



**FORNETIX**

# How a Simple Key Management Solution Can Help Ensure Your Company Is Ready to Do Business with the Department of Defense

**A Cost-Effective Solution for Meeting  
NIST 800-171 Requirements**



## The Challenge

The Department of Defense (DOD) put out a deadline mandating that specific controls be put in place for Covered Defense Information (CDI) and Controlled Unclassified Information (CUI) residing in nonfederal information systems. Many DOD contractors and subcontractors have missed this deadline.

This means thousands of companies intending to do business with the U.S. Government have no choice but to update their cybersecurity standards to even be considered for the job. Unfortunately, many companies are finding, as with most new regulations, the Government’s list of requirements is long, convoluted, and often confusing.

**National Institute Science and Technology (NIST) 800-171: “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”** outlines the new requirements. This document is daunting. And those working for a foreign entity or a contractor seeking first time opportunities with the DOD are feeling a bit overwhelmed by the implications.

## Making Sense of the Requirements

Below we break down how an encryption key management solution can work efficiently and effectively within the NIST 800-171 framework to bring about the specific changes your company needs to be compliant and ensure data security.

### System and Communications Protection – NIST 3.13.10: Establish and Manage Cryptographic Keys for Cryptography employed in Information Systems

CUI Security Requirements	NIST SP 800-53 Relevant Security Controls	ISO/IEC 27001 Relevant Security Controls
3.13.10 – Establish and manage cryptographic keys for cryptography employed in the information system.	SC-12 – Cryptographic Key Establishment and Management	A.10.1.2 – Key Management

### What does NIST SP 800-53, Relevant Security Controls SC-12, “Cryptographic Key Establishment and Management” mean?

Per [NIST Special Publication 800-53 \(Rev. 4\)](#), “the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access and destruction.]”



*“Companies intending to do business with the U.S. government have no choice but to update their cybersecurity standards to even be considered for the job.”*



## Supplemental Guidance

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with external visibility to organization information systems and certificates related to the internal operations of systems.

## Necessary Relevant Security Controls

<b>SC-12(1)</b>	<b>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT   AVAILABILITY</b> The organization maintains availability of information in the event of the loss of cryptographic keys by users. Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).
<b>SC-12(2)</b>	<b>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT   SYMMETRIC KEYS</b> The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.
<b>SC-12(3)</b>	<b>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT   ASYMMETRIC KEYS</b> The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].

As crippling data breaches continue to be an almost daily threat, encryption key management control enhancements have become imperative to keeping data secure. The DOD's demands listed above need to be integrated with your system so that information requiring encryption can be properly protected in creation, while in use, in transit, and at rest.

**The only sure way to meet these stringent requirements is with a strong key management solution.**

## The Solution

### How VaultCore™ Helps You Meet or Exceed NIST 800-171 Requirement for Controlled Unclassified Information (CUI)

*SC-12(1) The organization maintains availability of information in the event of the loss of cryptographic keys by users*

Fornetix® VaultCore is an advanced encryption key management system capable of automating the key lifecycle across the entire enterprise with groundbreaking precision and speed. Fornetix's commitment to meeting or exceeding NIST requirements means VaultCore effectively logs, records, and stores each action and enables you to export detailed, comprehensive logs in Common Event Format (CEF) into your log manager or Security Information and Event Manager (SIEM). **This ensures you've maintained your information in the event of the loss of keys.**

*SC-12(2): The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes*

VaultCore's state of the art cybersecurity technology simplifies encryption key management and amplifies encryption's full potential by automating the creation, deployment, and enforcement of key management across an entire organization —



across all devices – including connected devices, and the supply chain. This sophisticated solution streamlines the process, reduces human error, and typically returns a positive ROI in the second year. **The VaultCore appliance is FIPS 140-2 Level 2 certified, and an unprecedented 5-minute integration with top Hardware Security Module (HSM) providers instantly increases protection to FIPS 140-2 Root Level 3.**



*SC-12(3): The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key.]*

Certificate management plays a crucial role in security. A typical, large organization spends millions per certificate outage. With VaultCore, the request or renewal, approval, generation and deployment, and usage and monitoring of certificates can all be automated with a set it-and-forget it approach. A one-time setup process is all you need to automate what is currently an extensive, manual process, often complicated by human errors.

**VaultCore can create keys and interact with Certificate Authorities and effectively support management of not only certificate categories 1-4, but also Class 5 certificates.**

Delivered as a physical hardware or virtual appliance, VaultCore can also verify the cryptographic integrity of data to ensure critical code has not been tampered with between the facility and third-party vendors. This is a significant benefit in thwarting attacks which can come from smaller, less secure partners. And with industry-leading capacity, VaultCore can manage over 100 million keys, more than enough to serve the growing needs of any industry.

**NIST 3.13.11: Employ FIPS-validated cryptography when used to protect the confidentiality of CUI**

**Necessary Relevant Security Controls**

CUI Security Requirements	NIST SP 800-53 Relevant Security Controls	ISO/IEC 27001 Relevant Security Controls
3.13.11 – Employ FIPS validated cryptography when used to protect the confidentiality of CUI.	SC-13 – Cryptographic Protection	A.10.1.1 – Policy on the use of cryptographic controls A.14.1.2 – Securing application services on public networks A.14.1.3 – Protecting application services transactions A.18.1.5 – Regulation of cryptographic controls

**What does NIST SP 800-53, Relevant Security Controls SC-13, “Cryptographic Protection” mean?**

Per NIST, Special Publication 800-171 (Rev. 1), “*cryptography can be employed to support many security solutions including, for example, the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the required formal access approvals.*”

*Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on other security requirements, organizations define each type of cryptographic use and the type of cryptography required (e.g., FIPS-validated cryptography).”*

The following recommendations are made for mechanisms designed to protect stored data and data in transit.

**A.10.1.1 Policy on the use of cryptographic controls:**

VaultCore reduces threats to your data by executing and scheduling operations in seconds. Traditionally complex and sophisticated commands required for distribution and enforcement of policy across an organization are now made simple. VaultCore provides full control from an easy-to-navigate web interface.

**A.14.1.2 Securing application services on public networks:**

Interoperability is crucial in providing effective key management and swiftly securing data. VaultCore allows you to communicate far and wide on a variety of networks – meeting or exceeding industry standards – by supporting both KMIP and PKCS#11.

**A.14.1.3 Protecting application services transactions:**

VaultCore’s unique ability to provide the wrapping of keys and certificates at the enterprise level ensures service transactions are secure. This includes:

- **Class 1** categorization for individuals intended for email
- **Class 2** for organizations, for which proof of identity is required
- **Class 3** for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority
- **Class 4** for online business transactions between companies
- **Class 5** for private organizations or governmental security
- VaultCore can support management of all 5 transaction categories

**A.18.1.5 Regulation of cryptographic controls:** Regulatory requirements are specific to your geographical region and vary greatly from one locale to the next. Understanding all legal, regulatory, and business requirements that your organization are subject to should first be formally understood, documented, and tracked.

VaultCore optimizes control, visibility, and reporting through a centralized control panel accessed via a simple web interface. Administrators have clear visibility of all encrypted devices and are provided signed, validated audit log information on key management and key consumption. Transparent reporting includes who accessed the key, the event time, and the success or failure of the operation. The challenges of collecting access reports, finding client credentials, and organizing data from multiple locations for compliance purposes or internal reporting become a thing of the past.


## SUMMARY


Once you understand the regulatory requirements necessary to meet NIST 800-171 requirements, it’s easy to understand how Fornetix’s VaultCore can simplify the process of meeting the requirements while simultaneously improving your security posture. VaultCore is competitively priced and, on average, savings are recognized in two (2) years. With VaultCore, you’re capable of setting a re-key schedule that matches your desired policy – an efficient approach – that ultimately saves companies tens of thousands of dollars (or more) by turning a manual, time-consuming process into a simple click of a button, removing known risks associated with human error, rotating keys, and deploying policy.



## Find Out More About VaultCore

**FREE TRIAL:** [www.fornetix.com/freetrial](http://www.fornetix.com/freetrial)  
**FREE DEMO:** [www.fornetix.com/demo](http://www.fornetix.com/demo)

 **1-844-539-6724**

 **5728 Industry Lane,  
Frederick, MD 21704**