NNT & NIST 800-171 Compliance Briefing

NIST 800-171 CONTROL FAMILIES

NIST 800-171 is a subset of re-quire-ments taken from the NIST 800-53 publication that apply specifically to Controlled Unclas-sified Information (CUI) shared by the federal government with a non-federal entity. The controls are divided into 14 different secu-rity control families

> Access Control
> Awareness and Training
> Audit & Accountability
> Configuration Management
> Identification & Authentication
> Incident Response
> Maintenance
> Media Protection
> Personnel Security
> Physical Protection
> Risk Assessment
> Security Assessment
> System & Communications Protection
> System & Information Integrity

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

NNT solutions enable you to quickly establish the foundational & critical controls required by NIST 800-171:

> NNT delivers Security through System Integrity to ensure all system remain provably healthy, secure & compliant at all times.
> Any deviations from a secure state are quickly alerted & intel-ligently analyzed for effective breach prevention & detection.
> Prove your adherence to 171 ei-ther through generally available reports or audit specific reports

Talk to us to find out more!

WHAT IS NIST 800-171?

The purpose of the 800-171 publication is to provide ***non-federal*** organizations with recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI):

> When the CUI resides in nonfederal information systems and organizations.
> When the information systems where the CUI resides is not operated by organizations on behalf of the federal government.
> Where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

WHO MUST COMPLY WITH NIST 800-171?

The requirements apply only to components of **NON-FEDERAL** information systems that ***process, store, or transmit*** CUI, or that provide security protection for such components. The CUI requirements are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and non-federal organizations.

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

WHAT ARE THE DEADLINES FOR COMPLIANCE?

The deadline to meet NIST 800-171 compliance was December 31, 2017, and it is estimated that only 1% met that deadline.

HOW DO THESE REQUIREMENTS IMPACT ME AND MY ORGANIZATION?

The impact for compliance may not be apparent or obvious at this moment, but it is only a matter of time before 800-171 is strictly enforced. The impact of non-compliance could potentially result in contract termination, criminal fraud, and possibly lawsuits claiming breach of contract.

WHAT IS CUI & HOW TO KNOW IF YOUR BUSINESS HANDLES IT?

Controlled Unclassified Information (CUI) consists of anything which should not be made public, but which also is not sensitive enough to require high-level security clearance. Examples include:

> **Personal Information** – Things like legal documents, health information, Social Security numbers, credit card information and various other per-sonal information that is not gener-ally available to the public.
> **IT Security** - Anything, which might compromise the integrity of infor-mation systems or the way in which data, is processed, stored and trans-mitted.
> **Financial Information** – Anything from corporate financials, taxes, purchase orders, bank transactions to payroll. If it contains financial data, it must comply.
> **Intellectual Property** – This covers things like research, engineering and architectural data, drawings/schemat-ics/build specifications, project plans, technical reports, patents, etc....
> **Corporate Information** – Partner-ship agreements, procurement and acquisition agreements, proprietary business information and safety information.

The rule of thumb is that if a system or network device processes, stores or transmits CUI it must comply with 800-171. This includes routers and switches, not just servers and desktops.

Helpful Background Information

Learn about other important federal security mandates such as NIST 800-53, DFARS, and how NIST 800-171 and FIPS are related in this helpful resource section below.

What is NIST 800-53?

> NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) is a publication that's intended as a comprehensive guide to securing **FEDERAL** information systems.

What is Defense Federal Acquisition Regulation Supplement (DFARS)?

> DFARS is a supplement to the Federal Acquisition Regulations (FAR) that provides Department of Defense specific acquisition regulations that DoD government acquisition officials, and those contractors doing business with DoD, must follow in the procurement process for goods and services.

> NIST SP 800-171 was designed specifically for **NON-FEDERAL** information systems — those in use to support private enterprises. Revisions to the DFARS clause in August 2015 made this publication mandatory for defense contractors who have the DFARS 252.204-7012 clause in any contract.

How are NIST 800-171 and FIPS related?

The CUI requirements recommended in 800-171 are derived from Federal Information Processing Standards (FIPS) Publication 200 and the moderate security control baseline in NIST 800-53 and based on the proposed CUI regulation (32 CFR Part 2002, Controlled Unclassified Information). FIPS are publicly announced standards developed by the US federal government to use in computer systems by nonmilitary government agencies and government contractors.

FIPS 200 is the second standard that was specified by the Information Technology Management Reform Act of 1996 (FISMA). It is an integral part of the risk management framework that NIST has developed to assist federal agencies in providing levels of information security based on levels of risk. FIPS 200 specifies minimum-security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements.

Helpful Links

> NIST 800-171 *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf*

> DFARS *https://www.nist.gov/mep/dfars-cybersecurity-requirements*

> FIPS *https://www.nist.gov/information-technology-laboratory/fips-general-information*

WHAT ARE THE CONTROL REQUIREMENTS, WHERE DO YOU START AND WHICH NNT PRODUCTS HELP ACHIEVE COMPLIANCE?

While 171 is very descriptive in what needs to be accomplished to meet security compliance around CUI, it does not advise or prioritize on where to start. The Center for Internet Security is a collaborative organization that understands companies use multiple frameworks including 800-171 to help guide their cybersecurity strategy. The CIS Controls were developed to work as a companion to additional frameworks like 800-171 to help prioritize efforts and action to become compliant.

These Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that make them implementable, usable, scalable, and compliant with all industry or government security requirements.

CIS Controls™

Figure 1: The CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.

NNT & NIST 800-171 Compliance Briefing

WHAT ARE THE CONTROL REQUIREMENTS, WHERE DO YOU START AND WHICH NNT PRODUCTS HELP ACHIEVE COMPLIANCE? CONTINUED...

Controls CSC 1 through CSC 6 are essential to a successful security foundation and should be considered among the very first things to be done. These are often referred to as **"Foundational Cyber Hygiene"** – the basic things that you must do to create a strong foundation for your defense.

NIST 171 Security Requirements	NNT	Solution	Equivalent CIS Critical Control
Access Control	■	Change Tracker Gen7 R2	CIS Control 1 & 2: Inventory of Authorized & Unauthorized Devices and Software
Awareness and Training			
Audit and Accountability	■	Change Tracker Gen7 R2 & Log Tracker Enterprise	CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
Configuration Management	■	Change Tracker Gen7 R2 & Vulnerability Tracker	CIS Control 1 & 2: Inventory of Authorized & Unauthorized Devices and Software and CIS Control 3: Secure Configurations for Hardware and Software
Identification and Authentication			
Incident Response	■	Change Tracker Gen7 R2 & FAST Cloud	CIS Control 5: Controlled Use of Administrative Privileges
Maintenance	■	Change Tracker Gen7 R2 & Vulnerability Tracker	CIS Control 4: Continuous Vulnerability Assessment and Remediation
Media Protection	■	Change Tracker Gen7 R2 & Vulnerability Tracker	CIS Control 4: Continuous Vulnerability Assessment and Remediation
Personnel Security			
Physical Protection			
Risk Assessment	■	Change Tracker Gen7 R2 & Vulnerability Tracker	CIS Control 3 & 4: Continuous Vulnerability Management and Continuous Vulnerability Assessment and Remediation
Security Assessment and Authorization			
System and Communications Protection	■	Change Tracker Gen7 R2	CIS Control 13: Data Protection