

Updated June 1, 2020

California Cap-and-Trade Program

Cap-and-Trade Program Data Security and Control

Cap-and-Trade Program Data Security

Cap-and-Trade Program (Program) data is managed in accordance with policies and practices of the California Air Resources Board (CARB) Office of Information Services and by the Western Climate Initiative, Incorporated (WCI, Inc.). CARB delivers services in accordance with State of California Department of Technology, Office of Information Security requirements. [California IT Policy, Standards, Instructions and Guidelines](#) are available on the California Department of Technology, Office of Information Security website.

WCI, Inc. is a non-profit corporation that provides administrative and technical services to support implementation of state and provincial greenhouse gas emissions trading programs. Currently, WCI, Inc. provides services to California, Nova Scotia, and Québec (Participating Jurisdictions). California and Québec participate in a linked Cap-and-Trade Program and Nova Scotia operates its own, stand-alone program. WCI, Inc. provides the [Compliance Instrument Tracking System Service](#) (CITSS) and [Markit Auction Platform](#) (MAP) through third-party service providers to support the Participating Jurisdiction's programs. WCI, Inc. and the Participating Jurisdictions consider data security to be of the highest priority. WCI, Inc. services incorporate system security measures in accordance with regulatory requirements of the Participating Jurisdictions.

CITSS is the primary Cap-and-Trade Program infrastructure service. CITSS is a single market registry used by multiple Participating Jurisdictions. CITSS enables Participating Jurisdictions to issue and retire instruments in accordance with their specific regulatory requirements. CITSS incorporates specific security requirements to protect the integrity of submitted information, including:

- To register in CITSS, an individual must complete the user registration process. This includes a Know-Your-Customer review for verification of an individual's name, primary residence, a valid government-issued identity document with a valid expiration date, date of birth, and proof of an open bank account.
- Other than Jurisdiction controlled accounts, CITSS only allows entity accounts to hold instruments. To obtain a CITSS account, entities must complete the account application process. This includes disclosure of corporate information

such as a government issued taxpayer or employer identification number and directors and officers for verification.

- The transfer of instruments within CITSS requires multiple actions (proposal, approval, and acceptance) performed by different individuals.

Cap-and-Trade Program Data Control

The Cap-and-Trade Regulation specifies requirements for the control and use of Cap-and-Trade Program data and credentials. Pursuant to the Regulation, CITSS users and the entities they represent are prohibited from releasing certain information that could compromise the integrity of the Program.

Prohibitions on the Release of Certain Information

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

Auction design and rules for participation protect the integrity of an auction, including fair and equitable access for all qualified auction participants. The California Cap-and-Trade Regulation prohibits auction participants from releasing information regarding auction or reserve sale participation. This includes releasing information regarding 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)). CARB evaluates the release of such information for possible enforcement action.

Maintain Effective Control of Program Data

Controlling access to Program data protects an entity as well as all Program participants. CARB strongly encourages all entities with a CITSS account to maintain written procedures and policies that provide effective control of entity Program information.

Maintain Effective Control of Program Credentials

- Account credentials are associated to a single individual. The California Cap-and-Trade Regulation prohibits users from sharing credentials 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, or information has been accessed by unauthorized individuals, take steps immediately to prevent unauthorized access to these systems.

- Contact your Information Technology 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 \(IC3\)](#).