cimtrak
detecting change throughout the enterprise

cimcor.com

UTILIZING CIMTRAK FOR COMPLIANCE WITH NIST 800-171 CONTROLS

When most people think of the Federal Information Security Modernization Act (FISMA) they immediately think of the security of IT systems and data at U.S. federal agencies. What is often not considered is the fact that sensitive data is often shared with federal contractors. NIST special publication 800-171 deals with the unique risk that exists when information is not directly controlled by an agency.

While 800-171 chiefly serves to define requirements, which protect information confidentiality, it also discusses the necessity of ensuring the integrity and availability of U.S. federal government data through the implementation of a comprehensive IT security program. For this reason, special publication 800-171 also maps its requirements to the broader NIST 800-53 controls.

Trusted by numerous U.S. federal government agencies and contractors, CimTrak helps these entities in complying with many facets of 800-171. This document describes the requirements that CimTrak assists with, how it helps meet those requirements, and additionally provides the mappings between NIST 800-171 and 800-53.

CIMCOR

800-171 REQUIREMENT	HOW CIMTRAK HELPS	800-53 MAPPING
3.3 AUDIT AND ACCOUNTABILITY		
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. 3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	CimTrak detect changes across a broad ranges of systems and applications in the IT environment and generates comprehensive audit trails and reporting. Audit trails and reports generated by CimTrak include information on "who" is making a change so that it can be directly traced to a system user. CimTrak's ability to capture information in real-time means that abnormal change events can be investigated immediately, thus ensuring the maximum security of sensitive data.	AU-2, AU-3, AU-3(1), AU-6, AU-12
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	CimTrak can seamlessly send change events to most any Security Information and Event Manager (SIEM) where they can be further analysed and correlated. Integration with a SIEM is easy and done directly from the CimTrak Management Console.	AU-6(3)
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.	CimTrak provides real-time audit information and can generate reports on a set schedule, or on demand. Both audit trails and reports are extremely detailed and provide a wealth of information regarding changes including "who" made the change, "what" exactly changed, "when" it changed, and "what process" made the change.	AU-7
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	CimTrak audit trails are stored within the CimTrak Master Repository in an secure, encrypted format where alterations are not able to take place.	AU-9
3.3.9 Limit management of audit functionality to a subset of privileged users.	Viewing of CimTrak audit data can be restricted to only certain, approved users.	AU-9(4)

800-171 REQUIREMENT		HOW CIMTRAK HELPS	800-53 MAPPING
3.4	CONFIGURATION MANAGEMENT		
3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	CimTrak's core competency is to keep data secure by establishing, maintaining, and monitoring system baselines. Baselines can be created at any point throughout a systems lifecycle. System baselines are securely stored within the CimTrak Master Repository where they are monitored for changes. Changes to a system's baseline can be tracked over time and alerts issued should an unexpected change occur, indicating a possible compromise.	CM-2, CM-6, CM-8, CM-8(1)
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	As indicated above, CimTrak tracks information system baselines in order to track changes and create an audit trail which can be reviewed in order to identify malicious or unapproved changes. With CimTrak's integrated Ticketing Module, changes can be automatically approved and promoted to the baseline or be disapproved and removed from the baseline. Further, notes can be entered with change justification and the module supports multi-level approval structures. The CimTrak Ticketing Module can be used as a stand-alone solution for organizations without an existing system, or easily integrated to a third-party system.	CM-3
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	CimTrak can provide an inventory of which programs, ports and services are running on a system. This allows unused or uneeded program, ports and services to be restricted or disabled, maximing system and data security.	CM-7(1), CM-7(2)
3.4.9	Control and monitor user-installed software.	CimTrak can identify user-installed software in order to ensure uneeded or unallowed software is not installed.	CM-11

WHY CIMTRAK?

Relied upon by organizations of all sizes including numerous Fortune 500 companies and government agencies, CimTrak offers users a full-featured file integrity monitoring solution that is simple to install, configure and manage, all without the budget busting price tag and complexity associated with many FIM solutions. CimTrak's unique SmartFIM™ technology means that you get more done in less time, saving your organization both time and money. Backed by a world-class support team, CimTrak users rest assured that their systems are always in a state of constant integrity.

CIMTRAK IS SECURITY

CimTrak has been built with the stringent needs of government customers in mind. CimTrak has been certified to Common Criteria EAL Level 4 + FLR, the highest government certification for a software product. In addition, the CimTrak cryptographic module has been certified to meet the Federal Information Processing Standard (FIPS)140- 2. Further, your critical data is secure. All communications between CimTrak components are fully encrypted and the CimTrak Master Repository stores your files and configurations in both a compressed and encrypted form. No other integrity and compliance tool can match these stringent safeguards to protect your information.