**PROCEDURE:** CAL-CSIRS DESIGNEE REQUEST INSTRUCTIONS, ROLES & KSA’S

**OWNER:** Office of Information Security, California Department of Technology **DISTRIBUTION**: ISO and/or CIO Community **ISSUE DATE:** October 2022

**INSTRUCTIONS:** California Compliance and Security Incident Reporting System (Cal-CSIRS) Designee Request instructions, roles, & knowledge, skills and abilities (KSA’s).

When completing the **CAL-CSIRS DESIGNEE REQUEST FORM** remember the following:

* Complete form in its entirety.
* At a minimum, accounts must be assigned to the designated CIO and ISO. Additional accounts may also be given to the Incident Preparer, Assessment Manager, Assessment Responder, and the Assessment Reviewer roles.
* A state issued email address and one phone number (desk or cell) must be provided in order to successfully login to Cal-CSIRS. Each designee will be prompted upon login to select the means in which they would like to receive the two-factor authentication pin code. This code will be sent to the provided email address, cell phone (via text message), or desk phone (via phone message).
* If a designee is assigned to multiple roles, be sure to list all roles on the form.
* If a designee is assigned to multiple entities, the designee information will need to be provided with each entity’s designee request submission. This will allow for the designee to have accessibility to all designated entities on their personal Cal- CSIRS dashboard. This information must also be listed on the designee request form.
* It is important that the Cal-CSIRS designee list remains current. This will allow for the OIS Program Managers and/or the California Highway Patrol, Computer Crimes Investigation Unit are able to contact the designees in order to provide assistance or to request clarification.

How to complete the California Department of Technology **SERVICENOW REQUEST FORM**:

* The state entities designated ISO or CIO [as identified on the Designation Letter (SIMM 5330-A)] must complete the following steps in order to request Cal-CSIRS designees:
  + Go to <https://cdt.ca.gov/>
  + Scroll to bottom of page and select “Submit Service Request”
  + Log in to your account
  + Complete the ServiceNow request for Cal-CSIRS Designee Access
  + Attach the completed Cal-CSIRS DESIGNEE REQUEST FORM to the ServiceNow request, this form can be found on the CDT – Security page: <https://cdt.ca.gov/policy/simm/#SIMM>
  + Submit
* Once the ServiceNow ticket is submitted, it will then be routed within the Office of Information Security (OIS) for approval and account creation.
* Once account(s) are created, the designee(s) will receive their username and password directly.

**ROLES & KSA’S:** Cal-CSIRS Roles, KSA’s, and account recommendations for incident management and risk reporting.

# INCIDENT MANAGEMENT

Incident Preparer Tasks:

* Point of contact for an entity, regarding actual and potential cyber incidents.
* Ability to create and submit incidents for own entity or on behalf of another entity.
* Ask questions, get clarification, investigate incident to complete a thorough Cal-CSIRS report.
* Answers the appropriate incident questions within Cal-CSIRS regarding incident overview, incident details, and workflow notes.

Incident Preparer KSA’s:

* General knowledge of network structure, as well as the basic purpose of network components (hub / switch, firewall, etc.).
* General knowledge about information security.
* Knowledge about their own entity’s Office of Information Security, regarding their office’s authority, responsibilities, and deliverables.
* Knowledge about the State requirements, regarding Incident Reporting (SIMM 5340-A).
* Knowledge about Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C).
* General knowledge about the 9 ‘Incident Types’ reported by State entities:
  1. Denial of Service Attack
  2. Malware
  3. Information Asset (Property)
  4. Loss or Theft
  5. Information Disclosure5. Misuse
  6. Outage or Disruption
  7. Social Engineering / Phishing
  8. Unauthorized Access
  9. Unauthorized Data Destruction

# RISK REPORTING

Assessment Manager Tasks:

* Point of contact for an entity, coordinating common control and risk assessments.
* Start new Security Controls Self-Assessments for Information Systems.
* Start new Security Controls Self-Assessments for Common Controls.
* Assign or change participants in the roles of Assessment Respondent and Assessment Reviewer.

Assessment Manager KSA’s:

* Understands which information systems are identified as mission critical systems in an entity.
* Familiar with staff resources and knowledge of who the key stakeholders are that will be answering control questions and reviewing responses.
* Ability to engage resources to manage the review process and complete timely.
* Does not need to be an entity manager.

Assessment Participant(s) [Includes the Assessment Responder(s) and the Assessment Reviewer(s)] Tasks:

* Works with system owners, security team, and senior managers to enter the following information:
* Designates the FIPS 199 categorization
* Answers the security control questions
* Assigns a risk score for identified risks
* Assigns a risk “owner” for each identified risk
* Identifies how risks will be addressed

Assessment Participant(s) [Includes the Assessment Responder(s) and the Assessment Reviewer(s)] KSA’s:

* General knowledge about information security.
* Specific knowledge of a particular information system (Therefore it may be appropriate to assign different people this role depending on the information system being reviewed, or the area of a system being reviewed).
* The ability to measure security control’s effectiveness and answer security control questions.

**RISK REPORTING – Minimum Recommended Accounts** Tiny Entity:

* Total employees: 0-50
* Maximum available accounts: 6
* Minimum recommended accounts and roles:
* Assessment Manager: 1
* Assessment Responder: 1
* Assessment Reviewer: 1 Small Entity:
* Total employees: 51-600
* Maximum available accounts: 12
* Minimum recommended accounts and roles:
* Assessment Manager: 2
* Assessment Responder: 2
* Assessment Reviewer: 2 Medium Entity:
* Total employees: 601-2,000
* Maximum available accounts: 18
* Minimum recommended accounts and roles:
* Assessment Manager: 2
* Assessment Responder: 2
* Assessment Reviewer: 2 Large Entity:
* Total employees: 2,001-10,000
* Maximum available accounts: 22
* Minimum recommended accounts and roles:
* Assessment Manager: 2
* Assessment Responder: 2
* Assessment Reviewer: 2 Huge Entity:
* Total employees: 10,001 +
* Maximum available accounts: 22
* Minimum recommended accounts and roles:
* Assessment Manager: 3
* Assessment Responder: 3
* Assessment Reviewer: 3