COMPLIANCE NOTE

Centrify Mapping to the NIST 800-171 Requirements

The National Institute of Standards and Technology (NIST), which is responsible for developing information security standards and guidelines, recently published Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, NIST Special Publication 800-171. Organizations are supposed to impose the NIST recommended requirements for protecting the confidentiality of CUI in the following areas:

1. When the CUI is resident in nonfederal information systems and organizations;
2. 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; and
3. 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.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contracts or other agreements established between those agencies and nonfederal organizations. – NIST Authors

Key provisions of NIST 800-171 address the security risks around identity and access management within distributed, cross-platform environments. Frequently, organizations that handle CUI have fragmented IT organizations along platform lines, with some part of the staff focused on managing the Microsoft Windows-based infrastructure, and additional groups focused on managing UNIX/Linux systems, Mac OS X workstations, web-based applications, mobile devices, databases, and the like.

There is probably enough justification on why the standards were created (or why we have seen FISMA, 800-53, PCI DSS, NERC / FERC, HIPAA, SOX, etc…). In today's world, cyber attackers will always find the path of least resistance into your protected networks and resources and the requirements are trying to get at the core issue: **With the majority of cyber-attacks, the research has shown the weakest point is your users and their credentials**. This also has been validated by the latest 2016 Verizon DBIR just released and other independent analysis of how a large percentage of breaches occur: **"63% of confirmed data breaches involved weak, default or stolen passwords"**.

And while unfettered privileged access is the holy grail of cyber-attacks, often the easiest way for attackers to gain access is through compromised end user and privileged user accounts. At the same time, traditional perimeter based security is insufficient to protect cloud and hybrid infrastructure, new styles of working, and new ways of connecting remotely. Security vendors offer solutions for parts of the growing identity problem but only Centrify offers a complete security platform that gives you full identity security across data center, cloud, and mobile endpoints.

Below you will see a high level mapping to the main sections / families of requirements to how Centrify addresses. Our intent here is to point out that we address many of the items listed (beyond the obvious non-fitting areas of physical security controls or training, for instance and offer a complete solution for Federal System Integrators to consider beyond the initial MFA requirements. Please see the following chart that outlines how Centrify assists organizations become NIST 800-171 compliant by mapping how Centrify helps organizations address the specific requirements within each family:

NIST 800-171 Requirement	Centrify Solution
3.1 Access Control	The Centrify Identity Platform is the only signal architecture solution to address access to any server, device, application, across the entire environment regardless of where it is located. The combination of Centrify Server Suite®, Centrify Identity Service™ and Centrify Privilege Service™ will enforce the policies and access rights of all individuals associated with CUI.
3.2 Awareness and Training	Centrify's granular access control capability of policy provide reinforcement of training and awareness training by preventing risky behavior. Centrify's audit capability provides detailed review of user session activity so that attempts of risky behavior can be identified.
3.3 Audit and Accountability	Centrify's detailed video style auditing capability provides for complete accountability of both the policy and role creator as well as the user. Three specific use cases are: 1.) Recognize insider threat, 2.) Identify teachable technical and security awareness events, 3.) Determine if the roles have the minimum privilege to ensure least access.
3.4 Configuration Management	The Centrify Server Suite agent can be configured as part of a base image for specific types of servers. Therefore, the first time the system boots it will automatically join Active Directory where Centrify can completely manage the user access and privilege management for all of the users accessing the system. Once joined Active Directory, Centrify can manage the complete access and privileges for all users accessing that system and enforce multiple types of multi-factor authentication and can both allow, and restrict, access to specific applications, programs, and utilities, based on Active Directory group membership.
3.5 Identification and Authentication	Centrify's Multi-Factor Authentication (MFA) Everywhere provides organizations the ability to ensure people are truly who they are and what access rights they have access by being able to leverage a "something I have and something I know" combined with a third method of acknowledging the right user is requesting access to their profile.
3.6 Incident Response	Centrify's Audit Solution assists organizations in assessing a response to an incident. While logging tolls provide information that an incident occurred Centrify's details video recordings of events that provide content and context to the event which allows responding to an incident and moving towards remediation much clearer.
3.7 Maintenance	The Centrify Server Suite provides for granular privilege management for users accessing any system. Because Active Directory becomes the foundation of all user access, users can be time boxed to only access systems during maintenance Windows, and Centrify can limit the access privileges on those users. Additionally, users accessing systems from outside the corporate network can be required to use multi-factor authentication.

3.8 Media Protection **3.9 Personnel Security** **3.10 Physical Protection** **3.11 Risk Assessment** **3.12 Security Assessment**	Centrify's Identity Platform does not address these requirements
3.13 System and Communications Protection	Centrify can be used to secure the communications between key systems within an enterprise, and using this technique enables IT architects to more quickly, and simply secure communication channels among key systems in the enterprise. Additionally, Centrify enables leased access, least privilege for users and limiting the functionality those users may have on any given system. This technique, using Centrify, can prevent unauthorized and unintended information transfers.
3.14 System and Information Integrity	Centrify direct audit can be used to identify unauthorized use of information systems, and can be used in conjunction with an enterprise SIEM tool for alerting.

About Centrify

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring. Centrify is trusted by over 5000 customers, including more than half of the Fortune 50.
Learn more at www.centrify.com.

Santa Clara, California	+1 (669) 444-5200	**Centrify Federal Team:**	+1 (703) 629-2136
		Email:	Federal_Sales@centrify.com
Asia Pacific:	+61 1300 795 789	**Corporate Email:**	sales@centrify.com
Brazil:	+55 11 3958 4876	**Web:**	www.centrify.com
Latin America:	+1 305 900 5354		