FORTRA™

GUIDE (TRIPWIRE)

FISMA SI-7 Buyer's Guide

Evaluating Your Next Compliance Solution

The Federal Information Security Management Act (FISMA) tasks government agencies with a major organizational, technological, and budgetary challenge. It can be hard to know how to best allocate your agency's resources and talent to meet FISMA compliance, and a big part of that challenge is feeling confident that you're choosing the right cybersecurity and compliance reporting solution.

This buyer's guide focuses on one of the most difficult security controls agencies must adhere to: NIST SP 800-53 SI-7. The SI-7 ("SI" meaning "System Information and Integrity") control instructs agencies on software, firmware and information integrity. As of 2017's executive order, "Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk."[1]

Government systems are categorized as low, moderate or high sensitivity. All controls are mandatory for everyone, but the set of mandatory controls gets larger for moderate- or high-sensitivity agencies. The subset of SI-7 controls that are most relevant to the largest numbers of agencies are 1, 2, 5 and 7. While an adequately-robust security and compliance solution will cover all SI-7 controls, the following are the subcontrols that typically require the most attention.

SI-7.1: Integrity Checks

As identified in NIST SP 800-53, "Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort."[2]

Questions for your vendor:

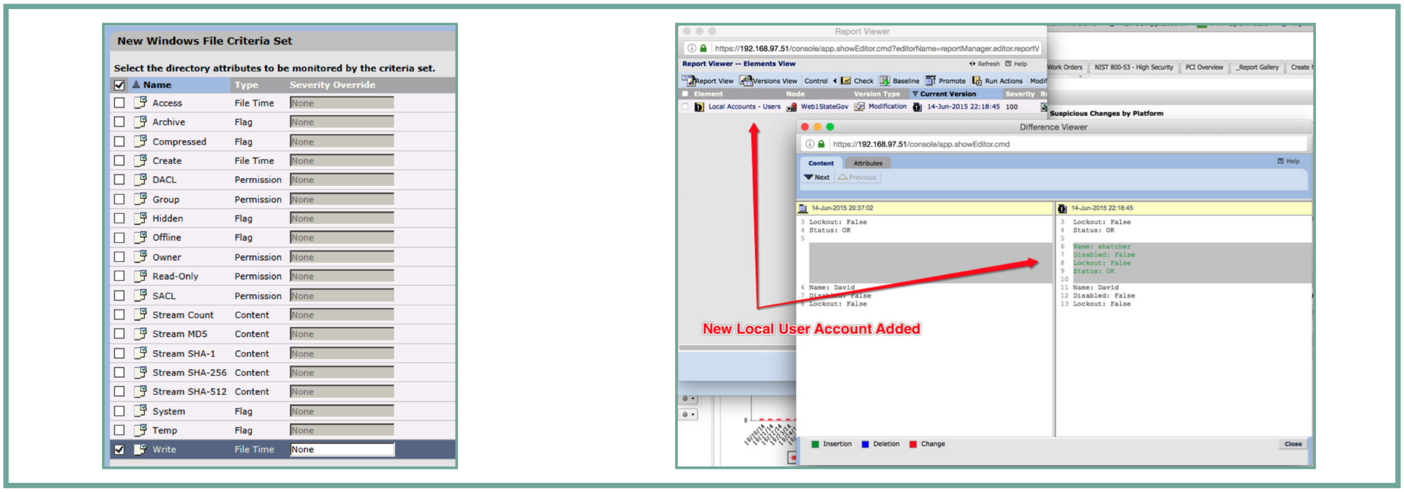
- Does it cover the full scope and range of assets, including Windows, Unix, Linux, routers, switches, firewalls and storage devices?
- Does the solution cover firmware? Can the solution perform checks while systems are In transition?
- In environments with rapid provisioning, does the solution integrate with virtualization, cloud and DevOps tools so that it's present when a new system is spun up?
- Can it detect the presence of a new threat (like a new hash) without having to rescan (i.e., in real time)?

SI-7.2: Automated Notifications of Integrity Violations

NIST SP 800-53 states, "The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers."

Questions for your vendor:

- Can it detect and alert on changes in real-time? Periodic scans can miss changes that are reverted back.
- Can It detect and alert on changes to attributes, such as the actual time of file modification if real-time Is not available?
- Can it filter expected, accepted and routine change, so as to only alert on changes that need to be investigated?
- Can it target changes that have been identified by MITRE ATT&CK or other cybercrime frameworks, so as to proactively identify changes of greatest concern?



New Windows File Criteria Set

Select the directory attributes to be monitored by the criteria set.

☑	Name	Type	Severity Override
□	Access	File Time	None
□	Archive	Flag	None
□	Compressed	Flag	None
□	Create	File Time	None
□	DACL	Permission	None
□	Group	Permission	None
□	Hidden	Flag	None
□	Offline	Flag	None
□	Owner	Permission	None
□	Read-Only	Permission	None
□	SACL	Permission	None
□	Stream Count	Content	None
□	Stream MD5	Content	None
□	Stream SHA-1	Content	None
□	Stream SHA-256	Content	None
□	Stream SHA-512	Content	None
□	System	Flag	None
□	Temp	Flag	None
☑	Write	File Time	None

Report Viewer

https://192.168.97.51/console/app.showEditor.cmd?editorName=reportManager.editor.reportV

Report Viewer -- Elements View

Element	Node	Version Type	Current Version	Severity
Local Accounts - Users	Web1StateGov	Modification	14-Jun-2015 22:18:45	100

Suspicious Changes by Platform

Difference Viewer

https://192.168.97.51/console/app.showEditor.cmd

```
14-Jun-2015 20:37:02
3 Lockout: False
4 Status: OK
5

6 Name: David
7 Disabled: False
8 Lockout: False
```

```
14-Jun-2015 22:18:45
3 Lockout: False
4 Status: OK
5
6 Name: ahatcher
7 Disabled: False
8 Lockout: False
9 Status: OK
10
11 Name: David
12 Disabled: False
13 Lockout: False
```

New Local User Account Added

Examples of actionable integrity check results.

- Is the system capable of tracking ownership, mission, management, FISMA group and location for each asset, so as to be able to report and alert appropriately?

SI-7.5: Automated Response to Integrity Violations

As identified in NIST SP 800-53, "Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur."

Questions for your vendor:

- Does the solution have the ability to take action on the endpoint? Can you create actionable workflows?
- Can the solution create a ticket in an ITSM system (like Remedy or ServiceNow) when required?
- Can the solution be instructed to act completely automatically—to quarantine or otherwise disable a system—in the case of serious anomalies (such as the appearance of a new executable)?
- Can the solution integrate with multiple sources of threat intelligence data streams to detect and identify malware and act accordingly?
- Can the solution capture the contents of system firmware? Can the system alert If there are deviations from approved firmware?

SI-7.7: Integration of Detection and Response

NIST SP 800-53 states, "Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges."

Questions for your vendor:

- Does the solution create an initial baseline of each asset? Are all monitored changes kept so that it's possible to review the history of changes over time?
- Can it compare the state of an element at one time to its state at an earlier or later time?
- Can it present changes in a side-by-side format that readily enables the viewer to see insertions, deletions and modifications from one point in time to another?
- Does the system present the information in a way that readily supports documentation for further security review or legal action?
- Does the system have the ability to assess authorized change vs. unauthorized change via integration to an CM ticketing system?

SI-7 Control Description and Supplemental Guidance from NIST

According to NIST SP 800-53, organizations

1. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and
2. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications."

—National Institute of Standards and Technology[2]

Tools and Solutions for SI-7

To comply with SI-7, agencies must find a tool that not only does integrity monitoring, but also automates notifications and responses to violations and then keeps track of those violations. That's a lot to ask of a single solution, although possible if it has a robust enough integrity monitoring toolkit.

Each and every data breach can be tracked to a file or configuration change. So if you can detect each new unexpected change as it occurs, you can remediate it and return your system back to a secure, hardened baseline.

This FIM solution should provide you with:

- Visibility into new threats—Perform Integrity checks against your systems during transition (SI-7.1)
- Real-time alerts on file and configuration changes (SI-7.2)
- Actionable event workflows that can isolate or shut down non-compliant systems (SI-7.5)
- Historical access to all deviations from approved system baselines, track historical events (SI-7.7)

The table below offers a more granular look at the types of change data your FIM solution should provide, and the benefit to tracking each type.

More Key Questions for Your Vendor

Not all FIM solutions run the gamut of what you need to meet and maintain continuous SI-7 compliance. When speaking to your compliance vendor, these essential questions will help you determine the quality of the solution in question:

- Does it monitor the file and system integrity while also covering the full scope and range of my assets?
- Does it generate automatic alerts as soon as a change occurs on my files or configurations?
- Does it walk you through remediation instructions to bring my systems back into compliance?
- Does it integrate with ITSM processes and other tools in my IT ecosystem?
- How does this tool help streamline and optimize proof of compliance in the audit process?
- Can you run Compliance reports without the need to rescan endpoints?
- Is the alerting and remediation capability robust enough to help you maintain a defined compliant state?

Examples and Benefits of Change Details

Change Feature	Benefit
Monitor for changes with over 65 attributes of a file or configuration to consider with attributes like file hash values (MD5, SHAH-1, etc.)	Deep understanding drives more accurate remediation
Version tracking to view each version of a file/configuration over a period of time	Historical understanding provides better decision making and delivers audit-ready evidence
Ability to detect users making changes, without requiring native OS auditing	Removes complexity of detecting changes
Ability to monitor any device with SSH or Telnet capabilities	Not complex and cumbersome since it's agentless and discovers difficult protocols
Scales to cover the entire IT stack (virtualization, cloud, physical/virtual servers/desktops, applications (databases, directory services, web applications, Exchange), network devices (routers, switches, firewalls and any other device that can utilize SSH)	Comprehensive coverage assures broad and deep security
Used wiht the Tripwire Dynamic Software Reconciliation app, Tripwire Enterprise matches patch changes to patch manifests	Quickly zero in on changes that aren't associated with patch activity during the patch window
Understand good vs bad changes based on context from the change management process and their potential impact on security	Minimize false positives, focus on the true problems
Automatically monitor changes on newly installed applications	Gain real-time change insights
Allowlist users, ports, services and applications, and alert/take action on unauthorized matches	Comprehensive and fast detection of potential threats
Kill unauthorized processes, uninstall unapproved applications, and isolate endpoints	Enforce integrity requirements and enhances security
Easily view side-by-side comparisons	Quick assessment of changes delivering faster remediation
Offers key insight into change events over a period of time	Gain better intelligence to make better decisions
Offers key insight into the vulnerability risks on assets	Better and faster risk assessments

Tripwire Enterprise and SI-7 Compliance

As a leading compliance solution provider, Fortra's Tripwire experts and engineers have ensured that implementing Tripwire® Enterprise will align your agency with audit-ready SI-7 compliance. Tripwire is the inventor of FIM. As such, file and system integrity monitoring is at the core of what we've been perfecting since 1997.

For over twenty-five years Tripwire has helped government customers baseline the key configurations of their critical systems (including content, file attributes and hashes), detect changes to those files and configurations in real-time and near real-time, and most importantly, to rapidly identify which of the thousands/millions of changes taking place each day need to be investigated and/or remediated.

Of course, Tripwire Enterprise covers more than just the SI-7 subcontrols covered in this guide. Conversely, if you only need FIM without Tripwire Enterprise's policy and remediation capabilities, you can opt for Tripwire File Integrity Manager instead.

This is how Tripwire Enterprise maps to the numerous subcontrols:

- **SI-7.1:** Tripwire directly provides SI-07 (1) controls for software and hardware with real-time agent-based file integrity management and critical change control. Tripwire Enterprise provides monitoring rules and hardening policies that cover all aspects of the file system (including services, ports, firmware and command-based configurations) to keep your systems secure.
- **SI-7.2:** In support of SI-07 (2), Tripwire Enterprise and Tripwire LogCenter® provide a full suite of alerting and actionable event workflows should integrity violations occur.
- **SI-7.3:** Tripwire Enterprise and Tripwire Log Center support the enforcement of customer defined requirements for SI-07(3) with centrally-managed consoles which can be deployed to support on-premise, cloud-based and hybrid infrastructure models.
- **SI-7.5:** In support of SI-07 (5), Tripwire Enterprise and Tripwire Log Center provide a full suite of alerting and actionable event workflows should integrity violations occur. Actionable workflows can be set to isolate or shut systems down in the event of a violation.
- **SI-7.6:** Tripwire Enterprise meets SI-07(6) controls by collecting and utilizing the MD5, SHA-1, SHA-256 or SHA-512 hash values on all file system elements it monitors. It then alerts if a change occurs that reflects a deviation from those hashes. Tripwire products also leverage FIPS-140-2 and TLS for fully-encrypted communications.
- **SI-7.7:** Tripwire products directly provide SI-07 (7) controls for software and hardware with real-time agent-based file integrity management and critical change control. Tripwire Enterprise offers cybercrime and MITRE ATT&CK dashboards that can monitor security-relevant changes of interest to the agency, regardless of whether or not those changes trigger a change to policy compliance.

  Tripwire products also provide monitoring rules and hardening policy that cover all aspects of the file system—including services, ports, firmware and command-based configurations—to keep your systems secure. We also provide a full suite of event collection, normalization, correlation and reporting techniques. Our monitoring includes a full set of response alerting and actionable workflows which can isolate systems should the need arise.
- **SI-7.8:** Tripwire Enterprise and Tripwire Log Center support the enforcement of customer defined SI-07(8) control policies and procedures by monitoring all aspects of the file system. Actionable workflows can be set to isolate or shut systems down in the event of a violation. Tripwire Enterprise has the ability to capture and forward audit events to Tripwire Log Center, or to one of many other SIEM tools on the market.
- **SI-7.9:** Tripwire Enterprise and Tripwire Log Center support the enforcement of customer-defined SI-07(9) control policies and procedures by monitoring items such as startup tasks, scheduled tasks, cron jobs, firmware changes and more. Tripwire Enterprise maintains a baseline of critical system components and will alert when any deviation from that baseline occurs. Tripwire Enterprise also Includes the ability to perform integrity checks at boot to ensure no tampering has occurred.
- **SI-7.10:** Tripwire Enterprise supports SI-07(10) by providing firmware rules which can be used to identify,

alert and take action against detected baselined firmware changes at boot. Tripwire Enterprise can also run integrity checks against installed software, startup and scheduled tasks, or any other defined task at boot, helping to ensure the systems integral state has not changed. Tripwire Log Center supports both aspects of event collection and alerting related to changes to firmware. It is critical to note that Tripwire Enterprise will also alert when new binary files are added to your system for the purpose of malicious activity.

- **SI-7.11:** Tripwire products can run with limited privileges, with monitoring abilities set by the privileges assigned. Tripwire also supports SI-07(11) by providing both rules and policy tests which can be used to collect all attributes related to limited privileges on file system components. Tripwire will alert when user defined privileges change or are altered. Tripwire Enterprise and Tripwire Log Center function well in confined physical locations and in virtual environments.
- **SI-7.12:** Tripwire's allowlisting capabilities can ensure user installed software is authorized by a defined "allowlist" of authorized software, and alert and take action on software which is not authorized. We also support this requirement by ensuring the primary components for installed software have not been modified from their baseline at installation. Once software is installed, Tripwire Enterprise can baseline, monitor, and alert in real time if components of that software have been modified, ensuring admins that the software is valid and not compromised. Tripwire can also compare software packages to the same software packages on other systems.
- **SI-7.13:** Tripwire products support SI-07(13) with rules and policy tests which can be used to monitor software components (including configuration files and file attributes) for software with limited or no warranty, or from unknown sources. Tripwire products will alert when changes to those software components occur. Tripwire can also alert if software is installed/running on systems it is not authorized to execute on.
- **SI-7.14:** Tripwire Enterprise can prohibit the use of software from sources with limited or no warranty (without source code present). Tripwire will alert in real time when software that is unauthorized is installed or executed. We do this by 1) baselining services and or processes that are authorized on endpoints and alert when new services or processes startup, and 2) using our optional allowlisting capabilities to allow alerting when unauthorized software or services are installed or running. While Tripwire Enterprise does not block software from executing, it can stop software from running or take actions to delete software, move software to quarantine and isolate systems once detected..
- **SI-7.15:** Tripwire Enterprise includes rules that validate trusted certificate authorities and policies that validate CA Cert directory and file settings, as well as root certificates, LSA authentication and security packages, and many others.
- **SI-7.16:** Tripwire Enterprise supports this by monitoring changes to task and cron schedulers. Tripwire does not set timers on software that is running, but can alert when software is started or stopped.
- **SI-7.17:** Tripwire Enterprise can support this control by ensuring deployed software is authorized, and that hash Information on software installers matches known cryptographic algorithms. In addition to ensuring the integrity of deployed software and support binaries, Tripwire's allowlisting capabilities can ensure deployed software is only operating through authorized ports assigned to the software. Tripwire also offers a Pen Testing service where a team of highly-skilled cybersecurity experts utilizes a combination of tactical and strategic approaches to discover and exploit vulnerabilities in your IT systems.

In short, Tripwire Enterprise—deployed out of box—has the ability to discover and act upon suspected cyberattacks. It can baseline files, directories, registries, and software components. Tripwire Enterprise can also baseline accepted listening ports and authorized software, ports, services, processes, and users—for instance, it will send alerts and take action when new listening or established port sessions take place. Our cybercrime capabilities help to keep your systems safe and secure.

References

1 https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure
2 https://nvd.nist.gov/800-53/Rev4/control/SI-7