What is FISMA?

What is FISMA?

The Federal Information Security Modernization Act (FISMA) was passed by Congress and signed into law in 2014. FISMA assigns responsibility to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to strengthen federal information system security through design and implementation of effective information security controls.

What is a FISMA audit?

A FISMA audit is performed to assess the effectiveness of information security programs and compliance with the requirements established under FISMA.

Our audit clients have strong legal and operational incentives to safeguard information systems and maintain compliance with data protection requirements. Annual FISMA audits are required by law for all federal agencies. In addition to maintaining legal compliance, FISMA audits provide the following benefits:

- **Continuous emphasis** on maintaining strong IT security practices
- **Increase security and protection of sensitive agency information**, to include agency missions and/or financial information

Who performs FISMA audits?

Agency inspectors general (IGs) are required to either perform an independent evaluation or contract an independent external auditor to perform the FISMA audit over the federal agency.

Performing a FISMA audit does not impact the independence of the auditor to also perform the financial statement audit. As the financial statement auditor understands the agency's control environment and key systems/processes, efficiencies can be gained by leveraging the same auditor for both the financial statement and FISMA audits. Our experience in performing federal financial statement audits has honed our ability to perform an effective and efficient FISMA audit. KPMG currently performs FISMA audits over 12 cabinet departments, and has therefore built extensive knowledge over federal information systems that can be applied to new engagements.

In conducting hundreds of postaward audits for the federal government, our professionals have the technical knowledge over information systems and resulting risks to appropriately assess control effectiveness and compliance with legal requirements over information security.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**