okta

Meeting the Latest NIST Guidelines with Leading-Edge Technology

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Meeting the Latest NIST Guidelines with Leading-Edge Technology

Today's Evolving Security Guidelines

Traditional security is insufficient to protect the cloud and hybrid infrastructure of today's enterprise. Our users have adopted new styles of working, and new ways of connecting. As IT becomes nimble—adopting ever increasing cloud solutions—the organization's sensitive information is everywhere.

Enter the digital identity. It's used in nearly every aspect of daily life. The average employee has a multitude of services (Experian says over 40[1]) registered to any one of their personal or business email accounts. At the enterprise, our employees use their identity to access critical data and services now sprawling across cloud, SaaS and on-premises applications.

Simply updating identity or access tools are not enough. Governments and enterprises need guidance in adopting and implementing today's identity and access management solutions. The National Institute of Standards and Technology (NIST), the foremost standards body for cybersecurity, has released updated guidance that aligns with market-driven business models, innovation and addresses the new risks these present.

> "If you are a defense or government supplier—or subcontractor to a government supplier—you will need to comply with NIST Special Publication 800-171(SP 800-171) Protecting Covered Defense Information in Nonfederal Systems and Organizations by December 31, 2017."

This white paper discusses certain compliance and legally-related concepts, but to be clear, it does not constitute legal advice. If you or your organization need legal advice, be sure to consult with your own counsel. All content provided in this document is made available for informational purposes only.

Today's risks require a marriage between security and identity

If the barrage of recent data breaches tells us anything, it's that identity is the new currency in the market. According to Symantec's Internet Security Threat Report, 1.1 billion identities were stolen in 2016 alone[2]. Armies of botnets are attempting to reuse and harvest stolen credentials in drive-by downloads or targeted phishing scams—all while we are still struggling with security basics. The 2017 Verizon Data Breach Investigations Report revealed that last year alone, 81% of hacking-related beaches leveraged weak or stolen passwords[3]. Society's standards around access and identity have been slow to evolve and in turn our authentication strategies have remained stagnant—for nearly 15 years. Passwords are still in use in most organizations and those same entities use multiple solutions to manage access across their sprawling enterprises. Identity represents a critical control point that, once addressed, dramatically improves security across the ecosystem. Entities supporting federal agencies are now being held to new identity standards,

[1] Mike Delgado. "Experian Reveals the Five Key Factors That Make People & Business More Vulnerable to Cyber Fraud." Experian. May 19, 2016
[2] "Internet Security Threat Report, Volume 22." Symantec. April 2017.
[3] "2017 Data Breach Investigations Report (DBIR)." Verizon. 2017.

requiring them to take a new look at Identity and Access Management (IAM) in accordance with updated guidelines and mandates. They are looking for a comprehensive solution that understands and meets these requirements.

NIST Meets the Changing Risk Landscape with Major Changes

In an effort to address today's risks nearly all standards have recognized that we can no longer secure access to our organization with single factor authentication: a simple password. For all federal agencies and government suppliers, NIST standards mandate the use of Multi-Factor Authentication (MFA) for privileged access and remote access to the network—essentially all of today's modern knowledge workers.

What is NIST?

Founded in 1901 the National Institute of Standards and Technology (NIST) is one of the nation's oldest physical science laboratories and is dedicated to supporting America's competitiveness. Responsible for The Cybersecurity Framework, NIST helps businesses and governments understand and address today's quickly evolving cyber risks.

Further, the latest release of NIST's Special Publication 800-63, Digital Identity Guidelines, wipes away our old password rules and places the burden of access in the hands of identity and access technology. Many other security standards are following suit as the Payment Card Industry Data Security Standard (PCI DSS) requires MFA around applications and infrastructure supporting and processing payment card data. Similarly, new mandates from New York Department of Financial Services (NYDFS) require certain covered enterprises to move beyond legacy authentication solutions and implement robust IAM that supports MFA and a federated architecture to reach today's cloud, mobile, and on-premises services.

Why NIST compliance matters to your enterprise

A leader in cybersecurity research and standards, NIST operates in an open and transparent manner inviting collaboration from the public and private sector. Addressing everything from critical infrastructure to sensitive government systems and industrial competitiveness, NIST standards provide a broad range of recommendations meeting the compliance needs of other regulations like NYDFS, the Health Insurance Portability and Accountability Act (HIPAA), and support industry standards like PCI DSS.

NIST is not just for federal, state or local government systems; over 30 percent of U.S. organizations[4] are using NIST guidelines, particularly the Cybersecurity Framework. In fact, if you are a defense or government supplier—or a subcontractor to a government supplier—you will need to comply with the latest NIST guidelines.

Recent federal acquisition directives for both civilian and DOD agencies require compliance protection for all information created by the government, or an entity on behalf of the U.S. Government. To provide a framework for compliance, NIST issued SP 800-171, Protecting Covered Defense Information in Nonfederal Systems and Organizations, containing 14 control families, with associated controls including guidelines for Authentication and Identity Management. NIST SP 800-171 geared towards protection of sensitive unclassified federal information that is housed in, processed or transmitted by non-federal information

[4] "NIST Impacts: Cybersecurity." NIST. 2017

systems and environments. The 800-171 fits neatly into The Cybersecurity Framework and is supported by the most recent release of NIST Digital Identity Guidelines.

Generally speaking, NIST compliance is often considered cumbersome and costly by many security teams. Navigating NIST recommendations for authentication and identity management is Okta's business. Okta's cloud-native access management centralizes IAM and offers a full range of factor and assurance level support across standard identity categories.

Meeting NIST Requirements with Okta is Easy

Organizations often begin with an assessment to identify gaps in compliance across their enterprises. Though Okta's solutions do not span across all 14 control families, Okta offers a centralized solution to meet your security and compliance needs around Identification and Authentication and Access Control. Key Okta attributes/capabilities include the ability to:

- Centralize identity management throughout the ecosystem,
- Implement simple authentication that is adaptive, risk-based and flexible,
- Reduce your attack surface with automated lifecycle management, and
- Enable visibility and response

Centralize identity management throughout the ecosystem

Regardless of compliance or business need, Okta ensures strong authentication across all services, everywhere. Workday, Microsoft Office 365, Salesforce, etc.—Okta integrates seamlessly with the applications you are already using. The Okta Identity Cloud uses standards based protocols and API's to integrate with over 5,000 applications, IT infrastructure, and devices. Our federated architecture is recommended by the latest NIST guidelines and is fully compliant with 800-63C's identity federation and assertion recommendations.

Identity management doesn't start and stop at the enterprise cloud services and neither does Okta. You can secure existing on-premises infrastructure with the same IAM from Okta. Supported by rich SAML, your cloud IAM can be your primary IAM with delegated authentication to AD or LDAP and third party IDP. Connect to a broader set of systems in the data center from RADIUS, Windows Credential Provider, to other infrastructure like Citrix, F5 and Remote Desktop.

Your IT team wants a simple and easy management that includes out-of-the-box integrations with a variety of applications, custom application integration options, phased deployment options, and centralized administration and management to ensure compliance across all applications and services. You need to reduce identity sprawl and unify under one, federated architecture that can intelligently provide the policy flexibility, automation, and intelligence to meet the demands of identity management in today's enterprise.

Implement simple authentication that is adaptive, risk-based and flexible

Okta not only meets regulatory mandates in secure authentication and identity protection but sets a new baseline with two-factor authentication across all solutions. Not just through the use of step-up security or added protection around critical infrastructure or services, Okta adds a simple one-time passcode to every Single Sign-On user so that two-factor authentication is now the authentication for every Okta user.

Context-driven protection

Okta's MFA is adaptive in addressing the entire digital profile including the user, device, and network. Okta's Identity Cloud monitors behaviors and detects anomalies in access behavior. Is the user attempting to connect from an unknown device? Are they on a trusted network or out-of-band? With this information, your team can dynamically adapt security and authentication policies to enforce step-up authentication for each individual user and situation. Further, Okta's new device login notification informs the user when an unknown device or browser attempts to connect.

NIST recommends shifting away from SMS-based two-factor verification. Okta Verify and Verify Push smartphone apps allow you to keep a second factor on your mobile and steer clear of SMS.

Factors for every situation

Okta's Adaptive MFA enables robust features that not only meet standards' recommendations but strengthen access and authentication across all users, applications and devices. Okta's Adaptive MFA meets updated NIST guidelines by enabling a comprehensive set of second factors shifting away from SMS-based verification to stronger options offered by mobile apps, biometrics and unique PINs. The Okta Verify and Verify Push smartphone apps allow users to authenticate leveraging smartphone apps with ease of use that is as simple as a tap acknowledgement from the user. Okta MFA also supports biometric access with Touch ID, and Windows Hello.

Flexible to meet users' needs

NIST's most visible changes in guidance are around password complexity rules announced in the Digital Identity Guidelines. Okta's flexible admin consoles allow IT to adjust password length, complexity and update schedules to meet this new paradigm. Further, you can enable Okta's Common Password Detection to meet these new guidelines and improve your users' password origination. Common Password Detection will detect and prevent users from defining weak or easily breached passwords.

Reduce your attack surface with automated lifecycle management

Okta allows you to easily and simply create a more defensible perimeter for the whole organization and protect against unauthorized access. Centrally manage the cycle of events in your users' identity from enrollment, to evolving access across systems and services, to renewal and termination. Managed consistently across enterprise services affords the greatest compliance with key controls.

Accurate entitlement and automate on- and off- boarding

Okta is centrally managed and automated which helps to ensure accurate entitlements and allows you to scale provisioning, deprovisioning across all users, groups, and permissions policies. Onboarding becomes turnkey. Administrators have at-a-glance visibility into users' access to every app, service and data store.

Reduce the risk of lateral movement

Better management not only equates to compliance but improved security. Reducing over-privilege and orphan accounts shrink your attack surface. With Okta, you gain assurance that each account has the right level of access, assigned by policies, and reinforced with step-up authentication based on membership groups and user/device context. Cut the lateral movement by unauthorized users and eliminate privilege escalation.

Enable visibility and response

You have not truly married your IAM with security until you connect directly to your security infrastructure and enable greater visibility and rapid response. With Okta real time authentication, data is accessible by one syslog API. Identity events are seamlessly tied to security management tools like Splunk, ArcSight, IBM QRadar, Palo Alto Networks, and F5 Networks, among others. You will be able to see brute-force or DDoS attacks as they occur. You can take immediate action to challenge account takeover attacks as they occur individually or in multiples across your enterprise. Real-time data from Okta enriches correlation and ultimately enable rapid response. Security teams react immediately reducing containment and mitigation time.

Okta’s NIST 800-171 Compliance Matrix

Map your assessment to Okta’s compliance with the NIST 800-171 controls.

3.1	Access Control	
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Okta offers a sophisticated lifecycle entitlement management that can ensure the right level of access to the right applications through a set of centrally managed policies. • Administrators can easily set access and entitlement rules based on attributes, such as user group membership. • Okta provides visibility into who has access to which data via simple access governance that offers the ability to see all users who have access to specific applications. • Defined users can be assigned to established groups and provided access to applications and services by group.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	

3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Privileged users can be placed into a group and control around accounts and resources can be provided within this group.
3.1.8	Limit unsuccessful log-on attempts.	Okta's SSO and MFA solutions allow IT admins to manage unsuccessful log-on attempts in accordance with the organization's policy guidance.
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Okta's SSO automatically monitors session activity and allows IT administrators to centrally manage organizational policy for session timeout and reauthentication processes. Session termination rules can be established as well as unlock processes using time out or Help Desk intervention.
3.1.11	Terminate (automatically) a user session after a defined condition.	
3.1.12	Monitor and control remote access sessions.	Okta's IAM and AMFA solutions offer a non-disruptive, non-intrusive, easily integrated solution that works with your Virtual Private Network (VPN), Remote Desktop Protocol (RDP) and Secure Shell (SSH). Okta's IAM maintains logs for monitoring and the ability for initial access with MFA for remote sessions.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
3.1.20	Verify and control/limit connections to and use of external information systems.	Okta's Single Sign-On (SSO) and MFA solutions can verify and control connections to external systems but may not limit those connections.
3.5	Identification and Authentication	
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	Okta's identity-led security framework can solve IAM control challenges by centralizing identity integration with Active Directory and LDAP to verify and manage users accessing corporate resources.

3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Policy guidance is set by the organization, but Okta's flexible policy framework allows for step-up authentication to verify users before they access accounts and services using Okta's SSO and MFA.
3.5.3	Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Okta's Adaptive MFA affords intelligent, contextual access based on the user groups defied in Okta's lifecycle management.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Okta's Adaptive MFA supports a variety of factors such as One-Time Password, Okta Verify, Okta Verify Push, physical tokens and biometric factors.
3.5.5	Prevent reuse of identifiers for a defined period.	User can be deactivated in SSO (instead of being deleted) to prevent reuse of identifier/username.
3.5.6	Disable identifiers after a defined period of inactivity.	Okta's SSO policies include a session logout after a defined period in accordance with the organization's policy guidance.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Okta's centralized management console allows IT professionals to adjust password lengths and complexities and update schedules in keeping with current NIST guidelines.
3.5.8	Prohibit password reuse for a specified number of generations.	SSO policies can be established to ensure a user does not match previous passwords in accordance with the organization's policy guidance. Using common password detection can help you meet compliance guidelines by detecting and preventing users from defining weak or breached passwords.

3.5.9	Allow temporary password use for system log-ons with an immediate change to a permanent password.	Okta eliminates the need for temporary passwords by sending a password reset link to new users.
3.5.10	Store and transmit only encrypted representation of passwords.	Okta encrypts passwords with a high number of iterations. Okta stores and transmits only encrypted data.
3.5.11	Obscure feedback of authentication information.	Okta's flexible policy management allows IT to determine if passwords should be obscured from the user or displayed to support NIST's latest guidance.

Conclusion

Meeting the latest federal cybersecurity requirements around identity and access does not have to cost tens of thousands of dollars or require months of implementation. Because of its size and breadth, NIST offers a broad range of standards often reflected by other standards. The guidance from NIST 800-171 is required for any supplier to the federal government—or sub-contractor to a government supplier—by December 31, 2017 or you risk losing the federal business. The hard part is assessing your compliance and developing plans to address any gaps. The NIST guidelines do offer security measures that your organization should already be implementing as part of maintaining a mature security program.

Okta provides a comprehensive solution that allows you to quickly meet the Identity Management and Access Control requirements and seamlessly improve your security posture. Okta offers a solution that immediately meets the most significant hurdle for most organizations. Okta's Identity Cloud and Single Sign-On solution integrates into the applications you are already using in the cloud and corporate data center. With any Okta solution you not only meet the latest security standards but shrink your attack surface by placing Adaptive MFA in front of literally everything in your enterprise. Lifecycle management is often the largest hurdle in identity management compliance. Okta gives IT admins the central management, policy flexibility, and at-a-glance views they need to efficiently manage the lifecycle of user identities. Finally, centralizing IAM must include visibility into authentication events in real time. Okta offers flexible data access via native, or API, SIEM integration. Security engineers can take immediate action on events thwarting attacks before they expand.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device. Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work

Learn more at: www.okta.com