTI if it comes directly from the IRS
24	Other government issued identification numbers (not just driver's license or state ID)	Yes	When in combination of a first name, or first initial, and last name
25	Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical or digital representation of biometric data	Yes	When in combination of a first name, or first initial, and last name
26	Mother's maiden name	No	
27	Computer IP address	No	
28	Computer MAC address	No	
29	Wireless Modem MAC address	No	
30	Computer password	No	
31	Wi-Fi password	No	
32	Employment history	No	
33	Maiden Name	No	
34	Name(s) or Number of children (i.e., how many children a person has)	No	
35	Child's footprint	No	
36	Gender of children	No	
37	Food or Drink dietary consumption records (which may identify a person's religion, body mass condition/index, or alcohol drinking habits)	No	
38	Full date of death	No	
39	Education	No	
40	Handwriting	No	

	List of Personal Information Identifiers	Notice Triggering	Comments
41	Height	No	
42	Weight	No	
43	Eye color	No	
44	Voice print	No	
45	Physical description (in words orphotographs)	No	
46	Sexual Orientation	No	
47	Gender/Trans-Gender	No	
48	Race	No	
49	Ethnicity	No	
50	Religion	No	
51	National origin	No	
52	Place of birth	No	
53	Scars	No	
54	Tattoos	No	
55	Gang affiliation	No	
56	Occupation	No	
57	Political affiliation or orientation	No	
58	Statements made by, or attributed to, the individual	No	
59	Device identifiers and serial numbers	No	
60	Information that reveals any network location or identity (Excluding any information manually submitted to a state agency by user, whether electronically or in written form, and information on or relating to individuals who are users serving in a business capacity such as business owners, officers, or principals of that business.)	No	

	List of Personal Information Identifiers	Notice Triggering	Comments
61	Vehicle License Plate Number obtained from Automated License Plate Recognition (ALPR) System	No	
62	Any unique number identifying a natural person	No	
63	Any unique symbol identifying a natural person	No	

Appendix C: Incident Management Workflow



Appendix D: Security and Privacy Incident Response and Breach Notification Policy

http://dgssp.dgs.ca.gov/sites/ETS/ETSISO/CDT%20Policies/Draft%20Incident%20Response%20and%20Breach%20Notification%20Policy.docx

Appendix E: Incident Identification and Classification

After receiving notification of a security incident, the SIRT reviews and assesses the incident and determine appropriate action by first classifying the incident based on the information gathered. The CISO/CPO has established the following incident classifications:

Level 1: An incident that has an immediate and/or potential ongoing negative impact to DGS information and/or resources. A Level 1 incident typically requires cooperation with executive ETS management and communication with Office of Legal Services (OLS). Characteristics of a Level 1 incident includes:

a. Loss of DGS information classified as confidential or personal;
b. Loss of DGS information classified as notice triggering. Notice triggering information is personal information specified in the Information Practices Act (IPA) that requires DGS to send a notification to affected parties when there is a breach;
c. Compromised information systems and/or operations;
d. Loss of DGS mission critical information systems;
e. Risk of potential financial loss; and/or
f. Risk of negative media exposure.
g. Notice-triggering security breaches as defined in SIMM-5340-A.

Level 2: An incident that involves or has potential for loss or destruction of resources that contain confidential or sensitive DGS information. A Level 2 incident typically involves incidents that have already occurred. Level 2 incidents include:

a. Theft or loss of IT or telecommunications equipment: USB drives, personal computers, laptops, cell phones, BlackBerrys, etc.;
b. Theft or loss of hard copy files;
c. Unauthorized destruction of electronic or hard copy files.

Level 3: An incident that involves policy violations, copyright infringements, or inappropriate use of DGS resources. A Level 3 incident should be reported to the ISO for a preliminary review of the event. The ISO will provide assistance on ways to

mitigate future incidents. Any personnel or office action is the responsibility of the office manager where the incident occurred or that supervises the offender.

Once the CISO/CPO classifies the incident, the procedures outlined in the DGS Security and Privacy Incident Response Plan are followed for documentation, investigation, mitigation, and reporting steps.

Appendix F: IRS Defined NIST SP 800-53 Security Controls IR-1 through IR-9

The following are security controls, with defined parameters, as mandated by IRS Pub 1075 Section 9.3.8 Incident Response. These incident response controls apply to both physical and information system security relative to the protection of FTI.

IR-1 Incident Response Policy and Procedures

DGS must:

a. Develop, document, and disseminate to designated agency officials:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls.

b. Review and update the current:

1. Incident response policy every three years.
2. Incident response procedures at least annually.

IR-2 Incident Response Training

DGS must train personnel with access to FTI, including contractors and data center employees if applicable, in their incident response roles on the information system and FTI. DGS must provide incident response training to information system users consistent with assigned roles and responsibilities:

a. Prior to assuming an incident response role or responsibility.

b. When required by information system changes.

c. Annually thereafter.

IR-3 Incident Response Testing

DGS entities entrusted with FTI must test the incident response capability at least annually.

a. DGS must perform tabletop exercises using scenarios that include a breach of FTI and should test the agency's incident response policies and procedures.
b. A subset of all employees and contractors with access to FTI must be included in table top exercises.
c. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

IR-4 Incident Handling

DGS must:
a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
b. Coordinate incident handling activities with contingency planning activities.
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises.
d. implement the resulting changes accordingly.

IR-5 Incident Monitoring

The agency must track and document all physical and information system security incidents potentially affecting the confidentiality of FTI.

IR-6 Incident Reporting

DGS must:
a. Require personnel to report suspected security incidents to internal agency incident response resources upon discovery of the incident.
b. Contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI *(see IRS Notification Process, section 19.5.3 of the plan document)*.

IR-7 Incident Response Assistance

DGS must provide an incident response support resource, integral to the agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IR-8 Incident Response Plan

DGS must:

a. Develop an incident response plan that:

1. Provides the agency with a roadmap for implementing its incident response capability.
2. Describes the structure of the incident response capability.
3. Provides a high-level approach for how the incident response capability fits into the overall agency.
4. Meets the unique requirements of the agency, which relate to mission, size, structure, and functions.
5. Defines reportable incidents.
6. Provides metrics for measuring the incident response capability within the agency.
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
8. Is reviewed and approved by designated agency officials.

b. Distribute copies of the incident response plan to authorized incident response personnel (DGS members of the SIRT).

c. Review the incident response plan at a minimum on an annual basis or as an after-action review.

d. Update the incident response plan to address system/agency changes or problems encountered during plan implementation, execution, or testing.

e. Communicate incident response plan changes to authorized incident response personnel.

f. Protect the incident response plan from unauthorized disclosure and modification.

IR-9 Information Spillage Response

DGS must respond to information spills by:

a. Identifying the specific information involved in the information system contamination.

b. Alerting authorized incident response personnel (DGS SIRT) of the information spill using a method of communication not associated with the spill.

c. Isolating the contaminated information system or system component.

d. Eradicating the information from the contaminated information system or component.

e. Identifying other information systems or system components that may have been subsequently contaminated.

Appendix G: Incidental Uses and Disclosures

Complete document is located at
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/incidentalu%26d.pdf

OCR HIPAA Privacy

December 3, 2002

INCIDENTAL USES AND DISCLOSURES
[*45 CFR 164.502(a)(1)(iii)*]

Background

Many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which individuals receive health care or other services from covered entities, the potential exists for an individual's health information to be disclosed incidentally. For example, a hospital visitor may overhear a provider's confidential conversation with another provider or a patient, or may glimpse a patient's information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices and, thus, does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

How the Rule Works

General Provision. The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied *reasonable safeguards* and implemented the *minimum necessary standard*, where applicable, with respect to the primary use or disclosure. See 45 CFR 164.502(a)(1)(iii). An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

Reasonable Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Appendix H: Report on Crime or Damage on State Property

The CHP State Security Division (SSD) coordinates the collection of crime and incident reports, via STD. 99, Report of Crimes on State Property Missing/Lost Property, for the Safety Service Program. Section 14613.7 of the Government Code requires state agencies to report all crimes and criminally caused property damage occurring on state owned or leased properties to the California Highway Patrol (CHP). The CHP is then required to compile all information received and report to the state Legislature when requested. The completed STD. 99's shall be forwarded to your local CHP office.
The Safety Service Program may be contacted via State Security Division at (916) 843-3230. https://www.chp.ca.gov/ProtectiveServicesDivisionSite/Documents/std_99.pdf

Appendix I: Incident Scenarios

Tabletop exercises will at a minimum include the eleven (11) Incident Handling Scenarios detailed in NIST SP 800-61 (revision 2) Computer Security Incident Handling Guide (pages 52-57). This appendix will be updated as more scenarios and use cases are developed by the SIRT.

The SIRT members are presented with a scenario and a list of related questions. The team then discusses each question and determines the most likely answer. The goal is to determine what the team would really do and to compare that with policies, procedures, and generally recommended practices to identify discrepancies or deficiencies. For example, the answer to one question may indicate that the response would be delayed because the team lacks a piece of software or because another team does not provide off-hours support.

General Scenario Questions

The following questions are applicable to almost any scenario. Each question is followed by a reference to the related section(s) of NIST SP 800-61 (revision 2) Computer Security Incident Handling Guide.

Preparation:

1. Would DGS consider this activity to be an incident? If so, which of DGS' policies does this activity violate? (Section 2.1)

2. What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact? (Section 3.1.2)

Detection and Analysis:

1. What precursors of the incident, if any, might DGS detect? Would any precursors cause DGS to take action before the incident occurred? (Sections 3.2.2, 3.2.3)

2. What indicators of the incident might DGS detect? Which indicators would cause someone to think that an incident might have occurred? (Sections 3.2.2, 3.2.3)

3. What additional tools might be needed to detect this particular incident? (Section 3.2.3)

4. How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process? (Section 3.2.4)

5. To which people and groups within DGS would the team report the incident? (Section 3.2.7)

6. How would the team prioritize the handling of this incident? (Section 3.2.6)

Containment, Eradication, and Recovery:

1. What strategy should DGS take to contain the incident? Why is this strategy preferable to others? (Section 3.3.1)

2. What could happen if the incident were not contained? (Section 3.3.1)

3. What additional tools might be needed to respond to this particular incident? (Sections 3.3.1, 3.3.4)

4. Which personnel would be involved in the containment, eradication, and/or recovery processes? (Sections 3.3.1, 3.3.4)

5. What sources of evidence, if any, should DGS acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained? (Sections 3.2.5, 3.3.2, 3.4.3)

Post-Incident Activity:

1. Who would attend the lessons learned meeting regarding this incident? (Section 3.4.1)

2. What could be done to prevent similar incidents from occurring in the future? (Section 3.1.2)

3. What could be done to improve detection of similar incidents? (Section 3.1.2)

Other Questions:

1. How many incident response team members would participate in handling this incident? (Section 2.4.3)

2. Besides the incident response team, what groups within DGS would be involved in handling this incident? (Section 2.4.4)

3. To which external parties would the team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why? (Section 2.3.2)

4. What other communications with external parties may occur? (Section 2.3.2)

5. What tools and resources would the team use in handling this incident? (Section 3.1.1)

6. What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)? (Section 2.4.2)

7. What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)? (Section 2.4.2)

Scenarios

Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)

On a Saturday afternoon, external users start having problems accessing DGS public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of DGS' networking staff responds to alerts from an Internet border router and determines that the DGS' Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the DGS' public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

The following are additional questions for this scenario:

1. Whom should the DGS contact regarding the external IP address in question?

2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?

3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

Scenario 2: Worm and Distributed Denial of Service (DDoS) Agent Infestation

On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. DGS has already incurred widespread infections before antivirus signatures become available several hours after the worm started to spread.

The following are additional questions for this scenario:

1. How would the incident response team identify all infected hosts?

2. How would DGS attempt to prevent the worm from entering DGS before antivirus signatures were released?

3. How would DGS attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?

4. Would DGS attempt to patch all vulnerable machines? If so, how would this be done?

5. How would the handling of this incident change if infected hosts that had received the DDoS agent had been configured to attack another DGS website the next morning?

6. How would the handling of this incident change if one or more of the infected hosts contained sensitive personally identifiable information regarding DGS employees?

7. How would the SIRT keep DGS users informed about the status of the incident?

8. What additional measures would the team perform for hosts that are not currently connected to the network (e.g., staff members on vacation, offsite employees who connect occasionally)?

Scenario 3: Stolen Documents

On a Monday morning, DGS Office of Legal Services (OLS) receives a call from the Federal Bureau of Investigation (FBI) regarding some suspicious activity involving DGS' systems. Later that day, an FBI agent meets with members of management and OLS to discuss the activity. The FBI has been investigating activity involving public posting of sensitive government documents, and some of the documents reportedly belong to DGS. The agent asks for DGS' assistance, and management asks for the incident response team's assistance in acquiring the necessary evidence to determine if these documents are legitimate or not and how they might have been leaked.

The following are additional questions for this scenario:

1. From what sources might the incident response team gather evidence?

2. What would the team do to keep the investigation confidential?

3. How would the handling of this incident change if the team identified an internal host responsible for the leaks?

4. How would the handling of this incident change if the team found a rootkit installed on the internal host responsible for the leaks?

Scenario 4: Compromised Database Server

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The SIRT investigation determines that the attacker successfully gained root access to the server six weeks ago.

The following are additional questions for this scenario:

1. What sources might the team use to determine when the compromise had occurred?

2. How would the handling of this incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?

3. How would the handling of this incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including PII) each night and transfer it to an external address?

4. How would the handling of this incident change if the team discovered a rootkit on the server?

Scenario 5: Unknown Exfiltration

On a Sunday night, one of DGS' network intrusion detection sensors alerted on anomalous outbound network activity involving large file transfers. The intrusion analyst reviews the alerts; it appears that thousands of .RAR files are being copied from an internal host to an external host, and the external host is located in another country. The analyst contacts the incident response team so that it can investigate the activity further. The team is unable to see what the .RAR files hold because their contents are encrypted. Analysis of the internal host containing the .RAR files shows signs of a bot installation.

The following are additional questions for this scenario:

1. How would the team determine what was most likely inside the .RAR files? Which other teams might assist the incident response team?

2. If the incident response team determined that the initial compromise had been performed through a wireless network card in the internal host, how would the team further investigate this activity?

3. If the incident response team determined that the internal host was being used to stage sensitive files from other hosts within the enterprise, how would the team further investigate this activity?

Scenario 6: Unauthorized Access to Payroll Records

On a Wednesday evening, DGS' physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The following are additional questions for this scenario:

1. How would the team determine what actions had been performed?

2. How would the handling of this incident differ if the payroll administrator had recognized the person leaving her office as a former payroll department employee?

3. How would the handling of this incident differ if the team had reason to believe that the person was a current employee?

4. How would the handling of this incident differ if the physical security team determined that the person had used social engineering techniques to gain physical access to the building?

5. How would the handling of this incident differ if logs from the previous week showed an unusually large number of failed remote login attempts using the payroll administrator's user ID?

6. How would the handling of this incident differ if the incident response team discovered that a keystroke logger was installed on the computer two weeks earlier?

Scenario 7: Disappearing Host

On a Thursday afternoon, a network intrusion detection sensor records vulnerability scanning activity directed at internal hosts that is being generated by an internal IP address. Because the intrusion detection analyst is unaware of any authorized, scheduled vulnerability scanning activity, she reports the activity to the incident

response team. When the team begins the analysis, it discovers that the activity has stopped and that there is no longer a host using the IP address.

The following are additional questions for this scenario:

1. What data sources might contain information regarding the identity of the vulnerability scanning host?

2. How would the team identify who had been performing the vulnerability scans?

3. How would the handling of this incident differ if the vulnerability scanning were directed at DGS's most critical hosts?

4. How would the handling of this incident differ if the vulnerability scanning were directed at external hosts?

5. How would the handling of this incident differ if the internal IP address was associated with DGS's wireless guest network?

6. How would the handling of this incident differ if the physical security staff discovered that someone had broken into the facility half an hour before the vulnerability scanning occurred?

Scenario 8: Telecommuting Compromise

On a Saturday night, network intrusion detection software records an inbound connection originating from a watch list IP address. The intrusion detection analyst determines that the connection is being made to DGS's VPN server and contacts the incident response team. The team reviews the intrusion detection, firewall, and VPN server logs and identifies the user ID that was authenticated for the session and the name of the user associated with the user ID.

The following are additional questions for this scenario:

1. What should the team's next step be (e.g., calling the user at home, disabling the user ID, disconnecting the VPN session)? Why should this step be performed first? What step should be performed second?

2. How would the handling of this incident differ if the external IP address belonged to an open proxy?

3. How would the handling of this incident differ if the ID had been used to initiate VPN connections from several external IP addresses without the knowledge of the user?

4. Suppose that the identified user's computer had become compromised by a game containing a Trojan horse that was downloaded by a family member. How would this affect evidence gathering and handling and analysis of the incident? What should the SIRT do in terms of eradicating the incident from the user's computer?

5. Suppose that the user installed antivirus software and determined that the Trojan horse had included a keystroke logger. How would this affect the handling of the incident? How would this affect the handling of the incident if the user were a system administrator? How would this affect the handling of the incident if the user were a high-ranking executive at DGS?

Scenario 9: Anonymous Threat

On a Thursday afternoon, DGS's physical security team receives a call from an IT manager, reporting that two of her employees just received anonymous threats against DGS systems. Based on an investigation, the team believes the threats should be taken seriously and notifies the appropriate internal teams, including SIRT, of the threats.

The following are additional questions for this scenario:

1. What should the incident response team do differently, if anything, in response to the notification of the threats?

2. What impact could heighten physical security controls have on the team's responses to incidents?

Scenario 10: Peer-to-Peer File Sharing

DGS prohibits the use of peer-to-peer file sharing services. DGS's network intrusion detection sensors have signatures enabled that can detect the usage of several popular

peer-to-peer file sharing services. On a Monday evening, an intrusion detection analyst notices that several file sharing alerts have occurred during the past three hours, all involving the same internal IP address.

1. What factors should be used to prioritize the handling of this incident (e.g., the apparent content of the files that are being shared)?

2. What privacy considerations may impact the handling of this incident?

3. How would the handling of this incident differ if the computer performing peer-to-peer file sharing also contains sensitive personally identifiable information?

Scenario 11: Unknown Wireless Access Point

On a Monday morning, DGS help desk receives calls from three users on the same floor of a building who state that they are having problems with their wireless access. A network administrator who is asked to assist in resolving the problem brings a laptop with wireless access to the users' floor. As he views his wireless networking configuration, he notices that there is a new access point listed as being available. He checks with his teammates and determines that this access point was not deployed by his team, which may indicate a rogue access point was installed.

1. What should be the first major step in handling this incident (e.g., physically finding the rogue access point, logically attaching to the access point)?

2. What is the fastest way to locate the access point? What is the most covert way to locate the access point?

3. How would the handling of this incident differ if the access point had been deployed by an external party (e.g., contractor) temporarily working at DGS?

4. How would the handling of this incident differ if an intrusion detection analyst reported signs of suspicious activity involving some of the workstations on the same floor of the building?

5. How would the handling of this incident differ if the access point had been removed while the team was still attempting to physically locate it?

Appendix J: Additional Provisions Applicable to Cradle to Career Data System

For purposes of security and privacy incidents relating to the Cradle to Career ("C2C") Data System the following definitions and provisions apply:

Privacy Incident

An incident involving the potential disclosure or non-consensual sharing of personal information or personally identifiable information (as defined in this Appendix J) such as a natural person's name, home address, email address, social security number, and phone number, or any other information from which an individual can be identified.

Security Incident

An occurrence that actually or potentially jeopardizes the security objectives (i.e., the confidentiality, integrity, or availability) of an information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of this Agreement, applicable laws, regulations, rules, security policies or standards, security procedures, or acceptable use policies.

Breach

A privacy breach occurs when there is unauthorized access, collection, use or disclosure of personal information, personally identifiable information, and/or protected health information. Such activity is "unauthorized" if it occurs in contravention of the C2C Data System Participation Agreement or applicable laws, regulations, rules, policies or standards, including, without limitation, applicable privacy legislation including, without limitation, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 or Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). California Information Practices Act of 1977 (Civil Code Section 1798.82) defines a breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business". 45 C.F.R. Section 164.400 et seq. (HIPAA) defines a breach as the "acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI.

Personally Identifiable Information

Personally Identifiable Information (PII) is information, in any medium (paper, electronic, orverbal) that alone, or in combination with other information, is linked or linkable to a specificindividual in a manner that would allow a reasonable person in the community to be able to identify that individual [1]with reasonable certainty.

PII includes, without limitation, the following whether in full or in variation:

- name, parent's name, mother's maiden name;
- social security number, driver's license number, student identification numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- home/mailing address, location of residence (including full zip code), telephone number, fax numbers, email addresses;
- financial matters[2];
- employment history;
- enrollment and education status[3];
- medical insurance policy number;
- Protected Health Information (PHI)[4],
- device identifiers and serial numbers, Web Universal Resource Locators (URLs),Internet Protocol (IP) addresses;
- personal characteristics that describe an individual (e.g., age, gender, race, ethnicity,language spoken, physical description, sexual orientation, gender identity);
- biometric identifiers, including finger and voice prints, full-face photographs and anycomparable images;
- all elements of dates (except year) for dates that are directly related to an individual,including birth date, admission date, discharge date, death date, and all ages over 89and all elements of dates (including year) indicative of such age;
- any other unique identifying number, characteristic, or code linked or linkable to anindividual; and
- Information that is subject to protection under any California or federal statute or regulation because it is personally identifiable, as such statute or regulation may beinterpreted by the agency responsible for its implementation or by any judicial opinion issued by a court of competent jurisdiction.

[1] "Physical description" comes from Government Code section 11015.5(d)(1). It can mean race/ethnicity and it canalso mean an actual description such as height, weight, tattoos, eye color, etc.

[2] "Financial matters" comes from Government Code section 11015.5(d)(1). This would usually be related to bankaccount number, payment amounts, security codes, income.
[3] "Education" comes from section Government Code section 11015.5(d)(1).
[4] Protected Health Information has the meaning defined in 45 C.F.R. § 160.103.

SIRT Contact List

The SIRT Contact List includes the Information Security Officer of the entity that provided the data to the C2C System that is the subject of a privacy incident and/or any other designee identified by that data provider. The role of the data provider Information Security Officer and/or designee shall include, without limitation, working with DGS regarding: (1) whether breach notification or maintenance of an individual-level record of the incident is required and (2) the contents of any communications, external to the SIRT members, relating to the incident. Data providers whose C2C System data is the subject of a privacy incident shall have access to all documentation relating to the incident including, without limitation, the Plan of Action with Milestones (POAM) to implement the lessons learned and executive summary reports.

Notice Triggering Information

In addition to the categories described in the Plan, "Notice Triggering Information" also includes personally identifiable information (PII) in education records even though such notice may involve maintaining a record of the unauthorized disclosure in lieu of, or in addition to, notice to the individual.

Breach Notification Decision Tree

The breach notification decision tree set forth in the Plan is modified to include the following:

- The first question "Breached data owned or licensed by DGS?" is modified to read "Breached data part of the C2C System?"
- The second question "Computing or storage device containing breached data owned/ licensed by DGS?" is modified to read "Computing, storage device, or service containing breached data owned, licensed or contracted by DGS?"

- The last oval “Breach notification required” is modified to read “Breach notification and/or maintenance of a record of the disclosure in the individual’s file”