



WHITE PAPER



BEST PRACTICES FOR FEDERAL COMPLIANCE

CONTENTS

OVERVIEW	3
DEFENSE-IN-DEPTH	3
POLICIES AND PROCEDURES	4
FOUR PHASES OF THE CERTIFICATION & ACCREDITATION PROCESS	4
CONCLUSION	5
APPENDIX A	6
Guidelines for Selecting a Compliant Hosting Provider	6
ABOUT CARPATHIA GOVERNMENT SOLUTIONS	7



Secure Compliant Solutions

OVERVIEW

In 2002, U.S. Congress enacted into law Title III of the e-Government Act known as the Federal Information Security Management Act (FISMA). FISMA mandates that every federal agency develop, document and implement an agency-wide program to provide information security for the systems that support the federal government.

Responsibility for oversight and implementation of FISMA was delegated by congress to the Office of Management and Budget (OMB). The U.S. Government tasked the National Institute for Standards and Technology (NIST) to develop special publications that outline the framework and processes for the implementation, certification and accreditation of federal information systems. In response, NIST developed the [800 series of special publications](#) that establishes the controls and guidelines required to achieve compliance.

All federal information systems used for and by the federal government are required by law to go through a certification process to validate that the system is compliant with the minimum baseline controls established by NIST 800 series special publications. In order to validate that each federal information system is compliant with the minimum baseline, NIST established a formal Certification and Accreditation (C&A) process. Now, federal agency CIO's are responsible for establishing an agency-wide compliance program from the top down to certify that all information systems under agency control are federally compliant.

This whitepaper will outline best practices for federal compliance and the C&A process used to certify federal information systems.

DEFENSE-IN-DEPTH

Defense-in-depth means the implementation of multiple layers of intrusion and access controls from the perimeter up to the system. Government evaluators perform audits, utilizing checklists that map to NIST special publication 800.53 controls in order to validate compliance. Implementation of defense-in-depth controls at the physical and network layers that map to NIST 800.53 controls will provide adequate protection of information assets and data, in addition to ensuring compliance.

Listed here are examples of Defense-in-Depth controls:

Physical

- ◆ Perimeter fencing
- ◆ Card Key or Biometric readers
- ◆ Security Guards
- ◆ CCTV
- ◆ Secure Media Handling
- ◆ N+2 on all critical infrastructure
- ◆ Fire and Smoke detection and suppression
- ◆ EMP and Tempest proof server rooms
- ◆ Access on need-to-know basis