WATKINS | MEEGAN

Information Assurance – Why it may apply to your organization?

Does your organization provide services around information and information systems (IT systems and infrastructure) that support the operations and assets of a federal agency? Have you been asked by your Contracting Officer or COTR about information security controls in your organization or Federal Information Security Management Act (FISMA)?

Many of you may ask what is FISMA and how does it apply to your organization. Federal Information Security Management Act (FISMA), also referred to as Title III of the E-Government Act (Public Law 107-347), 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 those provided or managed by another agency, contractor, or other source. FISMA forces agencies to understand the security of their systems and holds them accountable for resolving deficiencies. The agencies and their contractors must have their IT systems and infrastructure supporting the federal agency certified and accredited, more commonly known as the Certification and Accreditation (C&A) process in the industry.

C&A is a process where auditors inspect information security controls of the IT systems and infrastructure using the National Institute of Standards and Technology (NIST) 800-53/53A and NIST 800-37 publications; and FIPS 199 and FIPS 200 guidelines. The end result of the C&A process is an assessment of whether the systems and infrastructure are compliant (or in compliance) with the standards and publications.

Until recently, FISMA was applicable only to federal agencies and a very few government contractors. Lately more and more agencies have begun expanding the applicability of the FISMA compliance to their contractors and requiring the contractors to demonstrate that appropriate information security controls are in place and operating consistently. In the event the contractor cannot provide reasonable assurance that information security controls are implemented and consistently functioning, the contractor must develop and implement a remediation plan to achieve FISMA compliance.

Requirements of FISMA: FISMA is specific in its requirements and stipulates that a government agency or its contractor's information security program must include process and documentation that clearly describe the following:

- Periodic risk assessments
- Information security policies and procedures
- An assessment of threats, including their likelihood and impact
- Policies and procedures for detecting security vulnerabilities
- Evaluation and periodic testing of how well security policies are working
- An inventory of software and hardware assets

- Security awareness training and expected rules of behavior for end-users
- An evaluation of the technical, management, and operational security controls
- Procedures for reporting and responding to security incidents
- A process for addressing any deficiencies reported
- Contingency plans to ensure continuity of operations in the face of a disaster

Source: http://csrc.nist.gov/groups/SMA/fisma/overview.html

For some organizations, FISMA is well-known and is no surprise; however, other companies are only now assessing the FISMA requirements and its applicability to their contracts. While the requirements of FISMA may seem mandatory and extremely detailed, an organization's other internal or compliance efforts can be leveraged to satisfy some of the requirements stipulated by FISMA. It may feel overwhelming and seem like a lot to accomplish if your organization is being exposed to FISMA for the first time; however, it can be done. It requires executive management support, understanding and knowledge of the requirements, appropriate skill sets, detailed planning, and timely execution, to stay on course for a successful implementation.