



County of Monterey

Board of Supervisors
Chambers
168 W. Alisal St., 1st Floor
Salinas, CA 93901

Board Report

File #: A 20-014, **Version:** 1

a. Authorize the Director of Information Technology to execute a Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Cyber Assessment Rules of Engagement in order to allow an upcoming no-cost cyber Red Team Assessment (RTA) to be performed by CISA as a mean to proactively test the County's cybersecurity defenses.

RECOMMENDATION:

It is recommended that the Board of Supervisors:

a. Authorize the Director of Information Technology to execute a Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Cyber Assessment Rules of Engagement in order to allow an upcoming no-cost cyber Red Team Assessment (RTA) to be performed by CISA as a mean to proactively test the County's cybersecurity defenses.

SUMMARY/DISCUSSION:

With the ongoing threats to local government including but not limited to ransomware, the activities of nation state actors and threats to election security, the IT Department is registering for a no-cost Red Team Assessment from Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) in order to audit and test the county's cyber security defenses and incident response procedures. The goal is to obtain a review of these defenses and procedures and to subsequently improve or correct them as necessary.

In order to assist a variety of stakeholders to ensure the cybersecurity of our nation's critical infrastructure, CISA offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. CISA's cybersecurity assessment services are offered solely on a voluntary basis and are available upon request.

A CISA assessments Red Team Assessment (RTA) is a comprehensive evaluation of an IT environment where the CISA team attempts to gain unauthorized access into and persistence within the requesting entity's network through emulation of Advanced Persistent Threat (APT) activities. The CISA team will quietly connect to and probe a requesting entity's network using APT tactics, techniques, and procedures to determine the security posture of the entity's cyber assets and the effectiveness of their response capabilities to a sophisticated adversarial presence. These activities are coordinated with the County's Chief Security Officer and subsequently the departmental Information Security Officers (ISOs) and are executed in a manner so that no business services are disrupted during this assessment in any manner, shape or form.

Other California counties such as Santa Cruz County have successfully completed CISA assessments and have recommended them as valuable reviews of a county's cyber security posture.

OTHER AGENCY INVOLVEMENT:

County Counsel does not approve the CISA-generated Rules of Engagement with non-standard terms and conditions. The Chief Security Officer has reviewed and approved the attached Rules of Engagement as to form.

FINANCING:

There is no cost associated with the authorization to use the Homeland Security assessment and no impact on the County General Fund.

BOARD OF SUPERVISORS STRATEGIC INITIATIVES:

Authorizing the Director of the Information Technology Department to execute the Department of Homeland Security assessment Rules of Engagement will facilitate improvement of the County's information security infrastructure, processes and technology, which enables all County departments.

Mark a check to the related Board of Supervisors Strategic Initiatives

Economic Development

Administration

Health & Human Services

Infrastructure

Public Safety

Prepared by: Dan Kern, Chief Security Officer, 796-1449

Approved by:

Date: _____

Eric A. Chatham, Director of Information Technology, 759-6923

Attachments: DHS CISA Assessments; County of Monterey CISA ROE.