COMPLIANCE NOTE

Centrify Mapping to the NIST SP 800-171 Rev. 1 Requirements

Introduction

In December 2016, the National Institute of Standards and Technology (NIST), which is responsible for developing information security standards and guidelines, published NIST Special Publication 800-171 Revision 1 — 'Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations'. Organizations are supposed to impose the NIST recommended requirements for protecting the confidentiality of CUI in the following areas:

- When the CUI is resident in nonfederal information systems and organizations;
- When the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and
- 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 security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations." – NIST SP 800-171 Rev. 1

Key provisions of NIST 800-171 Rev. 1 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, research studies have shown that users and their credentials are the primary attack point. This has been validated by the Verizon's Annual Data Breach Report, whereby **81% of hacker-related data breaches involve either 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 requirements and on how Centrify addresses these. 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), and therefore offer a complete solution for Federal System Integrators to consider beyond the initial MFA requirements.

NIST 800-171 Rev. 1 Requirements	Centrify Solution
3.1 Access Control	The Centrify Zero Trust Security 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 Infrastructure Services and Centrify Application Services 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 and monitoring capabilities provide 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 Infrastructure Services 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 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 (MFA) 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 propagates and supports the concept of MFA Everywhere, which provides organizations the ability to ensure people are truly who they are and that they access just what they're supposed to access. MFA adds a layer of security that allows companies to protect against the leading cause of data breach — compromised credentials. Users provide extra information or factors when they access corporate applications, networks and servers. MFA uses a combination of factors — something a user knows (e.g., username, password, PIN, security question), something a user has (e.g., smartphone, smart card, hardware token), and something they are (e.g., biometrics, like a fingerprint).
3.6 Incident Response	Centrify's audit and monitoring capabilities assist organizations in assessing a response to an incident. While in general log files provide information that an incident occurred, Centrify's detailed video recordings of events provide the necessary content and context which allows for a swifter and more certain response.

3.7 Maintenance	The Centrify Infrastructure Services provide for granular privilege management for users accessing any system. Because Active Directory becomes the foundation of all user access, users can be time-bound to only access systems during a pre-defined maintenance window; and Centrify can limit the access privileges on those users. Additionally, users accessing systems from outside the corporate network can be required to use MFA.
3.8 Media Protection **3.9 Personnel Security** **3.10 Physical Protection** **3.11 Risk Assessment** **3.12 Security Assessment**	These requirements are not applicable to the Centrify solutions.
3.13 System and Communications Protection	Centrify can be used to secure the communications between key systems within an organization. Using this technique enables IT architects to more quickly and simply secure communication channels among key systems in the organization. Additionally, Centrify enables least access and least privilege for users by 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 capabilities can be used to identify unauthorized use of information systems and can be used in conjunction with a SIEM tool for alerting.

About Centrify

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a-Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organizations, including over half the Fortune 100, trust Centrify to proactively secure their businesses.

Think Zero Trust Security. Think Centrify.

Contact Centrify

SANTA CLARA, CALIFORNIA:	+1 (669) 444-5200	EMAILS:	sales@centrify.com
EMEA:	+44 (0) 1344 317950		federal_sales@centrify.com
ASIA PACIFIC:	+61 1300 795 789	WEB:	https://www.centrify.com
BRAZIL:	+55 11 3958 4876		
LATIN AMERICA:	+1 305 900 5354		
FEDERAL SALES	+1 703 629 2136		