CENTRIFY WHITE PAPER, DECEMBER 2011

Addressing FISMA Compliance through Centralized Identity & Access Management Leveraging Microsoft Active Directory

A guide to achieving Federal Information Security Management Act (FISMA) requirements across Windows, UNIX, Linux and Mac OS X systems

Abstract

The Federal Information Security Management Act (FISMA) lays out a comprehensive set of security requirements that are an on-going focus for federal IT managers. FISMA addresses security issues in a comprehensive manner, covering everything from identity management to physical building security. This white paper focuses specifically on identity and access management (IAM) issues, using the guidance provided by NIST Special Publication 800-53 recommended Security Controls for Federal Information Systems, as a roadmap. In addition, requirements related to continuous monitoring of IT security controls as detailed in NIST Special Publication 800-137 are covered.

While FISMA compliance is a complex process due to the broad scope and diversity of federal information systems, the core IAM requirements come down to commonsense and well established principles that can be addressed through a strategy of centralized management, policy enforcement and continuous monitoring. This whitepaper demonstrates how to address these requirements in a robust and cost-effective manner by leveraging existing Active Directory infrastructure to centrally manage non-Windows systems and applications. It then details Centrify's unique ability to extend Active Directory with suite of integrated solutions for cross-platform identity, access and privilege management and continuous monitoring of systems.

Contents

Understanding FISMA and How It Fits in the Federal Compliance Landscape

The federal government's *information systems* – a term used within the federal government to encompass physical hardware, software and related infrastructure – play an indispensible role in virtually every aspect of its operations; they encompass databases of every kind, personnel records, business transactions, budgets, and a wide array of other information. Some of this information must by law be made easily accessible to other agencies and possibly to the public, while some of it must be kept strictly confidential to only a few individuals. Therefore, it is not surprising that federal agencies and the private-sector organizations and contractors who work for them must be aware of a wide array of legislation and best-practice guidelines governing information systems security and compliance.

This white paper covers one of the most pressing and comprehensive set of security requirements that is currently top-of-mind for federal IT departments. Known by the acronym FISMA, the Federal Information Security Management Act was Title III within the larger E-Government Act of 2002. In short, FISMA defines a comprehensive framework for establishing and monitoring the security of information systems within all federal agencies and the private-sector organizations and contractors who work for them. It cuts across all federal agencies, both defense and public-sector.

FISMA comprehensively covers security issues, which includes diverse topics such as the physical security of facilities and training. This white paper focuses on issues related to identity and access management for operating systems and the applications and databases running on them. It analyzes FISMA's core requirements for IT managers and lays out a roadmap for addressing these requirements in a powerful yet cost effective manner by leveraging existing Active Directory deployments in order to manage non-Windows systems and applications.

Before tackling FISMA in depth, let's quickly review the overall compliance landscape within which FISMA operates.

Overview of Federal Security Requirements and their Implementation

Congressional legislation and presidential executive orders are the starting point for federal security requirements and implementation. By nature, legislation and executive orders focus on goals and milestones, which means they are usually vague in terms of implementation details. Various governmental organizations such as the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), among many others, are tasked with developing specific standards and guidelines for addressing the requirements laid out in the legislation and executive orders.

One practical consideration is that not all information systems require the same level of security and effort. To determine which systems fall within the purview of a particular law, IT managers must conduct risk-based assessments of their environment. What are the key infrastructure components that must be in place in order to conduct business? What processes are required to ensure that information systems remain available? What safeguards are needed to keep systems, and the data they hold, from being compromised? Much of the guidance issued by agencies such as OMB and NIST is written flexibly so that different organizations can apply standards that are appropriate to required security level. In this white paper, we focus on solutions that deliver the highest-possible level of security, and individual IT managers can determine to what extent these are needed in their environment.

Especially in areas such a national security, a new emphasis is being placed on securing systems and data. Federal agencies are also beginning to take a broader approach to security by incorporating auditing and reporting requirements in order to establish accountability and ensure that security measures are working as planned.

Current economic factors have increased the pressure to find cost-effective solutions that can leverage existing infrastructure and do not require additional investment. This has also led to a new focus on standards-based solutions that can be deployed uniformly within agencies and between agencies, and can interoperate with private-sector systems as well. Such solutions must be simple to deploy, easy to manage, and help IS managers streamline operations while at the same time offering a sophisticated degree of control over a complex environment of heterogeneous systems and applications.

Appendix A provides brief descriptions of relevant federal information system security compliance regulations and the guidelines developed to address them. The following sections provide a high-level distillation of the most relevant ones related to FISMA.

Prior Regulations and Guidelines that Influenced FISMA

In the years before FISMA, two pieces of legislation are particularly worth mentioning:

- The need to manage federal information systems more efficiently can be traced back to the **Clinger-Cohen Act of 1996**, which required each agency to name a Chief Information Officer who was charged with developing and implementing "sound and integrated information technology architecture". Most important, CCA elevated overall responsibility for managing IT acquisition to the Director of the Office of Management and Budget (a White House agency), which then issued guidelines that must be followed by the agencies. CCA required agencies to adopt performance-based management principles and encouraged commercial off-the-shelf (COTS) procurement to promote standardization and the elimination of standalone government systems.

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (**USA PATRIOT Act**), Public Law Pub.L. 107-56, expanded the authority of law enforcement agencies to search and collect data in areas such as telephone and e-mail communications, and eased restrictions on foreign intelligence gathering within the United States. Although it was not primarily directed at the security of information systems, it did specify that data stored on federal agency systems be tightly controlled and consistently labeled as "For Official Use Only," "Law Enforcement Sensitive," "Sensitive But Unclassified," or "Classified."

FISMA and Key Associated NIST and OMB Guidelines

The E-Government Act of 2002 recognized the need to define a comprehensive framework for establishing and monitoring security programs for federal agencies. For IT managers, Title III of the E-Government Act was of particular interest. Entitled the Federal Information Security Management Act (**FISMA**), it requires each federal agency to develop, document, and implement an agencywide program to secure the agency's information systems. It applies not just to the agency's own information systems but to those of other agencies, contractors and others with whom it works.

Taken together with prior legislation and OMB and NIST guidelines (described later), FISMA requires executive agencies within the federal government to:

- Plan for and develop a comprehensive security program
- Ensure that appropriate officials are assigned security responsibility

- Provide continuous and real-time monitoring of security controls to be used as the source for periodic review and reporting of information systems based on risk.
- Engage in annual security reporting to the OMB
- Provide internal security awareness training
- Authorize system processing prior to operations and, periodically, thereafter
- Follow guidelines issued by NIST for information security controls

There are several key guidelines that address FISMA:

- **OMB Circular A-130, Management of Federal Information Resources**, requires federal executive branch departments and agencies to implement FISMA.
- **NIST Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems**, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.
- **OMB Memorandum M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,** details actions Federal CIOs, CISOs need to take provide continuous monitoring of security IT controls.

  "Agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way. Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other agency management all need to have different levels of this information presented to them in ways that enable timely decision making."

- **NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems** (ISCM), helps to ensure that deployed security controls continue to be effective and that operations remain within stated organizational risk tolerances in light of the inevitable changes that occur over time. In addition, NIST SP 800-37, *A Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, defines the core risk management requirements that NIST SP 800-137 builds on.

In the section "Centrify Addresses the Core Technical Requirements of FISMA through NIST Special Publication 800-53", later in this document, we examine the NIST guidance in detail because it provides the most concrete roadmap to FISMA compliance for both security controls and ongoing reporting and continuous monitoring.

Additional Regulations and Guidelines that May Affect FISMA Projects

A few other regulations may be mentioned as complementing FISMA. Although not the subject of this white paper, they are nonetheless worth mentioning since they have overlapping requirements and frequently come up in FISMA discussions.

- Homeland Security Presidential Directive 12 (**HSPD-12**), Policy for a Common Identification Standard for Federal Employees and Contractors 2004, requires federal executive departments and agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors. HSPD-12 addresses access both to physical facilities and to information systems and it designates major milestones for implementation. In practical terms, HSPD-12 has driven the adoption of smart cards as the

agreed-upon method for implementing more secure authentication to computing systems based on something stronger than traditional username/password challenge systems.

- NSPD-54/HSPD-23 made the NSA the lead agency in monitoring and protecting all of the federal government's computer networks from cyber-terrorism.
- In addition to NIST Special Publication 800-53, NIST has also issued a number of Special Publications that expand on specific sections of SP 800-53. These NIST Special Publication 800-series documents provide guidelines for certifying the security of systems, classifying national security systems, assessing effectiveness, and other issues.
- Both the Department of Homeland Security and Department of Defense have issued security guidelines. In particular, DoD Directive 8500.1, also known as the DoD Information Assurance Certification and Accreditation Process (DIACAP), defines the DoD's risk management process for assuring the security of information systems throughout their lifecycle. Its 17 key accreditation categories are very similar to the categories set out for FISMA via NIST 800-53, and thus compliance with FISMA will substantially address DoD 8500.1 as well.
- The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC currently exists for Microsoft Windows Vista and XP operating system software.
- The National Industrial Security Program Operating Manual (NISPOM) was issued as a result Executive Order 12829 and under the authority of DoD Directive 5220.22. This manual provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts under the NISP.

In the next section, we examine the environmental and management challenges that IT managers face as they work to address FISMA.

The Fragmentation of Identity and Access Management within the Distributed Environment

Key provisions of FISMA address the security risks around identity and access management within distributed, cross-platform environments – risks, it should be noted, that are pervasive in public-sector organizations and not exclusive to federal agencies. Frequently within federal agencies you'll find that IT organizations have fragmented 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, applications, databases, and the like.

Federal agencies have broadly adopted Windows as the platform of choice for user desktops and basic network file and print services. Microsoft Exchange has been deployed for email, and a smattering of other Windows Server-based solutions such as SQL Server and SharePoint are being used. In the Windows environment, Microsoft provides a comprehensive identity management solution through Active Directory, and the Identity Lifecycle Management applications provide lifecycle management for user identities. IT departments have invested millions of dollars deploying Active Directory, with the result that they have built a highly scalable and fault-tolerant domain controller infrastructure as part of ongoing initiatives to meet security and business continuity objectives. The broad adoption of Windows as a core infrastructure also fits with the government initiatives to trim costs through adopting technology that can be adopted uniformly across agencies. Within this Windows estate, Active Directory is the core, strategic infrastructure.

Federal agencies have also widely deployed UNIX and Linux servers for enterprise-class applications and databases. But no single identity management solution enjoys anything like the pervasiveness of Active Directory

within the Windows environment. Federal IT organizations are dealing with a plethora of identity stores deployed to manage their UNIX/Linux platforms, including:

- Significant usage of locally managed /etc/passwd text files on individual systems.
- Use of Sun's outdated Network Information Service (NIS or NIS+).
- Use of LDAP-based directories such as OpenLDAP or the Sun ONE Directory.

Mac workstations are also a popular choice among many federal agencies, particularly for engineering and design applications. While identity management solutions exist for Mac networks, they represent yet another identity system for the IT staff to manage. Many of the key cross-platform integration features needed by administrators are lacking in the solutions that come from Microsoft and Apple.

Access control features are built into Active Directory and are heavily used to manage access to Windows resources. However, few solutions exist to expand access control to non-Windows environments. IT managers are often faced with implementing proprietary layered solutions that are costly and difficult to manage.

The identity management challenges multiply as we move up from the system layer to applications. As new Java and web applications are rolled out on platforms such as Apache, JBoss, Tomcat, IBM WebSphere and BEA WebLogic, developers are creating even more identity stores through the use of text files or database tables. Database platforms such as IBM's DB2 and Informix, along with enterprise applications such as SAP, add yet another set of individual identity stores.

Thus, the fact is that in many agencies, identity and access management for UNIX, Linux and Mac OS X systems, applications and databases is quite fragmented compared to Windows.

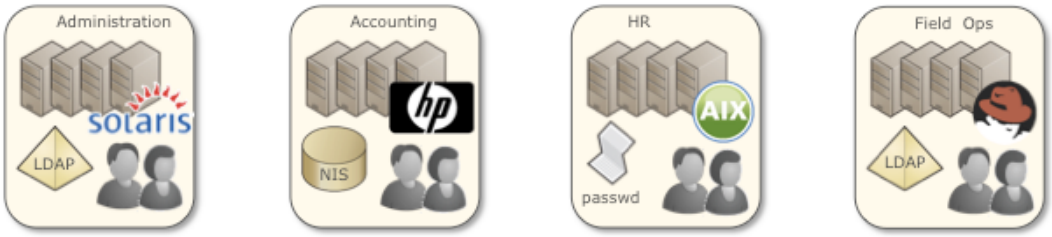

Figure 1-2. The fragmentation of identity management in the distributed environment: one user, multiple accounts, multiple identity stores, and fragmented (or no) policy mechanisms.

As the federal government's dependence on information systems has grown, so too has recognition of the enormous challenges involved in keeping them secure and available. FISMA in particular is driving security initiatives to classify information systems, and the data that they hold, and to design risk-based security plans. Because not all federal systems will require the same level of security and attention, role-based access controls, delegated administration, and fine-grained privilege management features are becoming increasingly important. IT auditing tools are also needed by security managers charged with monitoring systems for unauthorized or suspicious activity, and by independent IT auditors who will be periodically checking to ensure that the security controls in place are working as intended.

Centrify's Vision for Unified Identity and Access Management

Centrify's vision is to help organizations strengthen IT security and streamline operations by centrally securing their cross-platform servers, workstations and applications using Microsoft Active Directory. By enabling IT departments to control users' access to these resources, authorize what they can do, and audit their actions, Centrify eases regulatory compliance requirements and reduces the risk of internal and external security threats.

And, by extending an organization's existing Active Directory infrastructure to embrace non-Windows servers and applications, Centrify simplifies an organization's IT infrastructure and reduces costs.

Figure 4-1. Centrify eliminates the need for multiple identity and access management solutions in the distributed environment by consolidating management in Microsoft Active Directory: one user, one account, one directory, one policy mechanism.

Centrify delivers on this vision through the Centrify Suite, an integrated family of Active Directory-based auditing, access control and identity management solutions. Centrify solutions are next-generation technology, built on a common architecture that embraces open standards, making them quick-to-deploy, easy-to-manage, and cost-effective compared to complex and proprietary legacy products.

The Centrify Suite is comprised of the following solutions:

- **Centrify DirectControl.** Secures over 300 flavors of UNIX, Linux and Mac using the same authentication and Group Policy services deployed for your Windows environment. DirectControl also provides Active Directory-based single sign-on solutions for popular web-based servers (e.g., Apache, WebLogic and WebSphere), databases (e.g., DB2) and enterprise applications (e.g., SAP).
- **Centrify DirectAuthorize.** Centrally manages and enforces role-based entitlements for granular control of user access and privileges on UNIX and Linux systems.
- **Centrify DirectAudit.** Delivers auditing, logging and continuous, real-time monitoring of user activity on your Windows, UNIX and Linux systems.
- **Centrify DirectSecure.** Provides trust-based protection of sensitive information by dynamically isolating and protecting cross-platform systems and enabling end-to-end encryption of data-in-motion.

Centrify Suite is the only Active Directory-centric Identity and Access Management solution to receive NIST FIPS 140-2, Level 1 Validation.

(Certificate #1604, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1604)

For a comprehensive overview of Centrify solutions, request our free white paper, "Centralized Identity and Access Management of Cross-Platform Systems and Applications with Active Directory and the Centrify Suite." The following sections provide a brief overview of each solution's key features and benefits.

Centrify DirectControl Overview

Centrify DirectControl's core feature is its ability to enable UNIX, Linux and Mac OS X systems to participate in an Active Directory domain. The Centrify DirectControl Agent effectively turns the host system into an Active Directory client, enabling you to secure that system using the same robust Kerberos-based authentication, access control and Group Policy services currently deployed for your Windows systems. Additional seamlessly integrated modules snap into the DirectControl Agent to provide services such as web and database single sign-on and Samba

integration. The DirectControl management tools include extensions to standard Microsoft management tools, an administration console, out-of-the-box reporting, and an account migration wizard.

With Centrify DirectControl, organizations with diverse IT environments can leverage their investment in Active Directory to:

- **Centralize administration of user accounts and security policies with a directory.** By centralizing user account management and security policy in Active Directory, organizations can improve IT efficiency and standardize on a secure, connected infrastructure for their cross-platform environment. Using DirectControl they can eliminate redundant identity stores, provide administrators and end-users with a single sign-on account, standardize on a single set of tools and processes, and enforce enterprise-wide security and configuration policies for their cross-platform environment.
- **Use DirectControl Zones to provide secure, granular access control and delegated administration.** Only DirectControl, with its patented Zone technology, delivers the granular access control that real-world enterprises need to securely manage their cross-platform environments. Any logical collection of mixed UNIX, Linux or Mac OS X systems can be segregated within Active Directory as a DirectControl Zone. Each Zone can have a unique set of users, a unique set of administrators, and a unique set of security policies.
- **Extend web single sign-on to internal end-users and external business partners and customers.** Centrify delivers Active Directory-based web single sign-on for both intranet and extranet applications running on Apache and popular J2EE servers at a fraction of the cost of older point solutions. For intranets, DirectControl enables Active Directory-based web SSO via Kerberos and LDAP. For extranets, DirectControl leverages Microsoft Active Directory Federation Services (ADFS) to provide federated identity management for both business-to-business and business-to-customer web applications.
- **Simplify compliance with regulatory requirements.** DirectControl greatly simplifies the administrative, reporting and auditing tasks brought on by FISMA, Sarbanes-Oxley, PCI, HIPPA and other government and industry regulations by providing IT managers with a single point of administration from which to reliably manage user accounts, set access controls and enforce security policies. DirectControl Zones enable "need to know" access controls, and out-of-the-box reports verify who has access to what.
- **Deploy quickly without intrusive changes to existing infrastructure.** DirectControl's support for open standards and its unified architecture make it far easier to deploy than any other Active Directory-based solution. Certified for Windows Server 2003 and Windows Server 2008, DirectControl does not require proprietary schema changes in order to store UNIX identity data or to enable advanced features.

Centrify DirectAuthorize Overview

Centrify DirectAuthorize centrally enforces role-based privileges for fine-grained control of user activities on UNIX- and Linux-based systems. According to Gartner, UNIX and Linux systems inherently lack a scalable and simple model for administrative delegation, and organizations that give too many users root permission run unnecessary security risks and will invariably fail audits. By controlling how users access systems and what they can do, DirectAuthorize enables organizations to lock down sensitive systems and eliminate uncontrolled use of privileged superuser accounts.

Centrify DirectAuthorize is tightly integrated with Centrify DirectControl and is included in all Centrify Suite editions.

A unique and powerful DirectAuthorize feature is the Computer Role, which enables you to create a collection of computers that share a common set of management and security requirements. For example, you might create a Computer Role for web servers and a user role for web developers. The web developer role grants access to the web server Computer Role and defines a limited set of privileges. Membership in the web developer role could then

be controlled using an Active Directory group. Giving a web developer consistent access rights and privileges to web servers throughout your enterprise is then as simple as adding them to the Active Directory group. They do not get privileges to other computers where the web servers are located.

DirectAuthorize's key features and benefits are as follows:

Role-Based Access Control

- Lock down sensitive systems with granular controls that specify who can access a system, how they can access it, and what they can do.
- Use Computer Roles to make the assignment of user access rights more natural and easier to manage.
- Tie users' UNIX and Linux privileges to centrally managed Active Directory accounts.

Role-Based Privilege Management

- Grant users rights to execute commands with elevated privileges, eliminating the need for access to privileged accounts and passwords.
- Validate use of privileged commands by requiring a Change Control ticket be entered before execution is permitted.
- Simplify the execution of privileged commands for users.

Centrify DirectAudit Overview

Centrify DirectAudit helps you comply with regulatory requirements, perform immediate in-depth troubleshooting, and protect against insider threats for your UNIX, Linux and Windows systems. DirectAudit's detailed privileged session monitoring strengthens your compliance reporting and helps you spot suspicious activity by showing which users accessed what systems, what commands they executed, and what changes they made to key files and data. With DirectAudit you can also perform immediate, in-depth troubleshooting by replaying and reporting on user activity that may have contributed to system failures. And its real-time monitoring of current user sessions enables you to spot suspicious activity and take the required remediation steps under FISMA 2.0 to address risks to critical assets.

DirectAudit's key features and benefits are as follows:

- **Enhance compliance with regulatory requirements.** Practically every government and industry and government compliance regulation (including FISMA, SOX, PCI, HIPAA, and GLBA) requires detailed logging and audit trails of user activity, especially on mission-critical and sensitive systems. DirectAudit meets these needs by capturing detailed user session information – who logged into what systems, what commands they executed, what changes they made to key files and data. DirectAudit's flexible querying and reporting features enhance your ability to document compliance and provide robust tools for identifying and investigating potential security breaches.
- **Perform in-depth troubleshooting and configuration reporting.** From DirectAudit's central console you can quickly locate and replay user activity that may have contributed to a system outage. DirectAudit captures detailed session activity – both keystrokes and session output – so you can immediately diagnose problems or report on and document configuration and other changes.
- **Protect against insider threats and monitor real-time user activity.** DirectAudit lets you centrally view who is currently accessing all of your distributed UNIX, Linux and Window systems and immediately drill

down to see what they are doing. This real-time monitoring helps you proactively spot insider threats and gives you global visibility into activity across your organization.

Centrify DirectSecure Overview

Centrify DirectSecure is a policy-based software solution that secures sensitive information by dynamically isolating and protecting cross-platform systems and enabling optional end-to-end encryption of data in motion. By leveraging your existing Active Directory infrastructure and the native IPsec support built into today's operating systems, DirectSecure seamlessly blocks untrusted systems from communicating with trusted systems, and does so without the need to change your network or applications. The net result is improved adherence to regulatory compliance initiatives as well an additional layer of policy-driven protection against network attacks for mixed Windows, UNIX, and Linux environments, and prevention of unauthorized access to trusted computing resources and data.

Organizations with distributed, cross-platform systems are using DirectSecure to:

- Protect against external threats by isolating the enterprise from rogue or unmanaged computers or users
- Isolate servers holding sensitive information from the rest of the enterprise
- Encrypt data in motion
- Establish secure communication channels over public or open networks
- Isolate an individual tenant's network within an ISP's multi-tenant environment

Centrify DirectSecure capabilities also ensure:

- Centralized management of host-based network security policies is provided by Active Directory's Group Policy infrastructure. DirectControl provides enforcement of Group Policies once the system has been joined to the domain, enabling DirectSecure to enforce several additional policies required for this solution.
- Automated host credential management is provided through both Kerberos credentials assigned when joining Active Directory as well as automated PKI certificate issuance and renewal.
- Identity-based network authorization enables centralized management of granular access policies required to isolate logical groups of systems, preventing external communications.
- Port-level network encryption secures network communications for any application without requiring changes to the application operating at the network layer.

DirectControl Zones Provide the Foundation for Secure, Cross-Platform Access Control

To better understand Centrify's unique value proposition in providing cross-platform access control, a further discussion of one of DirectControl's core features — Zones — is required.

From an identity management perspective, it is very hard to ensure that UNIX/Linux/Mac OS X UIDs are unique throughout the enterprise. This is especially true when user accounts are held in a variety of identity stores: NIS, /etc/passwd files or LDAP-based directories. If there is no way to map these multiple UNIX identities to a single Active Directory account, an organization will be forced to undergo a painful UID rationalization project before they can even began to add non-Windows systems into their Active Directory domains.

From a security and compliance perspective, it is neither desirable nor practical to allow all users in an enterprise to log on to all UNIX/Linux/Mac OS X systems, which could be the net result if UNIX identities were simply

imported together into Active Directory and UNIX-enabled. Organizations frequently need a way to create logical groups of non-Windows systems to preserve existing security boundaries.

To deal with all these challenges, Centrify has developed its unique Zone technology.

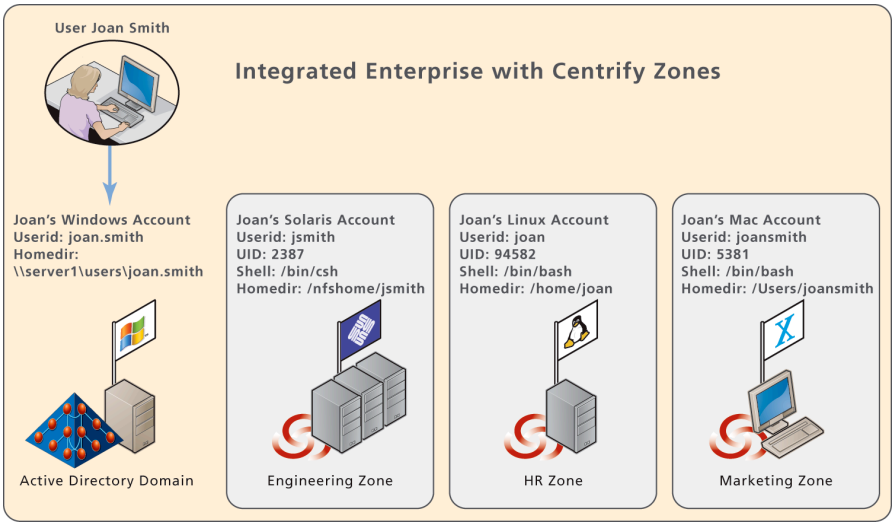

Figure 4-2. An example of Zoning for identity management

Centrify Zones provide:

Centralized UNIX Identities. The fastest and most efficient means of consolidating a set of complex and disparate non-Windows identities into Active Directory

Least-Access Policy. The most flexible solution for creating least-access and least-privilege security models for a diverse set of users, systems and roles

Delegated Administration. The most secure means of delegating user and administrator privileges in a highly granular manner

A Centrify Zone is a collection of attributes and security policies that define the identities, access rights and privileges shared by a group of users. A small organization might need only a single Zone to manage their Mac OS X users and desktops. A large organization may need a hierarchy of Zones to manage users who need access to thousands or tens of thousands of UNIX, Linux and Mac OS X systems that are used as everything from end-user workstations to web application servers.

Centrify Zones addresses the key challenges organizations face when consolidating multiple identity stores into Active Directory.

Centralized UNIX Identities

One critical challenge is the difficultly of ensuring that UNIX user identifiers (UIDs) are uniquely associated with users across an organization. This is especially true if user accounts reside in a variety of identity stores that include NIS, /etc/passwd files, and LDAP-based directories.

If an organization can't map these multiple UNIX identities to a single Active Directory account, it may be forced to rationalize all UIDs — a tedious procedure — before it can even begin adding non-Windows systems to Active Directory domains. With Centrify, IT departments can use Zones as a permanent solution for identity mapping andas a technique for quickly migrating multiple user identities to a single Active Directory account.

Least-access Policy

Zones provide a flexible means of managing a set of users and computers that all need to share a common set of policies and delegated rights.

For example:

- Create a Zone for Mac OS X users and their computers, regardless of where they are located geographically or what department they work for.
- Create a Zone for an engineering department whose users must all share access to a set of UNIX development systems, whether located in a data center or in the cloud.
- Create a Zone for a branch office that has its own set of administrators tasked with managing all the UNIX, Linux and Mac OS X systems at their location.

A user's Active Directory account can be mapped to more than one UNIX identity, and a computer can be assigned to multiple Computer Roles (part of Centrify DirectAuthorize described below), enabling you to create identity management, access control, privilege management and delegation solutions that are as simple or as sophisticated as you need them to be for your particular environment.

This approach enables you to manage your non-Windows environment by tying the rights a user has on a UNIX, Linux or Mac OS X computer with a single, definitive identity centrally stored and managed in Active Directory.

Delegated Administration

In addition to allowing users to be organized into logical groups, Zones make it possible to delegate management to the various levels of administrators who manage those systems — increasing overall organizational security.

Each Zone can have its own set of administrators, each with specific privileges for that Zone. Administrator rights are assigned on a Zone-by-Zone basis. Administrators with rights for one Zone do not automatically have rights to other Zones.

For example, one administrator may have rights to add new systems to Zone A and Zone B, while another administrator may only have rights to change user access in Zone B.

By segregating both users/computers and administrators into secure, logical groups, Zones give an organization the granular level of control it needs to maintain appropriate levels of confidentiality and ensure compliance with regulatory standards for separation of duties.

Delegation of administration by Zone is a powerful — and indispensable — feature for a large organization employing thousands of privileged users and administrators. Segregation of administrators in logical groups removes the potential for abuse that comes with giving administrators blanket access privileges. For example, there is no reason for a web site administrator to have rights to create new user accounts or to modify user access to a payroll server.

Setting up multiple Zones is not required. Some organizations choose to add computers to a single Global Zone. Using Centrify's management tools, IT can quickly and easily set up any number of additional child Zones based on their identity management and access control needs, either at the time users or computers are added to Active Directory or at any time later.

With this understanding of the Centrify Suite and its unique Zone technology, we're now ready to examine how Centrify uniquely addresses the essential IT requirements for FISMA compliance as laid out by NIST Special Publication 800-53 and 800-137.

Centrify Addresses the Core Technical Requirements of FISMA through NIST Special Publication 800-53 and 800-137

NIST Special Publication 800-53 and 800-137 provides guidelines for selecting and specifying security controls for information systems and monitoring the effectiveness of these controls supporting the executive agencies of the federal government. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems.
- Providing a recommendation for minimum security controls for information systems categorized in accordance with **FIPS 199, Standards for Security Categorization of Federal Information and Information Systems**.
- Providing a stable yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies.
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.
- Automating the monitoring of security controls outlined in NIST SP 800-53 for a real-time and dynamic view of the effectiveness of those security controls and the security posture of the organization.

As shown in the following table, **NIST Special Publication 800-53** breaks selected FISMA requirements (paraphrased) into 17 security control families, and each family is categorized in one of three ways: management, operational, or technical. Management categories provide guidance on tasks such as assessing risk and acquiring systems and applications, and thus for the most part Centrify's solutions do not address these specifically. Operational categories cover tasks such as planning for and implementing training or disaster recovery routines and the following table notes instances where Centrify solutions can be of assistance. Technical categories provide detailed guidance for tasks such as implementing access controls or performing auditing. The table notes briefly which Centrify solutions address these technical issues, and the sections following the table provide more information on specific critical issues.

Note: NIST SP 800-53's 17 security control families are closely aligned with the 17 security-related areas in **FIPS 200**, which specifies the minimum security requirements for protecting federal information and information systems. Thus in general compliance with NIST SP 800-53 covers the requirements of FIPS 200.)

NIST SP 800-53 Security Categories and Overview of Centrify's Solutions			
ID	Family	Category and Synopsis of Key Requirements	Centrify Solution
AC	Access Control	**Technical.** Guidance on managing and implementing policy-based access to information systems. Includes requirements for separation of duties, least privilege access to systems, recording successful and unsuccessful login attempts, session lock or termination on inactivity.	Centrify DirectControl centralizes all authentication and access control within Active Directory and through its unique Zone feature enforces granular access control to systems and enables delegated administration. Centrify DirectAuthorize enables least-privilege access through its fine-grained access controls and unique restricted environment feature. See "Centrify Solution for Access Control (AC)" later in this section.
AU	Audit and Accountability & Continuous Monitoring	**Technical.** Guidance on requiring systems to generate auditable events, and to capture sufficient detail to both (1) establish what occurred, who performed an action, and its outcome and (2) monitor, analyze and report on activity, and provide after-the-fact analysis. **Continuous Monitoring.** NIST SP 800-137 provides guidance on Information Systems Continuous Monitoring (ISCM) including implementation, automation and response.	Centrify DirectAudit captures detailed session events, metadata and video linked definitively to Active Directory identities. All session activity, including system output is recorded. Sessions and logs are centrally stored for real-time monitoring and historical reporting and analysis. Role-based control of audit data ensures authorized access to DirectAudit session data. See "Centrify Solution for Audit and Accountability (AU) and Continuous Monitoring "later in this section.
CM	Configuration Management	**Operational.** Guidance on documenting baseline system configuration and developing plans for systematic and automated change control. Includes requirements for preventing unauthorized changes, getting notification of changes, testing and validating changes, monitoring for configuration changes, and inventorying system components.	Centrify DirectControl enforces Group Policy settings to ensure that security policies are consistently enforced across all systems joined to Active Directory. Centrify DirectAuthorize can protect against unauthorized system changes by limiting personnel to a specific set of commands. Centrify DirectAudit can verify these controls are working and monitor for unauthorized or suspicious activity. See "Centrify Addresses Requirements for Configuration Management (CM)" later in this section.
IA	Identification and Authentication	**Technical.** Guidance on uniquely identifying and authenticating users. Includes policies for maintenance of authentication devices such as keycards and protecting authentication processes from exploitation.	Centrify DirectControl centralizes all authentication and access control within Active Directory, ensuring entitlements are definitively linked to a single identity. See "Centrify Addresses Requirements for Identification and Authentication (IA)" later in this section.

NIST SP 800-53 Security Categories and Overview of Centrify's Solutions			
ID	Family	Category and Synopsis of Key Requirements	Centrify Solution
MA	Maintenance	**Operational.** Guidance on policies for system maintenance: procedures, timeliness, record-keeping, assessing the effectiveness of tools, and controlling who performs maintenance.	Centrify DirectAuthorize can be used to control who can access systems, at what times, and what actions they can perform, such as upgrades and updates.
PS	Personnel Security	**Operational.** Guidance on assigning a risk designation to all positions and screening personnel for risk factors. Includes guidance on terminated personnel, including disabling system access.	Note that implementing Active Directory-based identity management using Centrify DirectControl provides assurance that terminated personnel immediately lose privileges not only to Windows resources but to non-Windows systems and applications as well.
RA	Risk Assessment & Continuous Monitoring	**Management.** Guidance on categorizing information systems through a risk-based assessment of the harm done by unauthorized access. Includes related issues such as vulnerability scanning. **Continuous Monitoring.** NIST SP 800-137 provides guidance on Information Systems Continuous Monitoring (ISCM) including implementation, automation and response.	Centrify DirectAudit can provide assurance that access controls are working as designed on Windows, UNIX and Linux systems, and that it provides continuous monitoring and reporting facilities. Centrify DirectAudit captures detailed session events, metadata and video linked definitively to Active Directory identities. All session activity, including system output is recorded. Sessions and logs are centrally stored for real-time monitoring and historical reporting and analysis. Role-based control of audit data ensures authorized access to DirectAudit session data. See "Centrify Solution for Audit and Accountability (AU) and Continuous Monitoring "later in this section.
SA	System and Services Acquisition	**Management.** Guidance on capital budgets and investment control through lifecycle planning. Includes rules on keeping systems/software in compliance with licenses and agreements and configuration change management. Also addresses special security needs for development systems.	Note that Centrify DirectControl's Zone technology can help assure the segmentation of development systems as defined in this section.
SC	System and Communications Protection	**Technical.** Guidance on separating application functionality from system management functionality and isolating security functions from non-security functions. Includes preventing unintentional data sharing across networks, denial of service protection, transmission integrity, and flaw remediation	Centrify DirectSecure provides server isolation technology to protect systems at the network interface. Policy based IPsec security prevents unauthorized access as well as protecting data in transit between trusted systems.

NIST SP 800-53 Security Categories and Overview of Centrify's Solutions			
ID	Family	Category and Synopsis of Key Requirements	Centrify Solution
SI	System and Information Integrity	**Operational.** Guidance on identifying system flaws, keeping hardware up to date, protecting against malicious code protection, following security alerts/advisories, and verifying correct operation of security functions. Includes guidance on detecting and protecting against unauthorized software changes and restricting the ability to input information to authorized personnel.	Centrify DirectAuthorize can protect against unauthorized system changes by limiting personnel to a specific set of commands. Centrify DirectAudit can verify these controls are working and monitor for unauthorized or suspicious activity.

NIST SP 800-53 contains hundreds of pages of detailed guidance and requirements. In addition, information systems must be classified in three categories: low-impact, moderate-impact and high-impact. These categories are used to structure risk-based assessments of the degree of security and resources required for groups of systems. In many cases, NIST SP 800-53 provides alternative wording for a single requirement to accommodate these different levels of security.

As a result, it is not practical to definitively address all requirements in all their complexity. The following sections provide more details on how Centrify addresses key identity and access management requirements outlined in NIST SP 800-53. Each section contains a summary of the most relevant requirements from key technical categories in the previous chart, followed by an explanation of how Centrify addresses them. Available on request, Centrify can also provide point-by-point analysis in an RFP-type format.

Centrify Solution for Access Control (AC)

Following are *paraphrased* excerpts of the most relevant requirements, along with an explanation of how Centrify addresses them. The various requirements have been grouped into related areas.

Active Directory-Centrify Account Management

Selected FISMA requirements:

- **AC-2 Account Management.** Employ automated mechanisms to manage account data, automatically terminate temporary or time-limited accounts, audit account creation and modification.
- **AC-7 Unsuccessful Login Attempts.** Enforce a limit of consecutive invalid access attempts by a user during a time period.

Centrify capabilities:

Centrify DirectControl enables IT organizations to consolidate user identities for their UNIX, Linux and Mac OS X systems in Active Directory, thus centralizing the enforcement of account and password policies. This has a wide range of administrative benefits, including:

- A single Active Directory account now holds entitlements across systems and applications. In addition to their Windows-related privileges, a user's Active Directory account can now be used to set up and control access to UNIX/Linux and Mac OS X systems, and to non-Microsoft applications. Disabling the Active Directory account immediately terminates access to those systems and applications, closing security risks associated with the orphan accounts that result when provisioning processes cause delays – or gaps – in removing system or application access.

- Native Active Directory features can be used to automatically disable an account at a specific date and time. At a more granular level, Centrify DirectAuthorize can be used to disable access to UNIX/Linux systems or to limit what privileges users have on UNIX/Linux systems during specific time windows. For example, backup operators can be given rights to access systems only during an 8-10 p.m. time window on Tuesdays and Thursdays. DirectAuthorize could also be set to give access to a user account only during a particular time window, such as December 20 to December 31 – for example, to let a temporary employee cover duties during a holiday.
- All interactive login attempts are captured by native Active Directory logging in the same way that Windows login attempts are captured. Consecutive invalid login attempts will result in the Active Directory account being locked out across all systems that leverage Active Directory for user authentication.
- DirectControl extends Active Directory's rules for password length, complexity and currency to UNIX, Linux and Mac OS X systems as well. When a user is required by policy to change a password, they receive a system prompt no matter what type of system they are logging into.

Privilege Management and Separation of Duties

Selected FISMA requirements:

- **AC-3 Access Enforcement.** Restrict access to privileged functions to specifically authorized personnel (for example, security administrators).
- **AC-5 Separation of Duties.** Enforce separation of duties through assigned access authorizations.
- **AC-6 Least Privilege.** Enforce the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.

Centrify capabilities:

Centrify's patented Zone technology is unique in its ability to provide fine-grained control over user access to systems. Here are some specific capabilities of Zones, DirectControl and DirectAuthorize that directly address these FISMA requirements:

- Organizations can segregate systems into logical groups, and only users who are authorized for a Zone can log in to systems within that Zone. Each Zone can have its own set of users, administrators and policies. For example, you could set up a Zone of systems designated as low-impact with one set of users and administrators, and with a set of policies that provide baseline security. You could set up another Zone of systems designated as high-impact with a very limited set of users and a variety of closely tailored policies.
- DirectControl enforces separation of duties by leveraging Active Directory's rich delegation model to provide delegated administration of UNIX, Linux and Mac OS X systems. Each Zone can have its own set of administrators, and each administrator could have his/her own set of rights. For example, one administrator may be authorized simply to add or remove other users from Zone membership, while another administrator may also be authorized to change Zone properties. As separation of duties dictates, these Zone administrators do not need elevated privileges – for example, they do not need to be able to create or delete accounts just to update Zone membership or Zone properties. A single user could also be an administrator of multiple Zones, with different privileges on each Zone.
- DirectAuthorize adds finer-grained access controls by defining user roles within a Zone. The role specifies which PAM-enabled interfaces or applications a user in that role can use to access systems in the Zone (for example, a backup operator may have access only through SSH).
- DirectAuthorize can also set time windows when a role can access a system, and set time periods when a role assignment is active. Backup operators may need access to sensitive systems only for a limited time

during a maintenance window. Or a contract system administrator may be on staff only for a specific time period.

- DirectAuthorize enforces least privilege management in two ways. It can grant users rights to execute commands with elevated privileges, eliminating the need for access to privileged accounts and passwords. For even tighter control, users can be assigned to a Restricted Environment with access only to a specific "whitelist" of commands. As a side benefit, DirectAuthorize simplifies the execution of privileged commands since users in a Restricted Environment no longer need to switch to root or other privileged accounts in order to run commands that require privilege.

Session Management

Selected FISMA requirements:

- **AC-8. System Use Notification.** Display an approved system use notification message before granting system access informing potential users.
- **AC-11 Session Lock.** Prevent further access to the system by initiating a session lock after a defined period of inactivity.
- **AC-12. Session Termination.** Automatically terminate a remote session after a period of inactivity.

Centrify capabilities:

Centrify DirectControl extends Windows Group Policy capabilities to UNIX, Linux and Mac OS X systems and servers. From a central console, IT security managers can easily define configuration and security policies and then deploy them in a consistent and reliable manner.

- Group Policy can, for example, be used to set up login banners that display required legal notices to users upon login. This is just one of dozens of messages regarding login, password maintenance, and others that can be customized.
- Session management is particularly important for workstations, and Centrify also provides unparalleled support for locking down Mac OS X and other Linux workstations using Group Policy. User sessions can be locked after specific periods of inactivity, requiring users to re-enter passwords. SSH-based user sessions can also be terminated after a specific period of inactivity, requiring the user to re-login.

Auditing

Selected FISMA requirements:

- **AC-13 Supervision and Review.** Supervise and review the activities of users with respect to the enforcement and usage of information system access controls.

Centrify capabilities:

Centrify DirectAudit captures detailed user session information - who logged into what systems, what commands they executed, and what changes they made to key files and data. DirectAudit's flexible querying and reporting features can document compliance, showing what systems a specific user accessed, or which users accessed a specific system.

Access Methods

Selected FISMA requirements:

- **AC-17 Remote Access.** Authorize, monitor, and control all methods of remote access.

- **AC-18 Wireless Access Restrictions.** Use authentication and encryption to protect wireless access.

Centrify capabilities:

- Centrify DirectControl and DirectAuthorize can be used to control what user accounts are authorized to log in to specific UNIX/Linux systems, whether interactively or remotely. Centrify DirectAudit can monitor and capture complete user sessions. Because OpenSSH is one of the most popular tools for remote access, Centrify provides a packaged and tested version of OpenSSH that has been enhanced for secure, Kerberized access to UNIX/Linux hosts, and Centrify provides Group Policies to configure OpenSSH usage.
- Because Mac OS X computers can easily be configured to share Internet connections wirelessly, Centrify also provides a Group Policy to disable this feature. Group Policy can be used to control a user's access to network configuration settings to ensure that only authorized administrators are allowed to configure the network.

Centrify Solution for Audit and Accountability (AU) and Continuous Monitoring

Selected FISMA requirements:

- **AU-2 Auditable Events.** Generate audit records for organization-defined events.
- **AU-3 Content of Audit Records.** Produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
- **AU-4 Audit Storage Capacity.** Allocates sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.
- **AU-6 Audit Monitoring, Analysis, and Reporting.** Regularly review/analyze information system audit records for indications of inappropriate or unusual activity, and investigate suspicious activity or suspected violations.
- **AU-8 Time Stamps.** Synchronize internal information system clocks.

Selected FISMA 2.0/NIST SP 800-137 requirements for Continuous Monitoring:

- **Assess ongoing security control effectiveness and respond.** Based on ongoing monitoring activities modify existing security controls or put in place additional controls.
- **Record all relevant changes to the information system operating environment.** Document what changes were actually made, who made them and the impact to the operating environment.
- **ISCM architecture requirements.** Support scalable data collection, data storage, retrieval and reporting capabilities.

Centrify capabilities:

- Centrify DirectAudit can capture complete sessions, including all user activity and system output. And DirectAudit can be configured to report on events and commands targeted for monitoring – for example, commands that would suggest an attempt to edit privileged system files, create back-door accounts, or copy sensitive data. Once the effectiveness of a control has been analyzed modifications to system access and privileges can be easily accomplished with Centrify DirectAuthorize and Centrify Zones.

- Unlike many keystroke loggers, DirectAudit captures system output as well, ensuring IT auditors have sufficient forensic evidence to clearly establish the outcome of an action. DirectAudit documents all the changes made on monitored systems and with DirectAudit's unique replay feature, they can walk event by event through Windows, UNIX or Linux sessions to see exactly what happened.
- DirectAudit's architecture supports a massive scalable collection and distributed search architecture data storage leverages Microsoft SQL Server, which provides the performance and scalability required by large IT infrastructures. In addition, SQL Server has a rich ecosystem of tools for reporting, monitoring, optimizing and archiving data. In addition, Centrify Insight, a Splunk App, organizations can analyze and report on authentication, authorization and other events occurring on UNIX, Linux and MacOS X systems managed by Centrify DirectControl.
- Through the DirectAudit console, IT security managers can view active sessions and historical sessions, or build custom views that show sessions by specific users, machines, time periods, or other criteria. Full-text searches can be used to find, for example, all instances of a password command across all sessions. By adopting a non-proprietary SQL data format, DirectAudit also enables robust reporting, querying and alerting through third-party tools such as SIEM and event dashboards.
- It should be noted that the DirectControl Agent on each managed UNIX and Linux system automatically maintains time synchronization with Active Directory.

Centrify Addresses Requirements for Configuration Management (CM)

Selected FISMA requirements:

- **CM-2 Baseline Configuration.** Develop, document, and maintain a current baseline configuration of the information system.
- **CM-4 Monitoring Configuration Changes.** Monitor changes to the information system conducting security impact analyses to determine the effects of the changes.
- **CM-5 Access Restrictions for Change.** Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
- **CM-7 Least Functionality.** Configure the information system to provide only essential capabilities and specifically prohibit and/or restrict the use of prohibited and/or restricted functions, ports, protocols, and/or services.

Centrify capabilities:

- Through DirectControl's Group Policy feature, IT managers will have the ability to centrally and securely distribute configuration and security policies to UNIX, Linux and Mac OS X systems and workstations. DirectControl automates the distribution of policies using the same rules as Active Directory: on system startup, at user log on, or at a periodic and configurable refresh interval. Policies can also be refreshed on-demand. One particularly powerful benefit is that a baseline configuration can be set through Group Policy, and when new systems are added to a Zone they automatically get the policies, providing quick and consistent provisioning of new systems.
- Centrify DirectAuthorize can be used to ensure that systems remain "locked down" from a configuration and change management perspective. All users authorized to access a system can be given a specific set of rights, permitting IT managers to determine who can make changes and what they can do. DirectAudit can then be used to record session activity, verifying that the controls are in place and working as designed.

- DirectControl Group Policy can be used to lock down system settings to assist in enforcing a least functionality configuration for target systems.

Centrify Addresses Requirements for Identification and Authentication (IA)

Selected FISMA requirements:

- **IA-2 User Identification and Authentication.** Uniquely identify and authenticate users. Employ multifactor authentication for remote system access that is NIST Special Publication 800-63 compliant.
- **IA-3 Device Identification and Authentication.** Identify and authenticate specific devices before establishing a connection.
- **IA-6 Authenticator Feedback.** Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Centrify capabilities:

- The entire Centrify Suite of solutions – DirectControl, DirectAuthorize and DirectAudit – link entitlements and actions to a single, definitive and centrally managed user identity stored securely in Active Directory. Because Active Directory is used to extend basic network services to staff and contractors, it is usually the first (or one of the first) information stores to be updated as users are added or their roles change, and the Active Directory account is unfailingly disabled upon termination in order to shut off email and network access. Thus, it makes sense to consolidate identity and access management in this centrally managed directory.
- For Mac OS X workstations that require it, Centrify also supports two-factor authentication via smart cards. Centrify supports not only CAC cards but PIV and .Net cards as well.
- The Centrify Agent uses the same native protocols as Windows systems when communicating over the network. This means that UNIX, Linux and Mac OS X systems communicate to Active Directory (via domain controllers) over an authenticated and encrypted connection. Passwords, policies and other communication are thus shielded from inspection over the wire, in contrast to many UNIX/Linux environments in particular where data travels "in the clear."

Centrify Suite Addresses Requirements for Systems and Communications Protections (SC)

Centrify Suite provides a robust solution to secure systems, addressing many of the requirements defined by NIST Special Publication 800-53. The Centrify white paper titled "FISMA Compliance through Centralized Identity & Access Management Leveraging Microsoft Active Directory" provides details on how Centrify Suite addresses requirements for these FISMA categories: Access Control (AC), Audit and Accountability (AU), Configuration Management (CM) and Identity and Authentication (IA).

The Systems and Communications Protection family (SC) of requirements defined within NIST 800-53 defines a set of requirements to ensure that federal systems and their communications are properly protected. The technical requirements that DirectSecure combined with the Centrify Suite address are described in more detail in the following sections.

NIST 800-53 Requirement	Centrify Suite Capabilities
SC-7 Boundary Protection The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. (1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces. (2) The organization prevents public access into the organization's internal networks except as appropriately mediated. (3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. (5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). (6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	The fundamental requirement is to provide a defense-in-depth security solution that provides for a layered defense of critical systems. Firewalls should be used as the first layer in the defense to prevent external access and denial-of-service attacks. However, once on the enterprise network, which is often a shared resources, there is a need for domain isolation of a group of systems that serve within a given security domain or boundary. DirectSecure provides for domain- or group-based isolation in which members of the specified domain or Active Directory group are allowed to communicate in a secured fashion once they have mutually authenticated each other through strong host-based credentials. The policies, which DirectSecure enforces, are defined within Active Directory as a Group Policy to ensure that all systems where the policy applies will enforce the same security policy and will trust the same centralized credential authority. These policies are typically defined to deny all inbound traffic unless otherwise explicitly allowed for a specific authenticated system. The policy can also specify, based on the application, the level of integrity and confidentiality required based on the application or port used for communication. The policies apply to both inbound connections as well as outbound, enabling the administrator to require a system to authenticate to another trusted host within his access group prior to any outbound communications. This will prevent communications to external, untrusted systems, effectively preventing data leakage.
SC-8 Transmission Integrity The information system protects the integrity of transmitted information. The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	DirectSecure leverages IPsec in transport mode for network security and can be configured to use Authentication Header (AH) in order to ensure that any communication has not been tampered with and that it originated from the trusted host. This security is applied to each packet individually and leverages PKI credentials to establish unique session authentication keys for each security association. Integrity algorithm can either use MD5 or SHA1.
SC-9 Transmission Confidentiality The information system protects the confidentiality of transmitted information. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	DirectSecure leverages IPsec in transport mode and its Encapsulating Security Payload (ESP) in order to provide confidentiality for every packet exchanged between trusted hosts. This security is applied to each packet individually and leverages PKI credentials to establish unique session encryption keys for each security association. Encryption can be configured to use the 3DES algorithm.

NIST 800-53 Requirement	Centrify Suite Capabilities
SC-11 Trusted Path The information system establishes a trusted communications path between the user and the following security functions of the system: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).	DirectSecure leverages IPsec transport mode to establish a trusted peer-to-peer connection between two hosts that share a common trust and are able to mutually authenticate. This trusted communications is established between any two nodes on the network that are authorized to communicate based on the policies that each system will enforce. DirectSecure for UNIX and Linux supports interoperable trusted communications with Microsoft Windows XP and newer workstations as well as Windows 2003 and newer servers. This enables trusted path communications for both server-to-server as well as end-user-to-server.
SC-12 Cryptographic Key Establishment and Management When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	In order to simplify strong host identity management and to ensure that all trusted hosts have their own PKI certificate, DirectSecure enforces the Active Directory Group Policy for Public Key autoenrollment. This policy will require each host to request and periodically renew a machine PKI certificate from the Microsoft Certificate Authority. Additionally, every host will automatically retrieve and maintain the list of Enterprise Trusted Root Certificate Authorities, which are also managed within Active Directory. This greatly simplifies the distributed management of strong host credentials across a large heterogeneous enterprise.
SC-17 Public Key Infrastructure Certificates The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	DirectSecure leverages a Microsoft Certificate Authority that will be integrated with the local Active Directory to ensure that all systems configured for automatic credential enrollment will have a common trust and will validate certificates according to a common policy using CRLs or OCSP where appropriate.
SC-23 Session Authenticity The information system provides mechanisms to protect the authenticity of communications sessions.	DirectSecure uses IPsec in a transport mode configuration where each session to be established between a pair of hosts must be authenticated and must establish a security association for the session. These security associations define policy for the session, including the keys to be use and how long those keys will be valid.

DirectSecure provides a critical set of services to provide the protection assurance required for all baseline requirements, even the high assurance baseline. While the requirements above describe the protection of the system and the data in transit between the systems and the cryptographic standards that should be addressed, Centrify Suite also provides additional services to mitigate the risks of a compromised DNS infrastructure as described in requirements SC-20, SC-21 and SC-22. DirectSecure will associate a computer name with an Active Directory account and, prior to any communications, will require authentication based on that Active Directory account. This serves to reduce the dependency on DNS for authoritative name services to simply providing name-to-IP-address resolution. In this configuration, if an attacker were able to compromise an existing DNS server or establish a rogue DNS server, authentication to an invalid host would not be possible because it would not have the machine credentials associated with the Active Directory account normally associated with trusted systems.

Summary

FISMA compliance, as defined by NIST SP 800-53, is a complex process that reflects the broad scope, diversity and challenges of securing federal information systems. However, all of its requirements inevitably come down to commonsense and well established principles. In this white paper we have focused on issues that can be addressed through a strategy of leveraging Microsoft Active Directory for cross-platform identity and access management. Here is a summary of key NIST SP 800-53 principles and Centrify's solution:

AC Access Control ▪ Manage user accounts employing automated mechanisms ▪ Restrict access to systems and to privileged functions on those systems to authorized personnel ▪ Enforce separation of duties ▪ Enforce least-privilege rights management	**Centrify DirectControl** ▪ Consolidates non-Windows user identities in Active Directory so that all accounts can be centrally managed using existing automated tools and processes ▪ Uses unique Zone technology to create logical groupings of systems that have a discrete set of users, administrators and policies **Centrify DirectAuthorize** ▪ Restricts access methods and privileges based on job role ▪ Enforces least-privilege rights management by limiting users to a specific set of commands
AU Audit and Accountability ▪ Capture audit records in sufficient detail to establish what occurred, the source, and the outcome ▪ Enable regular review and analysis for unusual or suspicious activity	**Centrify DirectAudit** ▪ Captures complete session details: who accessed the system, what commands they entered, and the system output ▪ Provides unique ability to replay sessions to clearly establish outcomes of user activity ▪ Enables both real-time and historical monitoring of sessions, and features robust search and reporting capabilities
CM Configuration Management ▪ Maintain a baseline configuration for all systems ▪ Monitor for configuration changes ▪ Restrict user ability to make changes	**Centrify DirectControl** ▪ Group Policy provides a secure and automated method for centrally managing security and configuration settings **Centrify DirectAudit** ▪ Can audit systems for occurrences of prohibited commands **Centrify DirectAuthorize** ▪ Can lockdown systems by restricting user's rights to make changes
IA Identification and Authentication ▪ Uniquely identify and authenticate users ▪ Employ multifactor authentication where necessary ▪ Obscure feedback of authentication information	**Centrify DirectControl, DirectAuthorize, DirectAudit** ▪ Links all entitlements and actions to a single, definitive and centrally managed user identity in Active Directory **Centrify DirectControl** ▪ Supports smart card authentication for Mac OS X workstations ▪ Sets up authenticated and encrypted connection between Active Directory and managed systems
SC Systems and Communications ▪ Boundary Protection ▪ Transmission Integrity ▪ Transmission Confidentiality ▪ Trusted Path ▪ Cryptographic Key Establishment and Management ▪ Public Key Infrastructure Certificates ▪ Session Authenticity	**Centrify DirectSecure** ▪ Prevents unmanaged or rogue computers from communicating with trusted systems ▪ Restricts access to specific resources and logically segments the network ▪ Provides end-to-end encryption of data in motion ▪ Automates the provisioning and management of PKI certificates

Appendix A: Table of IT Related Provisions Affecting Federal Agencies

Legislation & Executive Orders	
Clinger-Cohen Act 1996 (CCA)	The Clinger-Cohen Act of 1996 (CCA) was a combination of the Information Technology Management Reform Act of 1996 and the Federal Acquisition Reform Act (FARA) of 1996. The CCA required each agency to name a Chief Information Officer (CIO) with the responsibility for "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture." CCA required agencies to adopt performance-based management principles. Commercial off-the-shelf (COTS) procurement was encouraged to promote standardization and the elimination of standalone government systems.
USA PATRIOT Act	The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law Pub.L. 107-56, expanded the authority of law enforcement agencies to search and collect data in the areas of telephone, e-mail communications, medical, financial and other records; eased restrictions on foreign intelligence gathering within the United States; expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and enhanced the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. The data collected and stored on federal agency systems is tightly controlled and may labeled as "For Official Use Only," "Law Enforcement Sensitive," "Sensitive But Unclassified," or "Classified."
Critical Infrastructure Information Act	The Homeland Security Subtitle B-Critical Infrastructure Information Act 2002 (CIIA), Public Law 107-296,is a group of provisions that was enacted, in part, to respond to the need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets. The act defines when the Department of Homeland Security may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program, and it places limits on the disclosure of critical infrastructure information voluntarily submitted to DHS.
HSPDs 7, 12, 54/23	Homeland Security Presidential Directive 7 (HSPD-7) requires federal executive departments and agencies to develop methods and technologies to protect all critical infrastructures and resources – including physical and computer-based systems – of the government and economic sector in case of terrorist attack. The goal is to ensure the continuity and viability of essential infrastructures for minimal functioning of the U.S. government and economy. One outgrowth of this directive has been an increased emphasis on establishing uniform policies, approaches, guidelines, and methodologies for integrating federal systems within and across sectors. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors 2004, required federal executive departments and agencies to implement a governmentwide standard for secure and reliable forms of identification for employees and contractors. HSPD-12 addresses access both to physical facilities and to information systems, and it designates major milestones for implementation. In practical terms, HSPD-12 has driven the adoption of smart cards as the agreed-upon method for implementing more secure authentication to computing systems based on something stronger than traditional username/password challenge systems. NSPD-54/HSPD-23, issued in January 2008, directs a comprehensive national cybersecurity initiative aimed at deterring hostile action in cyber space by making it harder to penetrate our networks. It also made the NSA the lead agency in monitoring and protecting all of the federal government's computer networks from cyber-terrorism.

Standards, Guidelines and Publications	
National Strategy for Physical Protection of Critical Infrastructure and Key Assets	The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets 2003 identifies national goals and outlines the guiding principles for securing the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence. It establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities effectively and efficiently.
National Strategy to Secure Cyberspace	The National Strategy to Secure Cyberspace outlines an initial framework for both organizing and prioritizing efforts and provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve the national collective cybersecurity.
National Infrastructure Protection Plan	The National Infrastructure Protection Plan (NIPP) and supporting Sector-Specific Plans (SSPs) provide a coordinated approach to Critical Infrastructure and Key Resources (CIKR) protection roles and responsibilities for federal, state, local, tribal, and private-sector security partners. The NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources, which will help ensure that the government, economy, and public services continue in the event of a terrorist attack or other disaster. The plan calls for strong partnerships and information among the public and private sectors, and establishes a risk-management framework. A working group consisting of federal and private representatives was established for each of the identified major sectors of the critical infrastructure, and each department and agency of the federal government was also responsible for developing its own CIP plan. The DoD was in addition charged with creating plans in the areas of policy and strategy, intelligence support, industrial policy, defense security, information assurance, research and development, and education awareness.
OMB A-130	Office of Management and Budget Circular A- 130, "Management of Federal Information Resources," requires federal agencies to implement and maintain adequate security over information, information systems, and major applications. The main thrust of A-130 is to drive security responsibilities down to the users and managers of computer systems and information. Since computers and electronic access are available to almost everyone, this approach is necessary to address security in current information technology environments. Previous computer security policies and programs have focused on securing data processing centers and large custom applications.
NIST 800-18, 800-37, 800-137, 800-53, 800-59, 800-60	NIST Special Publication 800-18 provides guidance on developing systems security plans, which provide an overview of the security requirements of the system and describe the controls in place and monitoring for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. NIST Special Publication 800-59 provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system. The Department of Defense and the Director of Central Intelligence have authority to develop policies, guidelines, and standards for national security systems. The Director of Central Intelligence is responsible for policies relating to systems processing intelligence information. NIST Special Publication 800-60 recommends the types of information and information systems to be included in each category of potential security impact. It helps agencies consistently map the security impact levels to types of information (privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation) and information systems (mission critical, mission support, administrative). The guideline applies to all federal information systems other than *national security systems*.

Federal Desktop Core Configuration	The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC currently exists for Microsoft Windows Vista and XP operating system software.
DHS IT Security Essential Body of Knowledge	The DHS-NCSD developed the IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development as an umbrella document that links competencies and functional perspectives to IT security roles fulfilled by personnel in the public and private sectors.
ISO 27002/17799	ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It provides general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in a variety of areas, including security policy, physical security, access control, systems acquisition and maintenance, and compliance.
Committee on National Security Systems Instruction No. 4009	The National Information Assurance Glossary is an unclassified glossary of Information security terms intended to provide a common vocabulary for discussing Information Assurance concepts.
DoD Directive 8500.1 DoD Information Assurance Certification and Accreditation Process (DIACAP)	The United States Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) defines a risk-based management approach for managing DoD information systems and defines a standard set of formal activities for certifying and accrediting such programs.