## INTRODUCTION

Telecommunications plays a vital role both as a primary component of the state's emergency response system and as a key business enabler to agencies. Therefore, the state's telecommunications infrastructure is a prime target for sabotage, vandalism, and unauthorized use such as fraud and abuse. Unrestricted physical access to telecommunications equipment rooms provides an easy method for causing damage to the telecommunications infrastructure.

## EQUIPMENT ROOM SECURITY RECOMMENDATIONS

Therefore, the TD recommends that agencies establish and implement policies, practices, procedures and systems that ensure the security of all telecommunications equipment rooms under their control. At a minimum, this includes controlling access to telecommunications equipment rooms by:

- Installing a key card reader system or electronic locks on all access doors,
- Maintaining current and accurate records of all persons having authorized access,
- Verifying the identification and business purpose of all individuals requesting access,
- Providing escort and supervision to these rooms while work is in progress, and
- Reporting all suspected fraudulent access attempts to the California Highway Patrol.