OFFICE OF THE STATE CIO

IT POLICY LETTER

NUMBER:

ITPL 10-13

SUBJECT:

SECURITY REPORTING SCORECARDS

Emphasis: Transparency and accountability in achieving security compliance goals and objectives consistent with Chapter 404, Statutes of 2010, State Administrative Manual Chapter 5300, and Government Code Section 11545 and 11549 et.seq.

DATE ISSUED:

OCTOBER 4, 2010

EXPIRES:

Until Rescinded

REFERENCES:

Chapter 404, Statues of 2010
Government Code Section 11545 and 11549 et.seq.

ISSUING AGENCY:

OFFICE OF THE STATE CHIEF INFORMATION OFFICER

DISTRIBUTION

Agency Secretaries
Department Directors
Agency Chief Information Officers
Department Chief Information Officers
Agency Information Security Officers
Information Security Officers

PURPOSE

Given the government's increased use of Information Technology (IT) and Internet-based services, the state has a compelling need to ensure the confidentiality, integrity and availability of those systems and services are adequately protected from known and anticipated threats. In addition, there is an increasing demand for broader transparency and accountability in reporting government activities. Consistent with Chapter 404, Statues of 2010 (AB 2408), the purpose of this Information Technology Policy Letter (ITPL) is to:

- Establish the Security Reporting Scorecard process for reporting on state Agency[1] and department participation in required security reporting activities.
- Remind Department Directors, Agency Chief Information Officers (Agency CIOs), Department Chief Information Officers (CIOs), Agency Information Security Officers (AISO) and Information Security Officers (ISOs) of their reporting responsibilities.

[1] When capitalized, the term "Agency" refers to one of the state's super Agencies such as the State and Consumer Services Agency or the Health and Human Services Agency. When used in lower case, the term "agency" refers to any office department, board, bureau, commission or other organizational entity within state government. Within this ITPL, "agency" and "department" are used interchangeably.

BACKGROUND

The Office of the State Chief Information Officer (OCIO) has responsibility and authority for the establishment and enforcement of state IT in California State Government. This includes establishing and enforcing the state's IT strategic plans, policies, standards and enterprise architecture. In accordance with Government Code Section 11545 and 11549, the Office of Information Security (OIS), within the OCIO has the authority and responsibility for overseeing state agency compliance with security policies, standards and procedures to ensure the protection of state information assets and citizen data held in trust by state agencies.

As such, each state agency is responsible for the designation of officials within their agency to fulfill key security functions and reporting on its status of compliance with security policy, standards and procedures. While agency reporting and self-certification activities alone do not ensure the security of state information assets, they do demonstrate an agency's acknowledgement of the requirements and provide a measure of accountability. The schedule of security reporting activities and corresponding instructions and forms are published at: http://www.cio.ca.gov/OIS/Government/activities_schedule.asp.

POLICY AND PROCESS

The first publication of the Security Reporting Scorecards will be in November 2010 and reflect the agency's reporting status only. Publication may be expanded at a later date to identify the specific reports filed, in progress, or not filed, but will not reveal any detail that would reveal vulnerabilities to, or otherwise increase the potential for an attack on an information technology system of the agency.

The Security Reporting Scorecards will share a common "look and feel," with the ICP scorecards; however, the metrics used to prepare the scorecards are based solely on OIS's receipt of the required information by the reporting deadline.

Scorecards will be updated thereafter in February, May, August, and November. An agency is responsible for resolving any reporting deficiencies prior to the next scheduled update, in order for the status to be reflected in the next publication cycle.

In addition, OIS will continue to provide departments with a courtesy reminder of deficiencies and work with those needing additional attention to meet the reporting requirements.

Security Reporting Scorecards will be published on the OCIO's Web site under OIS's Policy Compliance page at:

http://www.cio.ca.gov/OIS/Government/policy.asp.

ROLES AND RESPONSIBILITIES

Agency CIOs and AISOs shall ensure departments are in compliance with the Security Reporting requirements through their department CIOs and ISOs.

CIOs and ISOs who are not affiliated with an Agency have the same responsibilities as Agency CIOs and Agency-affiliated department CIOs.

APPLICABLILITY

This ITPL applies to all state agencies, departments, boards, commissions, offices or other organizational entity under the direct executive authority of the Governor's Office.

	Recognizing constituency value, some Offices not under the direct executive authority of the Governor may choose to actively participate in the Security Reporting activities. Future publications may include the Security Reporting Scorecards of these agencies in order to acknowledge their participation and contribution toward achieving state security goals and objectives.
CONTACT	Questions concerning this policy should be directed to the Office of Information Security at (916) 445-5239 or via email to Security@state.ca.gov.
SIGNATURE	/s/ Teri Takai, Chief Information Officer State of California