

What is FISMA?

Today, especially in information security and audit circles, there are two separate laws commonly being referenced as "**FISMA**". To minimize confusion, the State Information Security Office prepared this paper to describe each and their respective requirements.

The first is a long standing State law, which applies to state agencies; known as the State Financial Integrity and Manager's Accountability Act (State FISMA) of 1983 (Government Code sections 13400 through 13407). This law mandates the following internal control requirements for state agencies:

- Maintain effective systems of internal accounting and administrative control as an integral part of its management practices. These controls include, but are not limited to, segregation of duties, limiting access to assets based on job-related duties, a system of authorization and recordkeeping, and establishing an effective system of internal review.
- Evaluate control systems on an ongoing basis and promptly correct any weaknesses detected
- Involvement of management at all levels in the assessment and improvement of systems to minimize fraud, errors, abuse, and waste of government funds.

It further requires state agencies to prepare a report and certification on the adequacy of the agency's control systems by December 31, of each odd numbered year. The report must be signed by the agency director and submitted to the agency secretary. Copies are also submitted to the Legislature, the State Auditor, the Governor, and the State Library.

Additional information about the State FISMA requirements can be obtained from the following sources:

- Department of Finance, Office of State Audit and Evaluations (OSAE) <http://www.dof.ca.gov/FISA/OSAE/auditmem.asp>
- California Law <http://www.leginfo.ca.gov/calaw.html>

The second is a more recently enacted Federal law known as the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347; Title III). This law is applicable to Federal agencies and State agencies that use or exchange information with Federal information systems. Essentially, this law mandates these agencies to develop, document, and implement an agency-wide information security program to include:

- Periodic assessment of risk
- Policies and procedures based on risk assessments
- Subordinate plans for security of networks, facilities, and information systems
- Security awareness training
- Periodic testing and evaluation, no less than annually
- Process for planning, implementing, evaluating and documenting remedial action
- Procedures for detecting, reporting and responding to security incidents
- Plans and procedures to ensure continuity of operations

A subsequent Office of Management and Budget (OMB) policy memo (OMB Circular A-130) further requires these agencies to follow the minimum information security requirements, standards and guidelines published by the National Institute of Standards and Technology (NIST).

Additional information about the Federal FISMA requirements can be obtained from the following sources:

- NIST Computer Security Resource Center <http://csrc.nist.gov/sec-cert/index.html>
- Title III, Public Law 107-347, 116 Stat. 2899 <http://csrc.nist.gov/policies/FISMA-final.pdf>