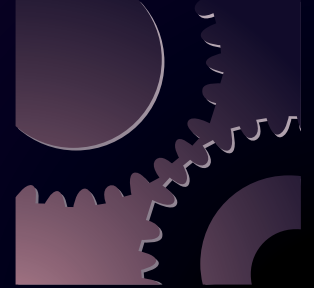


# PRESCRIPTIVE GUIDE SERIES



## FISMA:

ACHIEVING AND MAINTAINING  
COMPLIANCE TO ENSURE  
SECURITY OF SYSTEMS AND DATA

A TACTICAL GUIDE ENABLING YOU TO TAKE  
ACTION AND ACHIEVE OPERATIONAL EXCELLENCE.



The Leader in  
Configuration Audit & Control

# TABLE OF CONTENTS

About this Guide .....2

Why FISMA Matters.....2

Pressures of Compliance .....3

Annual FISMA Report Card.....3

Automating FISMA Compliance .....3

Tripwire and NIST Controls .....4

FISMA / Tripwire Federal Case Studies

    #1 CIO perspective.....6

    #2 Agency Information Systems Owner perspective .....7

    #3 Authorizing Official perspective .....9

Benefits of Tripwire for Continuous FISMA Compliance .....10

Next Steps .....11

*Tripwire software has been recommended, endorsed and/or certified by these agencies.*



## About this Guide

Tripwire has long been an important tool for federal agency IT departments, offering an iron-clad defense, or foundation for a layered compliance and security strategy.

This guide is intended to show how Tripwire® Enterprise can continue to help federal agencies, as well as the organizations that store, process or transmit federal information, and the contractors that do business with the federal government, by providing an automated method for meeting many of the most critical regulatory IT security standards of FISMA compliance.

This guide contains case studies from three fictional federal agencies, each capturing the perspective of a key stakeholder in the FISMA compliance process. The case studies highlight how a CIO, Information Systems Owner and Authorizing Officer approach and manage the internal issues of demonstrating FISMA compliance, and how they meet many of those challenges with Tripwire configuration audit and control solutions.

## Why FISMA Matters

In 2002, Congress passed and the President signed the E-Government Act, within which is Title III, the Federal Information Security Management Act (FISMA). This law requires federal agencies—and the foundations, educational institutions, and organizations that receive federal funds, as well as the contractors that do business with them—to develop, document, and implement information security programs to protect the confidentiality, integrity and availability of the data and systems that support agency operations, assets and mission.

In meeting compliance, agencies face a dual responsibility. First, is to meet the specific requirements established by NIST in support of the FISMA requirements; and second, is to be able to provide a risk-appropriate level of assurance that critical information security controls are operationally effective and producing the intended outcomes. In addition, agency officials are concerned that change management and configuration control are handled in a consistent and enforced manner to reduce vulnerabilities. According to the 2005 White House Office of Management and Budget (OMB) Annual Report to Congress on Implementation of FISMA, uneven implementation of security measures across the federal government leaves many weaknesses that must be corrected.

Above all, FISMA matters because in becoming compliant, agencies also become more efficient in their operations, and most importantly, more secure.

## Pressures of Compliance

Specifically, federal agencies are required to develop an agency-wide security program, and to implement and adhere to security configuration standards developed by the National Institute of Standards and Technology (NIST). Agencies must identify and resolve risks, and perform ongoing assessment and testing. They must also conduct annual reviews on the effectiveness of the agency's information security and privacy programs and report the results annually to the OMB.

Pressure to comply with FISMA is being felt at state, regional, local and tribal levels of government. Large agencies such as Homeland Security and the Department of Justice must comply, as well as smaller agencies, foundations, educational institutions, and organizations that receive federal funds, such as the National Gallery of Art and the Peace Corps. Private sector firms, including contractors that store, process or transmit federally owned data, must also meet FISMA compliance.

Understanding and reporting FISMA results each year can be a tedious process, much in part because it is a complicated, manual process with ambiguous guidelines. Agencies use various methods to collect the required security data, using databases, spreadsheets and other documents. There is no streamlined way to integrate all of the data coming in from various sources and methods. As one agency head recently remarked, FISMA reporting is "spreadsheet chaos."

Audit preparation time is also consuming and expensive. This is mainly because the implementation of the NIST control requirements can be an enormous effort, consuming significant budget and IT resources, all of which takes away from the agency's work on mission objectives. Funding can also be an issue. OMB reported agencies spent approximately \$5.5 billion in fiscal year 2006 to meet FISMA requirements. It is predicted that for agencies to comply with FISMA, it will require upwards of \$27.9 billion between 2008 and 2012.

## Annual FISMA Report Card

Each year, the House Government Oversight and Reform Committee issues a report card of federal agency progress in meeting FISMA requirements. With the need to balance time and resources, and the realities of high overhead in the early years of implementation, it's no wonder that so many agencies barely make a passing grade, or that many fail to report results. According to the OMB, the overall grade had been stalled at D or D+ for the previous three years. In 2006, seven agencies improved their grades, six performed worse than the year before, and 10 scored the same. Despite these inconsistencies, the committee did view the latest report card as showing "slow but steady improvement."

FISMA is a powerful motivator for improving federal IT security, and the annual report card has done a good job in helping to focus attention on this subject. But since the grades focus on targeted implementation data points (e.g., percent of contingency plans tested) rather than on overall information security effectiveness, it is possible to test, certify and accredit all your systems and get a splendid grade even if your systems continue to be subject to threats and vulnerabilities. To really secure systems and data, a new approach is needed that is tightly coupled to security requirements and uses automated solutions to implement and monitor key security controls.

## Automating FISMA Compliance with Tripwire Solutions

According to Gartner, Inc., "Government organizations that are required to meet FISMA compliance should use [compliance] as a control framework ... and for asset clarification. Use compliance as an opportunity to improve operational security not only by defining assets and documenting the current state of the organization, but also by implementing control objectives that drive effective risk analysis and management." Moreover, "Organizations should use compliance as an opportunity to implement technologies and processes that improve operational security as well as provide support for FISMA...compliance."<sup>1</sup>

In other words, given the choice of achieving good security through a focus on compliance or achieving compliance through good focus on security, the latter is always the more cost effective and sustainable option.

Achieving a known and trusted state is a challenging task for even the most technically adept and process-focused organizations. That's why more than 400 government agencies have adopted Tripwire software and service solutions to help radically simplify the task of automating the production of audit evidence necessary to demonstrate compliance with an ever-growing number of initiatives and requirements, and demonstrating that systems are in a known and trusted state. Tripwire enables this process by combining change detection and reporting with configuration assessment capabilities.

## **Configuration Assessment**

With configuration assessment, Tripwire Enterprise can proactively test and assess a server environment against pre-configured, out-of-the-box policies, helping to enable a minimal deployment window. Tripwire leverages industry standards, specifically benchmarks from the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), as well as the Defense Information Systems Agency (DISA). These benchmarks include tens of thousands of configuration assessments enabling automatic sustainable policy compliance testing for FISMA.

## **Change Detection and Reporting**

Tripwire Enterprise monitors file integrity and file structures on information systems, including hardware, software, network, and security infrastructure. It then provides detailed change audit information to enable agency staff to quickly pinpoint, analyze, and recover from any undesirable change. Tripwire delivers assurance that authorized changes are completed, and that unauthorized or ad hoc changes that circumvented policy are detected and immediately reported. With a verifiable audit trail, staff can then document every step to auditors or assessors and provide them with detailed reports that demonstrate changes made to information systems can be detected, corrections verified, and anomalies explained. The path from data to information to knowledge is quick and responsive.

## **Combination for Achieving and Maintaining Automated Compliance**

By combining change detection and reporting with configuration assessment, Tripwire Enterprise assesses every change as authorized, within policy and compliant, ensuring systems achieve a known and trusted state. Tripwire then helps maintain that known and trusted state by establishing a secure baseline to measure change against, and then monitors against that baseline through ongoing, tunable change detection and reporting.

## **Tripwire and NIST Controls**

In December, 2007, NIST released Special Publication 800-53 Recommended Security Controls for Federal Information Systems: Revision 2, which covers 17 security-related areas for protecting the confidentiality, integrity and availability of federal information and systems. These 17 areas include: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity.

Since the release of these high-level standards, NIST has begun to promote an Information Security Automation Program (ISAP) to enable automation and standardization of technical security operations. The ISAP strategic objectives include creating standards based automation of security checking and remediation and automating technical compliance activities (e.g. FISMA). ISAP's tactical objectives include enabling

# PRESCRIPTIVE GUIDE: FISMA

standards based communication of vulnerability data, customizing and managing configuration baselines for various IT products, assessing information systems, and reporting compliance status.

Tripwire can facilitate compliance with many NIST controls, especially operational and technical controls, by assuring that file system and registry objects and network device configurations do not change unexpectedly. The three case studies that follow identify specific NIST 800-53 controls that Tripwire change auditing solutions can help implement, maintain, and provide auditing proof. Tripwire can produce some or all of the required evidence of operational effectiveness for FIPS-199 Moderate-level systems in a mechanized and automated way (*see Table 1*).

CONTROL FAMILY	CONTROL	CONTROL FAMILY	CONTROL
<b>Access Control (AC)</b>	Account Management	<b>Configuration Management (CM) continued...</b>	Configuration Settings
	Access Enforcement		Least Functionality
	Information Flow Enforcement	<b>Contingency Planning (CP)</b>	Information System Backup
	Separation of Duties		<b>Identification and Authentication (IA)</b>
	Least Privilege	Device Identification and Authentication	
	Unsuccessful Login Attempts	Authenticator Management	
	System Use Notification	Cryptographic Module Authentication	
	Session Lock	<b>Incident Response (IR)</b>	Incident Handling
	Session Termination		<b>Maintenance (MA)</b>
	Supervision and Review: Access Control	Remote Maintenance	
	Permitted Action s/o Identification or Authentication	<b>Media Protection (MP)</b>	Media Access
	Remote Access		<b>Risk Assessment (RA)</b>
	Wireless Access Restrictions	<b>System and Communications Protection (SC)</b>	
<b>Audit and Accountability (AU)</b>	Auditable Events		Denial of Service Protection
	Content of Audit Records		Boundary Protection
	Audit Storage Capacity		Transmission Integrity
	Response to Audit Processing Failures		Network disconnect
	Audit Monitoring, Analysis, and Reporting		Cryptographic Key Establishment and Management
	Audit Reduction & Report Generation		Use of Validated Cryptography
	Time Stamps		Public Access Protections
	Protection of Audit Information	Session Authenticity	
Audit Record Retention	<b>System and Information Integrity (SI)</b>	Flaw Remediation	
<b>Certification, Accreditation, and Security Assessments (CA)</b>		Security Assessments	Information system Monitoring Tools and Techniques
		Continuous Monitoring	Information Input Restrictions
<b>Configuration Management (CM)</b>	Baseline Configuration		
	Configuration Change Control		
	Monitoring Configuration Changes		
	Access Restriction Changes		

**Table 1:** NIST SP800-53 Controls for Moderate Systems Addressed by Tripwire.

## FISMA/Tripwire Federal Case Studies

The three following case studies represent the challenges of FISMA compliance as seen through the perspectives of a federal CIO, Information Systems Owner and Authorizing Official. These case studies illustrate how Tripwire can help professionals/agencies meet specific FISMA objectives.

### Federal Case Study: CIO Perspective

Carmen Irvine-Osborn (fictitious name) has held the position of CIO for the regional offices of a major US Federal Agency for nearly 5 years. She has been a civil servant for nearly 30 years and is all too familiar with the challenges of meeting OMB, agency and local management mandates and objectives in the never-ending climate of budget constraints. Carmen recently hosted a planning session with the heads of the business and operational groups in her region. This annual workshop was intended to be the primary vehicle by which the business leaders in the region communicate to the IT department about their strategic and tactical directions in the coming year.

Carmen has used these meetings in the past as a way of helping the business leaders understand how information technology can help (and where it can't help) in meeting the objectives of the agency. Over the past several years she has found that her role in the dialogue was evolving more to one of being the enforcer of the standards and policies that put certain constraints on when and how IT can deliver business value. One of the highest visibility areas that Carmen found herself preaching about was information security, specifically the FISMA compliance requirements.

Many of the business leaders in the meeting carried the title of Authorizing Official in the context of the information systems for which Carmen's organization was responsible. Carmen knew that they had been through enough indoctrination regarding what being an Authorizing Official really meant that they were appropriately nervous about the formal act of *personally* accepting risk on behalf of the agency when they sign an Authorization To Operate for an information system. Between agency training and her own awareness campaign, she felt they were past the learning phase of the adoption curve and were now ready to have serious discussions about how best to spend scarce agency resources to achieve all priority objectives, including information security.

In many ways, Carmen was now paying the price for her success in raising the awareness of the expectations of the Authorizing Official. Now, instead of demanding to know how she was going to deliver the information technology products and services demanded by the agency, they were asking questions about how she was going to produce better, more accurate and more timely evidence of security control operational effectiveness. It seems the words from NIST's Dr. Ron Ross ("*The most dangerous person to an enterprise is an uninformed authorizing official*") were sinking in. Carmen knew that increasing the quantity and quality of evidence, particularly for FIPS-199 Moderate- and High-impact systems, would come at a cost, especially in light of the widely diverse approaches that her System Owners were taking in meeting the requirements.

Carmen gathered her System Owners and their Security Officers in a room not long after the business leader workshop and started the process of identifying and prioritizing the alternatives to step up to the more stringent evidence requirements and, hopefully, cut some costs along the way. She started the discussion by bringing all the stakeholders up to speed on the current OMB objectives relative to FISMA compliance. Now that the body NIST guidance documents created in support of the FISMA legislation were nearing completion, Carmen advised the team that the Office of the Inspector General (OIG) for the agency had made it clear that changes were necessary in the Security Assessment Reports, the primary output of the independent Certification Agent produced in the tri-annual (minimum) Certification and Accreditation process. No longer would it be acceptable to only provide evidence of those controls that were not operating effectively (negative reporting), but instead the assessment reports must now include specific and detailed evidence of those controls that *were* operating effectively (positive reporting).

Carmen reminded the System Owners of one of the NIST controls that was mandatory for all systems, control SA-2: Allocation of Resources. This control states, *“The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.”* So with the requirement that every system have a line item on their budget for security, Carmen wanted to know how much was being requested and what it was going to be used for. Her intent was to ensure that the monies spent on security were addressing the highest risks of the overall organization and were being spent in the most efficient ways possible.

In going around the table in search of best practices that might be leveraged throughout the organization, one system stood out. The owner of the Human Resources/Financial system was recommending the acquisition and deployment of Tripwire, a software solution focused on configuration assessment and change auditing. While many System Owners were recommending the purchase of one solution or another, the Tripwire solution seemed to be very tightly coupled with specific NIST controls and seemed to provide the kind of positive reporting evidence that the OIG indicated they would be looking for. The HR/Finance System Owner had provided a listing of the specific controls for which Tripwire could produce some or all of the required evidence of operational effectiveness for Moderate systems in a mechanized and automated way.

Carmen was intrigued by the possibility of one tool addressing so many critical NIST controls, and doing so in a way that meets the additional requirement placed on Moderate- and High-level systems to implement controls in a way that minimizes the degree of human involvement in the control’s operation. She quizzed the other System Owners regarding their plans to step up to the stringent evidence requirements for the 53 controls across 12 control families for which the HR/Finance System Owner was planning to use Tripwire as the implementation vehicle. Carmen reckoned that by deploying Tripwire across all systems, she could ensure that quality evidence of security control operational effectiveness could be produced and maintained in a uniform way that leverages the investment in software and training. By centralizing the implementation of these critical controls, essentially making them organizational common controls, she could satisfy a number of objectives that included higher quality control evidence, more cost effective production and maintenance of that evidence, more accurate and efficient response to audits and reporting entities and, most importantly, more secure systems.

## **Federal Case Study 2: Information System Owner Perspective**

Sarah Owens (fictitious name) carries the title of Branch Chief at a regional office of a US Federal Agency. Sarah’s role is to provide management and leadership to the administrative function within her region, which includes providing oversight to the information systems that support those functions. In the context of the agency’s FISMA compliance requirements, Sarah wears the hat of the System Owner.

The business functions supported by Sarah’s system would likely be found in most agencies (Financial reporting applications, Human Resource applications, Funds Distribution applications). While there are elements of these business functions replicated (complemented) to some extent at agency headquarters, Sarah’s system generally supports an agency-wide user community. Fortunately, the computing and storage infrastructure is largely centralized in a data center-class environment. Remote computing components exist in branch offices throughout the country, but the wide-area network fabric is provided by a central agency resource and offers tiered service levels.

Sarah’s accreditation boundary includes all the centralized and remote computing, storage and local area networking infrastructure, but not the wide-area network or any desktop/laptop/pda device as these were covered in other system accreditation boundaries. A number of Interconnection System Agreements (ISA) and Memoranda of Understanding/Agreement (MOU/A) are in place to support these interfaces. In addition, a number of agreements are in place to support both internet (VPN/HTTPS) and point-to-point (T1) data connectivity to external service providers (database support, software development, business partners).

One component of each of these agreements is language that establishes mutual expectations relative to visibility into the security control posture of the other party. On behalf of the agency, Sarah has expressed her intent to ask for and receive specific information from those with whom her system trades data regarding the strength and operational effectiveness of their security controls. Likewise, the external parties have expressed their intent to receive from Sarah some form of confirmation that her system is indeed providing the necessary protections for their data that is stored, processed or transmitted by her system. Trust but verify.

Following the FIPS-199 standard and the SP800-60 guidance, Sarah had selected three information types resident in her system:

C.3.2.3 Budget and Finance

C.3.2.2 Reporting and Information

C.3.5.4 Infrastructure Maintenance

This resulted in an overall high-water mark of Moderate. Having received an Authorization to Operate just over two years ago, Sarah knew that the tri-annual C&A cycle was coming up. She also knew that the NIST guidance had evolved a good deal in the past two years and that the baseline for acceptable evidence of control operational effectiveness was becoming solid and actionable. NIST SP800-53A: *Guide for Assessing the Security Controls in Federal Information Systems* is ready for prime time and is painfully clear regarding what constitutes acceptable evidence for audit purposes. Sarah's analysis of the guidance showed that at the Moderate level, there is a requirement to implement more controls as well as a number of control enhancements to make the control more robust. In addition, there was also a general expectation that the implementation of a given control rely less on manual (human) processes and more on mechanized (automated) tools. Doing so is one way to help ensure a higher degree of reliance on ongoing effective control performance.

Sarah's next challenge was to identify which of the 154 controls and 33 control enhancements that are required for a Moderate system could be satisfied in a way that meets the letter and spirit of the "automation" requirement. And of those control candidates, which offer the most bang for the buck in terms of buying down risk.

She already used agency standard systems and processes for account request, approval and management (Identification and Authentication control family), although some elements of the continuous monitoring requirements still fell upon her local system resources (regular access log and user list reviews). A centralized IT security group performed regular vulnerability scans on her system elements and provide reports and action items based on the results. Often these actions involved the timely application of vendor software patches and firmware upgrades, something her local system administrators were responsible for doing.

Sarah was comfortable with the current state of the controls in families such as Maintenance, Media Protection, Physical and Environmental Protection, Planning, Personnel Security, Contingency Planning, System Services Acquisition, Awareness and Training, System and Communication Protection. She felt they were highly leveraging agency common processes and standards, and were lower candidates for further automation.

That left a few key families of controls that could, with relatively minimal resource investment, be deployed with a degree of automation and repeatability that satisfies the control integrity requirements of a standard audit process. Sarah's technical staff had already been able to cobble together some semblance of automation

to a log file aggregation process that was being used in an attempt to satisfy a number of controls in the Audit and Accountability and System and Information Integrity families, but she knew that this solution would not pass muster in the new NIST world. A draft business case was floated a couple of years ago to make the case for the acquisition of a product from Tripwire which promised to satisfy the automation requirements of a number of critical controls.

Eleven controls and 7 control enhancements were attractive to address, but in the context of other priorities two years ago, the business case just wasn't strong enough to warrant the expense. After researching Tripwire Enterprise, Sarah determined that not only could it still satisfy the eleven controls and 7 control enhancements of the previous version, it now had the capability to address an additional 42 controls and 15 control enhancements across seven control families! Now we're talking about a significant percentage of the total required controls. And the nature of those candidate controls were among the highest priority ones, those that represent some of the greatest risk categories that are most vulnerable when deployed in a manual process. Now that's low hanging fruit!

Knowing which controls could be addressed by Tripwire Enterprise and how, Sarah felt it would be a fairly straightforward process to calculate the cost to manually execute and manage these important controls and what level of control operational performance might be expected by such an approach. She felt confident that the value of the acquisition and deployment of Tripwire would be easily realized by her technical staff who would benefit from more time to address more critical issues, by her Authorizing Official who would take solace in the knowledge that the residual risks are as low as they can be, and by her CIO who can step up to a major and essential security requirement with a relatively low investment.

### **Federal Case Study 3: Authorizing Official Perspective**

Andrew O'Reilly (fictitious name) has been both a contractor and a civil servant at a major U.S. Federal Agency for almost 30 years. Today he holds the title of Associate Director for Operations and is responsible for oversight of the agency's business functional support processes and systems. Having held positions in the finance organization, in human resources and in the procurement group, Andrew now finds himself in a senior position with responsibilities over all those business functions and more. In the context of the agency's FISMA compliance strategy, Andrew wears the hat of the Authorizing Official for a number of information systems.

Earlier in the year, as a part of the agency's informational awareness program relative to the FISMA agenda, Andrew attended a webcast that included speakers from his own agency, from OMB and from NIST. One comment on a slide used by Dr. Ron Ross of NIST said, "*The most dangerous person to an enterprise is an uninformed authorizing official.*" These words resonated with Andrew, as he was painfully aware that a core premise of the FISMA legislation was to ensure that a single, named senior agency official was fully accountable for the security posture of the information systems under their control. By signing an Authorization To Operate (ATO) letter for one of his systems, Andrew was essentially personally accepting the residual risks resident in the system on behalf of his agency.

Andrew had signed ATO letters in the past, but this was the first year in which his signature was based in large part on the Security Assessment Report (SAR) generated by the Certification Agent (CA) as an output of the just-completed Certification and Accreditation activities. He was well aware of the hoops through which his staff members were recently jumping to produce all the documentation and evidence required for the independent certification of his Moderate-level systems.

With a new ATO for his HR/Finance applications (included in a single system accreditation boundary) on his desk waiting for his signature, and Dr. Ross' comment fresh in his mind, Andrew began to dig into the SAR in the hope that he would find the kind of evidence of security control operational effectiveness that would help

him sleep better at night. Too often in the past, he had been presented with CA conclusions and recommendations regarding some of the required baseline controls which were *not* operating effectively or producing the outcomes intended, but little or no information (evidence) regarding controls that *were* working well.

This “negative reporting” worried Andrew. While he clearly needed to fully understand where the highest risks were, the likelihood and potential severity of those risks and the recommendations to mitigate them, he was not comfortable in placing his entire reliance on the operational effectiveness of the rest of the security controls based simply on the lack of a finding from the CA. What he wanted to see was tangible, current and reliable evidence of the operational effectiveness of all security controls. However, he knew that the management and technical staff of the HR/Finance applications were not among the loudest requesters of resources as they went through the audit process and he was concerned that this might translate into an assessment report that was light on real, quality evidence. After all, how could an organization that wasn’t asking for more resources and time possibly produce the kind of evidence of control operational effectiveness that would make an Authorizing Official completely comfortable in personally accepting all residual risk on behalf of the agency? How strong could their body of evidence be given their limited time and resources?

Indeed, as he read through the SAR, there were some of the 154 or so required NIST controls that had apparently been implemented, but for which valid evidence of the ongoing and continuous operational effectiveness was not present. For these, Andrew would have to rely on the lack of an audit finding to justify his decision to authorize the system for operation, or he could deny the system the authorization or issue an interim authorization pending the production of adequate evidence, neither of which were very attractive alternatives. Essentially, the System Owner and Certification Agent were saying “trust me” but Andrew knew it was his neck on the line.

But somewhat to his surprise, many of the controls tested by the CA did include evidence of ongoing control operational effectiveness, and these were some very critical, high risk controls at that. Andrew found reports generated by the Tripwire Enterprise utility that his team had installed a year ago. He recalled signing the purchase request for that utility for his HR/Finance System Owner based in large part on the promise of more effective and efficient adherence to FISMA requirements, and here was the tangible manifestation of that value in the Security Assessment Report.

Andrew found system (not human) generated evidence of the effective operation of 53 controls and 33 control enhancements across 12 control families. The failure of any of these controls could have a serious impact on the organization and agency, and knowing that the continuous monitoring of these controls was being accomplished through a proven and robust system utility, Tripwire Enterprise, Andrew felt very comfortable in signing the Authorization To Operate letter. After he did, his next call was to the owners of the other information systems in his organization to find out how they planned to leverage opportunities to mechanize and automate major elements of the control requirements, and how they planned to reduce the costs associated with the error-prone manual control monitoring processes in use today.

Tripwire, it seems, helped Andrew to sleep better.

## **Benefits of Using Tripwire to Help Manage FISMA Compliance**

Tripwire Enterprise is uniquely suited to the FISMA task. Tripwire configuration audit and control software detects every change made to the IT system, alerts when an unauthorized change is made, and assesses each change is within policy. Tripwire can facilitate compliance with many NIST controls, particularly operational and technical controls. By using Tripwire, federal agencies and their associated organizations can achieve and maintain a known and trusted state across their IT infrastructure.

Tripwire has worked with hundreds of agencies to ensure file integrity, improve security and operations, and provide the verifiable audit trail required of FISMA. Now with configuration assessment, Tripwire can

automate much of the FISMA compliance process with a deliberate and controlled approach to maintaining system and application integrity. The value Tripwire offers is immediate:

- **Reduce time and resources spent demonstrating effectiveness of IT controls.** Tripwire gives you the proof required to verify compliance with a single, verifiable audit trail. With Tripwire, you receive sophisticated, automated reporting required to complete quarterly and annual audits. Tripwire helps reduce the resources required to prepare for audits.
- **Maintain continuous compliance.** Tripwire exposes unauthorized changes through reconciliation with expected changes and allows IT staff to immediately identify any exceptions and trigger remediation of configurations that do not conform to policy, helping to meet the continuous monitoring requirements of FISMA.
- **Mitigate security risks.** Tripwire enterprise monitors and reports on every change made across the data center regardless of source, detecting unauthorized change and non-conforming configurations to proactively discover and manage security and compliance posture.

Tripwire solutions have a history with government agencies, offering an 'iron-clad defense,' or foundation for a layered compliance and security strategy. This has enabled public sector IT staff to protect electronic government assets from loss, misuse, or unauthorized access and modification. Now, with configuration assessment for FISMA policies, Tripwire offers an automated method for achieving and maintaining compliance.

## Next Steps

When working to achieve and maintain FISMA compliance, improve your agency's security posture, or increase operational efficiency, working from a common set of requirements and best practices will enable your agency to be successful. Meeting many of the requirements laid out by NIST 800-53A require an ability to assess configurations as well as detect and audit change within the IT infrastructure. Configuration Audit and Control will help you achieve and maintain the integrity of all IT configurations.

Tripwire, Inc. is the recognized leader of configuration audit and control software solutions, serving over 6,000 enterprises worldwide. As the first in the industry to combine configuration assessment with configuration change auditing, Tripwire ensures organizations reduce the effort required to maintain IT configurations, reducing risk, automating compliance and improving service availability.

## Learning from Others

Extensive information and other resources for helping your achieve your compliance, security, and operational goals are available from Tripwire. Resources mentioned throughout the Guide will help your organizations take the next step toward regulatory compliance, increased security, and improved service availability. Visit [www.tripwire.com/fisma](http://www.tripwire.com/fisma) or call toll free, 1.800.TRIPWIRE for more information.

<sup>1</sup> Gartner, Inc., "Findings From 'Security and Risk' Meeting: Augment FISMA Reporting with Technical Controls to Improve Operational Security," Amrit T. Williams, John Pescatore, April 4, 2006.



[www.tripwire.com](http://www.tripwire.com)

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182  
326 SW Broadway, 3rd Floor Portland, OR 97205 USA