SmartSuite

Framework / Cybersecurity / Other

FISMA (Pub.L. 113-283, 2014)

FISMA (Pub. L. 113-283, 2014) makes U.S. federal agency heads responsible for securing their systems, with OMB oversight, DHS directives, NIST standards and annual IG evaluation.



What it is

The Federal Information Security Modernization Act of 2014 (FISMA, Public Law 113-283, 128 Stat. 3073) is the U.S. statute, codified at 44 U.S.C. 3551 to 3558, that makes the head of every federal agency responsible for protecting the agency's information and information systems, including systems operated by contractors on its behalf, and that gives the Office of Management and Budget oversight and the Department of Homeland Security operational authority over civilian agency security. It was approved on December 18, 2014 and replaced the Federal Information Security Management Act of 2002 in full.

At a glance

PUBLISHER
United States Congress (enacted); overseen by OMB, administered by DHS through CISA, standards by NIST

TYPE
Regulation

VERSION
Federal Information Security Modernization Act of 2014 (Pub. L. 113-283, 128 Stat. 3073), 44 U.S.C. 3551 to 3558

EFFECTIVE
December 18, 2014

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: govinfo.gov/app/details/PLAW-113publ283

Why it matters

- **Accountability at the top** Section 3554(a) makes the head of each agency responsible for protection commensurate with the risk and magnitude of harm, and requires security to be built into strategic, operational and budget planning.
- **Binding standards** Under 40 U.S.C. 11331 the Secretary of Commerce makes NIST information security standards compulsory and binding, so FIPS 199, FIPS 200 and the SP 800-53 baselines are not optional for agencies.
- **Directives with force** DHS may issue binding operational directives, compulsory directions to safeguard federal information from a known threat (section 3552(b)(1)), such as CISA's BOD 26-04 on prioritizing security updates.
- **Independent evidence** Section 3555 requires an annual independent evaluation by the Inspector General or an external auditor, testing a representative subset of systems, with results summarized in OMB's report to Congress.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports FISMA

System Inventory and Categorization

List each information system, including contractor-operated ones, with its FIPS 199 category, owner, authorizing official and authorization status.

Program Element Tracker

Map the eight section 3554(b) elements (risk assessment, policies, subordinate plans, training, testing, remediation, incident procedures, continuity) to owners and evidence.

Control Baseline and Annual Testing

Hold the SP 800-53 controls for each system with the test result at least annually and the remediation actions opened for deficiencies.

Incident and Breach Log

Record incidents reported to the federal incident center and start the seven-day major-incident and 30-day breach notification clocks with the notices sent.

Directive Compliance

Track each binding operational directive and emergency directive, its required actions, due dates and the evidence returned to CISA.

IG Evaluation and Annual Report

Assemble the representative system subset, metrics and narrative for the section 3555 evaluation and the section 3554(c) annual report in one workspace.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | FedRAMP Rev. 5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST 800-37 Rev.2 | NIST 800-53 Rev.5

Official resources

FISMA Overview Document

Provides essential details and requirements outlined by the Federal Information Security Modernization Act.

cisa.gov/federal-information-security-modernization-act

NIST Special Publication 800-53

Provides a catalog of security and privacy controls for federal information systems and organizations.

csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

OMB Circular A-130

Describes management of federal information resources, integrating FISMA requirements and guidance.

whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

NIST Risk Management Framework (SP 800-37 Rev. 2)

Describes the seven-step process for categorizing systems and selecting, implementing, assessing, authorizing, and monitoring security and privacy controls (NIST SP 800-37 Rev. 2).

csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Frequently asked questions

Who is responsible for security under FISMA?

The head of each agency (44 U.S.C. 3554(a)), who delegates compliance to the Chief Information Officer; the CIO designates a senior agency information security officer whose primary duty is security. OMB's Director oversees policy (section 3553(a)) and the Secretary of Homeland Security administers implementation for civilian systems (section 3553(b)).

Does FISMA apply to contractors and cloud providers?

Indirectly. Section 3554(a) covers information collected or maintained on behalf of an agency and systems operated by a contractor or other organization on an agency's behalf, so the agency must ensure those systems meet the same standards. Cloud services reach agencies through FedRAMP, which sits inside FISMA.

What is a binding operational directive?

A compulsory direction to an agency to safeguard federal information and systems from a known or reasonably suspected threat, vulnerability or risk, issued by DHS consistent with OMB policy (section 3552(b)(1)). CISA publishes them, for example BOD 26-04 on prioritizing security updates. They do not apply to national security, DoD or intelligence community systems.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How quickly must an agency report a major incident?

Section 3554(b)(7) requires notice to the designated committees of Congress not later than seven days after there is a reasonable basis to conclude that a major incident has occurred, with updates as more is learned. Section 2(d) of the Act separately requires breach notification to Congress within 30 days of discovery and notice to affected individuals without unreasonable delay.

Which standards does FISMA make mandatory?

Section 3554 requires compliance with the information security standards promulgated under 40 U.S.C. 11331, under which the Secretary of Commerce makes NIST standards compulsory and binding. In practice that means FIPS 199 and FIPS 200 and the NIST SP 800-53 control baselines, applied through the Risk Management Framework.

License included / downloadable: Yes The Act is a U.S. public law published free of charge on govinfo.gov and in the United States Code.

Full framework page and mappings: smartsuite.com/frameworks/fisma-federal-information-security-modernization-act