NIST 800-171 & CMMC Requirements

Do you have contracts with the United States Department of Defense (DoD) or are you a subcontractor to a prime contractor with DoD contracts? If so, are you prepared for NIST 800-171 requirements? Do you understand about Cybersecurity Maturity Model Certification (CMMC)?

The NIST 800-171 publication outlines "basic" security standards and controls designed to provide guidance for the protection and safeguarding of Controlled Unclassified Information (CUI) by federal contractors and subcontractors who process, store, or transmit information as part of their routine business operations.

NIST 800-171 Defined

NIST 800-171 is a framework designed to provide guidance to anyone that handles Controlled Unclassified Information (CUI)

- When the CUI is resident in nonfederal information systems and organizations
- When the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies.
- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

Certification

Currently, there is no certification process for 800-171. By implementing the recommended 800-171 security controls, organizations essentially are self-attesting they meet and comply with the stipulated requirements.

CMMC auditing is conducted by accredited 3PAO (Third-Party Assessment Organizations).

How does this impact my organization?

The deadline to comply with 800-171 requirements was December 31st, 2017, and it is currently estimated that less than 1% have met those requirements. While the impact for non-compliance may not be apparent or obvious at this moment, it is only a matter of time before 800-171 obligations are strictly enforced. The impact of non-compliance

could potentially result in contract termination, criminal fraud and possibly lawsuits claiming breach of contract.

As a response to the initially low take-up of NIST 800-171, the CMMC has now been introduced to provide a graded, and therefore easier, adoption of security controls.

CMMC breaks the NIST 800-171 controls into five sub-groups and these provide a prioritized series of incrementally greater numbers of controls required at each Level of cybersecurity 'maturity'. For example, CMMC Level 1 only mandates 17 controls out of the total of 171, prioritizing the essential security controls of Access Control and firewalling, Physical and Logical Protection/segmentation of data and systems, and Vulnerability Management, Patching and Malware defenses. Each subsequent Level of CMMC progressively builds on the previous Level's controls.

Where to start and why?

The security requirements outlined in 800-171 should be complementary to an organization's existing IT strategy. 800-171 is very descriptive and requires the understanding of 171 controls across 14 categories which helps define what needs to be accomplished. However, it lacks any prescriptive detail of how to accomplish compliance success and what should be the priority of those requirements.

Learn about each requirement and how Netwrix can help you achieve NIST 800-171 compliance

Let Netwrix show you how a single solution addresses one-third of all the security and compliance requirements across the various 14 categories.

NIST 800-171	Product		
	Change Tracker	Greenbone Enterprise	Log Tracker
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute. 3.1.3 Control the flow of CUI in accordance with approved authorizations. 3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. 3.1.6 Use non-privileged accounts or roles when accessing non-security functions. 3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. 3.1.8 Limit unsuccessful logon attempts. 3.1.9 Provide privacy and security notices consistent with applicable CUI rules. 3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. 3.1.11 Terminate (automatically) a user session after a defined condition. 3.1.12 Monitor and control remote access sessions. 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.14 Route remote access via managed access control points. 3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information. 3.1.16 Authorize wireless access prior to allowing such connections. 3.1.17 Protect wireless access using authentication and encryption	✓		✓
3.3.1 Retain system audit logs to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record analysis, and reporting processes for investigation of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Compare and synchronize internal system clocks with an authoritative source to generate time stamps for audit records.	✓		✓

NIST 800-171	Product		
	Change Tracker	Greenbone Enterprise	Log Tracker
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users.	✓		✓
3.4.1 Maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 3.4.4 Analyze the security of changes prior to implementation. 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. 3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. 3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	✓	✓	✓
3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. 3.5.7 Enforce minimum password complexity and change of characters when passwords are created to allow access to systems. 3.5.8 Prohibit password reuse for a specified number of generations. 3.5.10 Store and transmit only cryptographically protected passwords.	✓		✓
3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	✓		✓

NIST 800-171	Product		
	Change Tracker	Greenbone Enterprise	Log Tracker
3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	✓	✓	✓
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.		✓	
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in systems and applications periodically and when new vulnerabilities are identified.	✓	✓	
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	✓	✓	✓
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, s/w development techniques, & systems engineering principles that promote effective information security. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	✓	✓	✓

NIST 800-171	Product		
	Change Tracker	Greenbone Enterprise	Log Tracker
3.13.6 Deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non□remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission. 3.13.9 Terminate network connections at the end of the sessions or after a defined period of inactivity. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	✓	✓	✓
3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of systems and real-time scans of files from external sources as files are downloaded, opened, or executed. 3.14.6 Monitor systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. 3.14.7 Identify unauthorized use of organizational systems.	✓	✓	✓

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social