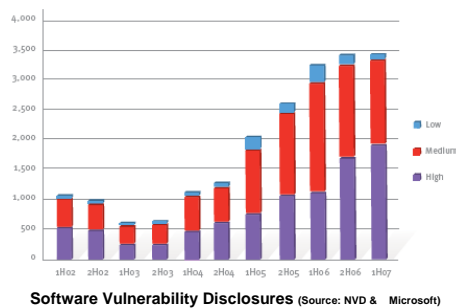


Highlights

- **Rapid Time to FISMA Compliance** – Receive reports and results within 24-72 hours
- **Automated & On-Demand** – Application security testing on an as-needed basis
- **Lower Compliance Costs** – Software as a Service (SaaS) means no hardware or software to purchase, install & maintain
- **Independent Expert Review** – Veracode is a recognized application security expert meeting compliance guidelines
- **Standards-Based Ratings** – Ratings based on NIST, CWE & CVSS to meet auditing standards

Key Facts

- **DoD Software Report** – Concludes that the government needs to take action to mitigate risks included in GOTS and COTS software
- **OMB Memo M-07-19** – Encourages agencies to use software-as-a-service (SaaS) providers to lower costs as part of the OMB's FISMA Reporting Instructions
- **OMB Memo M-04-04** – Details methods for determining assurance to meet FISMA guidelines and is utilized as an integral part of Veracode's ratings.
- **State of Software** – The National Vulnerability Database lists over 3,400 hundred vulnerabilities disclosed in the 1st half of 2007 alone



Veracode Solutions for FISMA

The Federal Information Security Management Act of 2002, or FISMA, legislation created a framework of security requirements for federal agencies and their affiliates. Federal agencies must comply with its rules and report on the effectiveness of their IT security programs to the OMB and Congress. With a majority of attacks focused at the application level, it comes as no surprise that application security is becoming increasingly critical to achieving FISMA compliance.

Applications have become the organization's new perimeter and a prime target for data and financial theft. According to government statistics, software vulnerabilities have reached an all time high, with over 3,400 new vulnerabilities disclosed in the 1st half of 2007 alone. The government recognizes this fact and has incorporated vulnerability scanning into FISMA by using NIST 800-Series guidelines and tracks application vulnerabilities as part of the National Vulnerability Database project.

Achieve FISMA Compliance with SecurityReview

Veracode's SecurityReview helps agencies rapidly achieve FISMA compliance in a simple and cost-effective way. Veracode's automated on-demand service allows agencies to conduct application security testing on an as-needed basis and without the need for costly tools or time intensive consultative engagements. Also, with no hardware or software to buy, install, maintain or upgrade agencies drastically reduce both their capital and operational expenses related to FISMA compliance. Agencies simply enter application information through Veracode's secure on-line portal and receive reports and results within 24-72 hours.

Independent Review with Standards-Based Ratings

As an expert in application security, Veracode is in a unique position to provide an independent assessment and standards-based rating to ensure your applications comply with FISMA rules. Auditors require proof that your applications are free from vulnerabilities and they need a method to evaluate findings against a well-known industry benchmark. Veracode's Ratings System solves this issue by producing a software security rating based on respected government standards including NIST for definitions of assurance levels, MITRE's Common Weakness Enumeration (CWE) for classification of software weaknesses and FIRST's Common Vulnerability Scoring System (CVSS) for severity and ease of exploitability. These universally accepted vulnerability scoring methods provide auditors confidence that you have effective security controls in place.

"Businesses should urge all IT vendors to use CVSS in their vulnerability and patch reporting."

John Pescatore



Speed Remediation Veracode Fix First Analysis



Veracode's Fix First Analysis quickly identifies flaws to reduce the time & effort associated with FISMA compliance

Compliance Milestones



Veracode's On-Demand Service tracks your application's ratings over time, enabling you to meet FISMA's requirement to create a plan of action with compliance project milestones

Veracode Solutions for FISMA Compliance

NIST Implementation Guideline for FISMA	Veracode Solution
Audit and Accountability	Periodic Application Security Audits - Veracode's security-as-a-service (SaaS) model allows agencies to easily setup periodic security audits of their applications
Certification, Accreditation, and Security Assessments	Independent & Trusted Review - Veracode meets requirements as an organization specializing in application security. As a result, agencies can utilize Veracode to conduct third party application security assessments.
Risk Assessment	Vulnerability Scanning - Veracode's unique ability to scan both custom and commercially developed applications allows agencies to meet FISMA requirements for software vulnerability scanning.
System and Services Acquisition	GOTS & COTS Security - Veracode is the only solutions provider which can scan packaged GOTS and COTS applications without requiring access to source code, allowing agencies to embed security into their procurement process in accordance with FISMA requirements.
System and Communications Protection	Integrated gray-box testing - Veracode is the only vendor that integrates both dynamic and static binary code analysis without which tests not only for vulnerabilities, but analyzes applications for the presence or absence of security features as required by FISMA.
System and Information Integrity	Malicious Code and Backdoor Protection - Veracode is the only solutions provider who can identify the presence of backdoors or malicious code within applications per FISMA's requirements.

For More Information

For information on software security services, best practices, and methodologies, contact us at.

Veracode, Inc.
 4 Van de Graaff Drive
 Burlington, MA 01803
 Phone: +1.781.425.6040
 Email: contact@veracode.com
www.veracode.com

SecurityReview is a registered trademark of Veracode, Inc.