# FISMA & DFARS COMPLIANCE

aronson LLC
ASSURANCE | TAX | CONSULTING
*Expanding What's Possible*

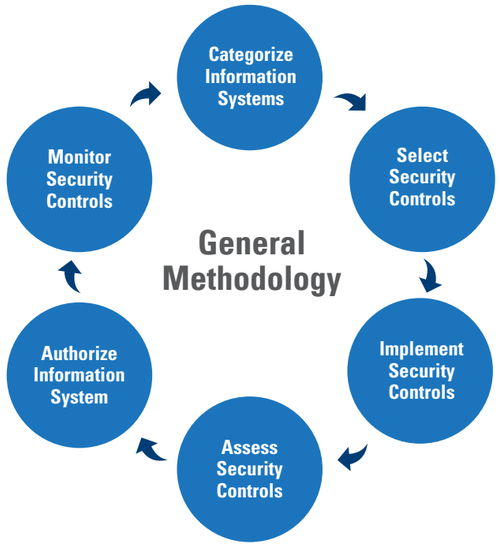
## Background

Considering the steady rise of cyber threats to public sector data, it is crucial for federal contractors to achieve compliance with federal laws and regulations regarding information system security. The Federal Information Security Management (FISMA) Act of 2002 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. This includes systems provided or managed by another agency, contractor, or other source. The newly signed law, the Federal Information Security Modernization Act of 2014 (FISMA 2014), makes several key changes to FISMA that includes an emphasis on continuous monitoring and security incident notifications.

Following the Office of Personnel Management (OPM) data breach, the Department of Defense (DoD) developed the Defense Federal Acquisition Regulation Supplement (DFARS) to provide requirements for securing covered defense information. DFARS provides specific regulations for the DoD and its contractors. Adherence to these frameworks is required in order to pursue and maintain coveted government business relationships. While compliance can appear to be a formidable undertaking, it's also a feasible and valuable investment. Currently, a standard "certification" for FISMA and DFARS compliance does not exist. Phase II of the National Institute of Standards and Technology (NIST) implementation project is to develop a security assessment credentialing program for FISMA that details requirements and responsibilities.

## Aronson Methodology

| Readiness | Assessment | Remediation | Authority to Operate | Monitoring |
|---|---|---|---|---|
| **Key Activities** | | | | |
| 1. Categorize systems<br>2. Select system boundary<br>3. Identify and document controls | 1. Develop project plan<br>2. Confirm system boundary<br>3. Conduct interviews and walkthroughs to assess the control environment<br>4. Review existing documents & conduct control analysis<br>5. Develop Gap Analysis & Recommendations Report | 1. Develop remediation roadmap<br>2. Develop or update policies and procedures<br>3. Design or revise processes and controls depending on the areas of deficiency<br>4. Implement revised controls<br>5. Conduct trainings for new or revised processes | 1. Develop test program<br>2. Conduct controls testing for design and operating effectiveness<br>3. Develop compliance report<br>4. Prepare documentation | 1. Establish Continuous Monitoring (CM) Framework / assess current framework<br>2. Develop CM program policies, procedures, tools, and templates<br>3. Support trainings for CM team<br>4. Support CM team with initial round of testing<br>5.Support CM team with program status reporting |

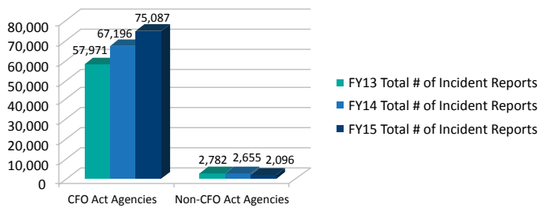



FISMA compliance is based upon categorizing in-scope systems to determine potential adverse impacts to security objectives. Confidentiality, integrity, and availability are the security objectives that must be evaluated for a system to assess whether its impact level would be high, low, or moderate. This then determines the required security and monitoring controls needed for operation.

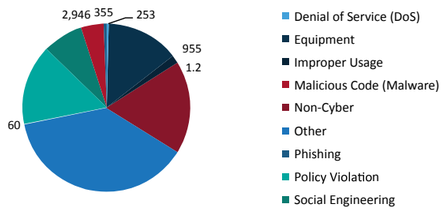
## Statistics & Industry Trends

Federal contractor incidents contribute to agency security reporting statistics. Contractors must safeguard information sufficiently considering previous and potential security incidents. The graphics below summarize incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT), which is the organization designated by the Office of Management & Budget (OMB) to receive incident reports on unclassified federal government systems. The Chief Financial Officer (CFO) Act of 1990 lists the "CFO Act Federal Agencies" and requires the CFOs to oversee financial management system compliance with auditing and internal control standards.

**FY2013 - FY2015 Federal Agency Incidents Reported to US-CERT**




**FY2015 CFO Act Agency Incidents Reported to US-CERT**




## Service Catalog

- Comprehensive FISMA / DFARS Compliance Assessment
- Remediation
- Security Awareness & Procedural Training Materials
- Breach Response Plan
- Continuous Monitoring Framework Development & Analysis

## Non-Compliance

U.S. agencies and organizations are encountering attacks and incidents from various adversaries including individuals, insiders, special interest groups, and nation-states. These opponents are armed with tremendous capabilities and nefarious motives targeted at obtaining federal data. It's vital for federal contractors to develop and maintain agile compliance programs to be a source of reliability instead of a liability for federal agencies. The ultimate cost of non-compliance with FISMA & DFARS is compromised federal data in the possession of an unauthorized individual. Additional adverse impacts for contractors could include lost business opportunities, terminated contracts, operational setbacks, and reputational damages. Contractors must maintain the trust that the federal government has placed in them by mastering compliance and continuously implementing enhancements.

## DFARS IT Regulations & Publication

252.204-7008, *Compliance with Safeguarding Covered Defense Information Controls*

252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*

NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations*

## FISMA Publications

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Federal Information Systems*

NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*

NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*

NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*

NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*

NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*

NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*

NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

**www.aronsonllc.com | 301.231.6200 |** 805 King Farm Blvd. Suite 300 | Rockville, MD 20850