Appendix A
Roles and Responsibilities by Affected/Reporting Entity Type

Reporting Entity Type	Reporting Entity	CHP-CCIU	CDT-OIS	CDT- SOC	Cal-CSIC	CMD-CND
State Executive Branch Entity	-Lead/Owner of incident reporting and response -Reports immediately via Cal-CSIRS -Establishes POC for media inquiries in case of escalation -Keeps its Directorate/Cabinet-level informed -Assists law enforcement with evidence collection and root cause determination -Implements corrective actions to reduce likelihood of recurrence. -Ensure the confidentiality, integrity and availability of all information related to the incident	-Lead on criminal investigations -Lead on notifications to federal government partners (FBI, DHS, etc.) -Assist with Administrative (policy violation) investigations when requested or required. -Ensure the confidentiality, integrity and availability of all information related to the incident	-Direct, oversee and track the reporting of incidents in Cal-CSIRS by state Executive Branch entities -Participate as a four core partner through the incident lifecycle -Direct and advise state Executive Branch entities on privacy issues and privacy breach notification requirements -Ensure root cause analysis and plan of action and milestones (POAM) for remediation are completed for state Executive Branch entities incidents to reduce likelihood or prevent reoccurrence -Ensure the confidentiality, integrity and availability of all information related to the incident	-Assists with anomaly detection notifications as anomalies are detected, and analysis and triage **IF** entity is using ca.gov, CGEN or other CDT services -Provide review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories -Coordinate with the Cal-CSIC and CCIU as appropriate -Correspond directly with CDT customer entities as appropriate -Provide remediation guidance to victim entity -Have victim entity update the Cal-CSIRS report as appropriate -Participate in discussions with CCIU, CMD and Cal-CSIC concerning ESF-18 escalation when appropriate. -Ensure the confidentiality, integrity and availability of all information related to the incident	- Develop and coordinate threat alerts and critical bulletins with four core partners and CDT SOC -Coordinate with CCIU, CDT SOC and other core partners for key threat indicators -Provide remediation guidance to victim entities -Initiate / coordinate discussions with four core partners and CDT-SOC concerning ESF-18 escalation when appropriate -Ensure the confidentiality, integrity and availability of all information related to the incident	-Provide review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories -Assist with incident response when requested or required -Ensure the confidentiality, integrity and availability of all information related to the incident

Appendix A
Roles and Responsibilities by Affected/Reporting Entity Type

Reporting Entity Type	Reporting Entity	CHP-CCIU	CDT-OIS	CDT- SOC	Cal-CSIC	CMD
Other State Government Branch (Judicial, Legislative)	-Reports to authorities and in accordance with applicable laws, contracts with state government, and industry regulations -Optional reporting to Cal-CSIC -Ensure the confidentiality, integrity and availability of all information related to the incident	-Lead on criminal investigations -Lead on notifications to federal government partners (FBI, DHS, etc.) -Assist with Administrative (policy violation) investigations when requested or required. -Ensure the confidentiality, integrity and availability of all information related to the incident	- May participate as a four core partner through the incident lifecycle for certain incidents - May assist and advise entities on privacy issues and privacy breach notification requirements -Ensure the confidentiality, integrity and availability of all information related to the incident	-Assists with anomaly detection notifications as anomalies are detected, and analysis and triage **IF** entity is using ca.gov, CGEN or other CDT services -Provide review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories -Coordinate with the Cal-CSIC and CCIU as appropriate -Correspond directly with victim entity **IF** entity is using ca.gov, CGEN or other CDT services -Participate in discussions with CCIU, CMD and Cal-CSIC concerning ESF-18 escalation when appropriate. -Ensure the confidentiality, integrity and availability of all information related to the incident	- Develop and coordinate threat alerts and critical bulletins with four core partners and CDT SOC -Coordinate with victim entity for key threat indicators -Provide incident response and remediation assistance as needed **for Non-State Executive Branch entities** -Create and update non-state Executive-Branch entity incident reports -Correspond directly with the non-state Executive Branch entity, and CDT SOC when victim entity is a user of ca.gov domain, CGEN or other CDT services -Initiate / coordinate discussions with four core partners and CDT-SOC concerning ESF-18 escalation when appropriate -Ensure the confidentiality, integrity and availability of all information related to the incident	-Provide review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories -Assist with incident response when requested or required -Ensure the confidentiality, integrity and availability of all information related to the incident

Appendix A
Roles and Responsibilities by Affected/Reporting Entity Type

Reporting Entity Type	Reporting Entity	CHP-CCIU	CDT-OIS	CDT- SOC	Cal-CSIC	CMD
Non-State Government Entities (Local, Tribal, Territorial)	-Reports to authorities and in accordance with applicable laws, contracts with state government, and industry regulations -Optional reporting to Cal-CSIC -Ensure the confidentiality, integrity and availability of all information related to the incident	-May participate as a four core partner through the incident lifecycle for certain incidents -May assist with criminal investigation when requested or required -May lead on notifications to federal government partners (FBI, DHS, etc.) -Ensure the confidentiality, integrity and availability of all information related to the incident	-May participate as a four core partner through the incident lifecycle for certain incidents -May assist and advise entities on privacy issues and privacy breach notification requirements -Ensure the confidentiality, integrity and availability of all information related to the incident	-Assists with anomaly detection notifications as anomalies are detected, and analysis and triage **IF** entity is using ca.gov, CGEN or other CDT services -Provide review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories -Coordinate with the Cal-CSIC and CCIU as appropriate -Correspond directly with CDT customer entities as appropriate -Provide remediation guidance to victim entity -Participate in discussions with CCIU, CMD and Cal-CSIC concerning ESF-18 escalation when appropriate. -Ensure the confidentiality, integrity and availability of all information related to the incident	- Develop and coordinate threat alerts and critical bulletins with four core partners, and CDT SOC when victim entity is a user of ca.gov domain, CGEN or other CDT services -Coordinate with victim entity for key threat indicators -Provide response and remediation assistance as needed and requested -Initiate / coordinate discussions with four core partners and CDT-SOC concerning ESF-18 escalation when appropriate -Ensure the confidentiality, integrity and availability of all information related to the incident	-Provide review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories -Assist with incident response when requested or required -Ensure the confidentiality, integrity and availability of all information related to the incident

Appendix A
Roles and Responsibilities by Affected/Reporting Entity Type

Reporting Entity Type	Reporting Entity	CHP-CCIU	CDT-OIS	CDT- SOC	Cal-CSIC	CMD
Private Sector	-Reports to authorities and in accordance with applicable laws, contracts with state government, and industry regulations -Optional reporting to Cal-CSIC -Optional reporting to Cal-CSIC	-May lead on notifications to federal government partners (FBI, DHS, etc.)	-May participate as a four core partner through the incident lifecycle for certain incidents		- Develop and coordinate threat alerts and critical bulletins -Coordinate with victim entity for key threat indicators -Provide response and remediation assistance as needed and requested -Initiate / coordinate discussions with four core partners and CDT-SOC concerning ESF-18 escalation when appropriate -Ensure the confidentiality, integrity and availability of all information related to the incident	