SHERLOCK CLOUD
A Secure Cloud Solution

San Diego Supercomputer Center @ UC San Diego
The Office of Management and Budget (OMB) through Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires executive agencies within the federal government to:

**PLAN FOR SECURITY**
Understanding the procedure

**SECURITY RESPONSIBILITY**
Ensuring appropriate officials are assigned

**SECURITY CONTROLS**
Periodically reviewed in their information systems

**AUTHORIZE SYSTEM PROCESSING**
Prior to operations and, periodically, thereafter

Title III of the E-Government Act (2002), entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
FISMA Security Certification

17 families of control, over 180 controls, sub-controls

Lifecycle documentation: Security Plan, Risk Assessment Plan, Contingency Plan, Incident Response Plan, etc.

Yearly security assessments (including third party audits)

Change Management (Change Control Board)

Background checks of staff

Strict government oversight and notification
WHAT IS NIST’S ROLE?

NIST

Standards, guidelines, and other publications to assist federal agencies implement FISMA

SP 800-53


Catalog of security controls for all U.S. federal information systems except those related to national security
FISMA Certified Program
Hosting for the last 8 years

FISMA Certification
Compliance with NIST 800-53 requirements

Sponsoring Agency
Centers for Medicare & Medicaid Services (CMS), adds additional requirements through the CMS Acceptable Risk Safeguards (ARS)

Yearly Federal Audit
Required of 800-53 & CMS ARS Security Controls