

Issued September 7, 2018

California Cap-and-Trade Program

Cap-and-Trade Program Data Security and Control

All CITSS users and the entities they represent are prohibited from releasing certain information and are required to maintain effective control of Cap-and-Trade Program data and credentials.

Prohibitions on the Release of Certain Information

The California Cap-and-Trade Program includes periodic auctions of emission allowances. CARB developed guidance for entities to [buy, sell, and trade compliance instruments](#), including how to purchase allowances at an auction.

The auction design and the rules for participation were established to ensure the integrity of the auction, including fair and equitable access for all qualified auction participants. Auction participants are prohibited from releasing information regarding auction or reserve sale participation, including information of an entity's intent to participate or not to participate at an auction; auction approval status; bidding strategy at past or future auctions; bid price and/or bid quantity information at past or future auctions; and information on the amount of any bid guarantee provided to the financial services administrator (section 95914(c)(1)).

Maintain Effective Control of Program Data

The California Air Resources Board (CARB) strongly encourages all CITSS users to ensure that any entity a user represents in CITSS maintains and follows written procedures and policies that provide effective control of entity program information. Controlling access to all program data protects an entity as well as all program participants. Also, the information listed in section 95914(c)(1) must be controlled to avoid violating the program requirements. CARB will evaluate any release of such information for possible enforcement action.

If you suspect that program information has been accessed by unauthorized individuals, CARB strongly encourages investigating how the unauthorized access occurred and improving entity procedures and policies to prevent future unauthorized access. CARB also strongly encourages users to notify CARB of any unauthorized access immediately, in particular with relation to any information listed in section 95914(c)(1). CARB requests that users immediately notify CARB of the incident by contacting the CITSS Help Desk (916-324-7659 or CACITSSHelpdesk@arb.ca.gov).

Maintain Effective Control of Program Credentials

CARB strongly encourages users to ensure that entities maintain and follow written procedures and policies that provide effective control of user credentials that provide

access to CITSS and the Auction Platform. Unauthorized access to an entity's accounts in these systems could harm the entity and possibly other program participants.

- Account credentials are associated to a unique individual; at no point should they be shared with another person (section 95834).
- Account representatives are responsible for any action undertaken with their account credentials. (section 95832(a)(4) and section 95832(c)(2))
- Violation of these provisions or the [CITSS Terms of Use](#) may result in removal of a user's access to CITSS and to the Auction Platform or other enforcement measures.)

CARB also recommends that an entity's staff be properly trained to recognize potential threats from cybercriminals. Information is available from the [Federal Bureau of Investigation](#) to help understand cybercrime risks and how to prepare.

If You Suspect Credentials Have Been Compromised

If at any time you suspect that credentials that provide user access to CITSS or the Auction Platform have been compromised, take steps immediately to prevent unauthorized access to these systems.

- Contact your IT support group and follow your organization's procedures for reporting and resolving the situation.
- Contact CARB's CITSS Help Desk (916-324-7659 or CACITSSHelpdesk@arb.ca.gov) to report the incident; immediately reset the passwords for all your organization's account representatives and viewing agents for CITSS and the Auction Platform.
- File a complaint with appropriate law enforcement officials in your area. You may also want to file a complaint with [The Internet Crime Complaint Center \(IC3\)](#).

CARB has received no reports of credentials being compromised for CITSS or the Auction Platform. If each participating entity maintains effective control of their credentials, no such events will occur.