California
DEPARTMENT OF TECHNOLOGY
Office of Information Security

**PROCEDURE:** CAL-CSIRS DESIGNEE FAQ'S

**OWNER:** Office of Information Security, California Department of Technology

**DISTRIBUTION**: ISO and CIO Community **ISSUE DATE:** JULY 2019

# California Compliance and Security Incident Reporting System (Cal-CSIRS) Frequently Asked Questions (FAQ)

**Q. What if I am in multiple roles for multiple entities?**

A. You will be issued a single user-id and password that can connect to each of your entities. Be sure to list all entities you are assigned on the Cal-CSIRS Designee Request form. A single user-id can be given access to multiple entities, and a single user-id can be assigned multiple roles within individual entities.

**Q. What if my entity needs more than one alternate reporting designee who can report incidents?**

A. Each entity may choose to designate alternate incident preparers to submit incidents into Cal-CSIRS on behalf of their assigned entity.

**Q. Will our AIO and AISO have access to all of the Departments included within their Agency?**

A. Yes, the security model is designed to segregate the agencies and department views.

**Q. How do I change the selected alternate reporting designee?**

A. If the alternate reporting designee information needs to be changed, follow the instructions in the Cal-CSIRS Designee Request Form Instructions located on the California Department of Technology (CDT) website: https://cdt.ca.gov/policy/simm/#SIMM

**Note:** The Cal-CSIRS Designee Request form is separate from the annual Agency Designation Letter (SIMM 5330-A) and facilitates access and authentication preferences for Cal-CSIRS. If you have a change in your CIO or ISO designation you will still use the SIMM 5330-A.

**Q. How does my new designee obtain the Cal-CSIRS User Manual?**

A. When a completed Cal-CSIRS Designee Request form is submitted to OIS, a Cal-CSIR User Manual will be sent to the new reporting designee.

**Q. Will previous SIMM 5340-B incidents be uploaded into Cal- CSIR?**

A. No. It is not feasible to import California Highway Patrol (CHP) and OIS data from existing and disparate reporting systems to the new system. We implemented a clean cut-over from the old reporting process to the new Cal-CSIRS reporting process.

**Q. If CHP Computer Crimes Investigations Unit (CCIU) decides to investigate, will they or the Emergency Notification and Tactical Alert Center (ENTAC) give me a separate number for the same incident?**

A. At the beginning of the incident investigation, CHP will use the Cal-CSIRS number; thus, you can reference the same Cal-CSIRS number, if you want an update or have questions. If the CHP-CCIU opens a case investigation, they may create a unique CHP case number for your incident.

**Q. Will an entity be able to print an individual incident report?**

A. Yes. The individual report will print all possible questions and any answers to those questions. In the incident report, reference the drop down menu: Action > Record Detail Report.

**Q. Will an entity be required to print and route a hard-copy of the report for signatures?**

A. No, with the implementation of Cal-CSIRS, routing a hard-copy for signatures will no longer be required. State entities must continue to inform their Privacy Officer, CIO and department director of incidents in accordance with state policy on incident handling and coordination (SAM 5340.3 and SAM 5340.4) instructions and procedures (SIMM 5340-A) as well as in accordance with their internal organizational processes and procedures. Further, the system will allow entities to create reports of open and closed incidents to facilitate Security Governance and Executive Management briefings.

**Q. Will Cal-CSIRS generate either the Std 152 or Std 99 form?**

A. Cal-CSIRs will allow you to print the data input into Cal-CSIRS to assist with preparing those reports. However, because those reports require much more information than Cal-CSIRS requires, you will still need to complete the Department of General Services Std 152 and California Highway Patrol Std 99 forms if applicable to the incidents you report through Cal-CSIRS, and send them to the Department of General Services (DGS) and/or CHP.

**Q. Will Two Factor Authentication (2FA) be required to access Cal- CSIRS?**

A. Yes. State entities will provide Cal-CSIRS user contact information for receiving the randomly generated code to OIS through the Cal-CSIRS reporting designation process. At login, the system will generate a one- time code to enter along with user id and password.

**Q. Will 2FA be required each time a user logs into Cal-CSIRS?**

A. No. 2FA will only be required once during the day if you are logging in/out/in on the same device.

**Q. What will be the retention policy for incidents in Cal-CSIRS?**

A. It will be in accordance with our Department's current retention policy for these records, which is currently 5 years from the date an incident is closed.

**Q. Is the data in Cal-CSIRS subject to Public Records Act (PRA) requests, or exempt from PRA pursuant to Government Code Section 6254.19?**

A. Yes, these records are subject to PRA requests. However, some data within Cal-CSIRS may be considered confidential and exempt from disclosure. For example, records for which the disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency (Government Code Section 6254.19). The Department's process is to review all requested records and redact when necessary the protected or otherwise exempt portions of the record before its release.

**Q. What is the "Situational Awareness" button?**

A. The situational awareness button allows a reporter to share information about anomalous or suspicious activity they've observed that has not risen to a reportable incident for their entity. As an example, a large department may wish to share that it is seeing an unusually high volume of traffic from a specific IP or IP range. The situation may not have resulted in an outage or disruption but could impact others and would be worth sharing. To create a Situational Awareness Report use the "Situational Awareness" button instead of the "Submit" button.

**Q. Who can see and who is notified when the Situational Awareness reports made through Cal-CSIRS?**

A. All Cal-CSIRS users may see a Situational Awareness report. The SAR allows the community to share information about suspicious activity trends and anomalies (for example an uptick in probe and scan activity) that may not constitute a reportable incident.

**Q. Who can see and is notified when a department submits an incident report?**

A. Authorized representatives from CHP's ENTAC and CCIU, authorized representatives from the California State Threat Assessment Center system, and authorized representatives from OIS, and authorized users in the reporting entity and its Cabinet-level Agency may see reports submitted by a department. Cabinet-level agencies have visibility of all entities reporting up to them. An email alert is sent only to authorized representatives from CHP's ENTAC and CCIU, authorized representatives from the California State Threat Assessment System, and authorized representatives from OIS when an incident is reported. Once reviewed by OIS an acknowledgement is sent to the reporting entity.

**Q. How will communications occur between OIS and/or CCIU and reporting entities?**

A. Cal-CSIRS is an incident reporting system not an incident management system. Conversations to manage incident response will still need to occur by telephone, but these can be documented and preserved as part of the report record in the workflow notes, and notes/comments fields.

**Q. I am an authorized reporting designee for my Agency, may I submit an incident on behalf of a department that reports up to our Agency?**

A. Yes. Please contact OIS if you need assistance with doing so.

**Q. I am an authorized reporting designee for my Department, may I submit an incident on behalf of another state department that we have an information exchange or system interconnection with business relationship with?**

A. No, the other department's authorized reporting designee will need to report the incident.

**Q. How is an incident closed?**

A. OIS will review reported incidents for completeness and will work with reporting entities to determine when they may be closed. Authorized reporters/preparers may update information in the system as it becomes available using the Save and Close button. Once the entity believes all required information has been entered they may select the Final Update button and this will send a notice to OIS

**Q. May we add additional information after an incident is closed?**

A. No. If needed, you may contact the OIS to make the needed comment/note.

**Q. How do we report an incident if Cal-CSIRS is offline?**

A. You will contact OIS during business hours to report the system is offline, and you or an OIS representative will enter your report once the system is back online. **If after regular business hours, and** you require immediate law enforcement assistance, you will contact the CHP's ENTAC at (916) 843-4199.

**Note: ENTAC is only to be contacted when immediate law enforcement assistance is needed after regular business hours.**

**Q. What is the Risk Assessment tab?**

A. Cal-CSIRS is designed to be a fully integrated governance, risk and compliance reporting system.