



Enforcing FISMA Regulations: NIST 800-53 And FIPS 200

The Federal Information Security Management Act of 2002 was put into effect within the United States in 2002. FISMA requires that government agencies operate secure computing facilities that are maintained by meeting recommended security controls and carrying out annual inventory, security and risk assessments. Documents that help agencies meet the requirements of FISMA Compliance are NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" and FIPS 200, "Minimum requirements for Federal Information Systems".

Although no single solution addresses all the security controls outlined by the NIST documents, our goal is to demonstrate how Nowell's offerings address some of the most important aspects of these documents.

This paper shows how Nowell's Shalom Software helps meet some of the most important aspects of these regulations by focusing on Access Control Enforcement, Auditing and Accountability of Information Systems.

WHAT IS SHALOM?

Shalom is a computer security tool that defeats Insider Threats such as Insider Information Espionage and Identity Theft. Information espionage occurs when trusted insiders leak information or compromise information systems. Identity Theft is a violation of access control policy – it happens when a hacker or an intruder steals a legitimate user's identity (such as a password or user name) and illegally gains access to information.

Shalom has the ability to prevent such threats by detecting anomalies in user behavior (for example, if someone is accessing sensitive information at 3 AM in the morning on the weekend when he normally is allowed access only at work during day time hours, that is an

anomaly). Bad insiders and ID thieves often exhibit anomalous, suspicious behavior that is highly unusual. Shalom has the ability to detect such behavior anomalies in computer accounts. It also reports and prevents intruders by additional authentication to the effect that unauthorized persons are identified and locked out of the system immediately. Shalom reports all anomalies, risks, and prevented intrusions to administrators for auditing and investigative purposes. According to the CSI/FBI Computer Security Survey, 70% of the risk of information loss is due to insiders. Shalom mitigates this risk factor using this method.

WHAT IS NIST SP 800-53? HOW DOES SHALOM HELP MEET THE MANDATES OF THIS DOCUMENT?

NIST 800-53 outlines some key areas of information security (called "security control families") that organizations must address to ensure a secure posture. One of them "Access Control" says that access to information should be restricted to only those person(s) who need that information. Shalom serves to strengthen the enforcement of access control policies. Shalom also enhances Audit & Accountability, Identification & Authentication Security Controls.

1. DIRECTIVE: Look out for anomalies in how access control policies are implemented (detect system, and network intrusions); use this information to fix security methods and processes.
2. DIRECTIVE: User accounts should be handled securely and should be managed properly [40]. Shalom enforces this policy by ensuring the integrity of computer accounts – that users do not have their computer accounts stolen or shared with anyone.
3. DIRECTIVE: Computer user accounts are at the heart of computer security - Shalom ensures the integrity of the computer account.
4. DIRECTIVE: Detect compromises such as use of expired or old accounts; Administrators should have a clear user account creation, suspension and termination policy that is enforced. Shalom locks out users who use their accounts in a

non-secure fashion by sharing passwords or leaving systems unattended. Shalom detects backdoor accounts.

5. Page 43 asks for USER ACCOUNT ACCESS ENFORCEMENT – Shalom was designed to ensure that user accounts are used as intended.
6. AC-3 DIRECTIVE: Ensure that user access is authorized; Shalom ensures this by preventing unauthorized users who behave suspiciously
7. AC-3 DIRECTIVE: Look out for access enforcement anomalies: Shalom does access anomaly detection of user accounts; By detecting and reporting anomalies, the Insider threat is addressed too; Shalom authenticates possible “bad insiders” and this serves as a clear deterrent.
8. AC-1, AU-2, AU-8 DIRECTIVE: Asks Administrators to review or audit the activities of users with respect to system security by looking out for anomalies – “indications of inappropriate or unusual activity” [52]. Shalom automatically will alert System Administrators to suspicious activities of users. It will tell which accounts have been compromised. This is an important answer to the Audit and Accountability requirements;
9. IA-2 asks for proper identification and authentication of users by various methods. Shalom authenticates persons using personal multifactor authentication on the observance of anomalies to prevent intruders [65].
10. Incident Response refers to the procedures that information security administrators follow after a compromise. Shalom offers tools to review suspicious events, and prevented attacks. This tool serves as a first step in carrying out proper incident response [69].

WHAT IS FIPS 200?

FIPS 200, "Minimum requirements for Federal Information Systems" is a document that outlines minimum requirements for the security of federal information systems

1. Access control directive: Ensure proper access controls: Organizations must ensure that information access is granted to only

those who are authorized. By detecting persons who try to gain unauthorized access, Shalom enforces this policy.

2. Audit and Accountability Directive: Organizations must take steps to audit (Record in detail) information systems enough to detect and prosecute unauthorized or inappropriate system activity; Shalom can be used as an audit tool to detect suspicious bad activity. Shalom provides effective reports that can be used for auditing purposes
3. Identification and Authentication Directive: Organizations must identify users using a unique user ID, and authenticate them; Shalom helps to enforce this requirement by ensuring that those who are logged in are who they claim to be using multifactor authentication of anomalous, unusual users.

CONCLUSION

FISMA compliance for any government agency is a long-term project requiring patience that will be addressed by a combination of several processes, people, security tools, and proper training. As was earlier said, no single product or solution can address all concerns, however Nowell’s security offering certainly goes a long way in helping meet FISMA compliance in some of the most important security control areas including Access Control, Audit, and Authentication.

In addition, Nowell’s Shalom AI will help defeat Insider Threats such as Information Espionage and Computer Identity Theft

NOWELL
SECURITY ENFORCEMENT
WWW.NOWELLGROUP.COM

Sources

- *National Institutes of Standards and Technology Special Publication 800-53 & FIPS 200*
- *The CSI/FBI 2003 Computer Security Survey*