eBOOK

Addressing CJIS
with Identity Governance

SailPoint

The scale of cybersecurity threats and breaches from internal and external actors continue to impact state and local governments. This has led to billions of identities and sensitive data that has been compromised. Organizations today expect to be breached, and unfortunately, it still takes months to find and contain a malicious actor inside the network. Furthermore, most organizations cannot produce a report showing who has access to sensitive systems and accounts within 24-hours.

Digital transformation and IT modernization strategies are at the top of most organization's priorities. As enterprise organizations continue to modernize, this entails more applications and data, extending the perimeter, different types of users, and robotic process automation or bots all accessing enterprise resources. How can organizations provide efficient and secure access to all applications and data on-premises and in the cloud while ensuring compliance and security?

Legislation, industry standards, and governing bodies continue to increase security and privacy control requirements, and federal, state, local governments, and commercial enterprises alike are subject to a myriad of compliance regulations. At times, privacy and security control requirements can hinder an organization's ability to be flexible, transform the enterprise, and conduct business efficiently and confidently. Security and compliance teams must work together to maintain efficiency and cybersecurity posture.

Navigating Security Frameworks and Standards

The National Institute of Standards and Technology (NIST) has developed the NIST Cybersecurity Framework (CSF) that has been highly adopted by government and industry. This voluntary framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors vital to the economy and national security. The CSF allows for the organization to plug-in control families from the NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations or other security and privacy frameworks. Many other frameworks have been derived from or include NIST SP 800-53 Security Controls, such as NIST SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The CJIS Security Policy guides the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.

The CJIS applies to every individual–contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity–with access to, or who operate in support of, criminal justice services and information.

Each of the frameworks, standards, and policies use similar concepts and best practices whilst terminology may differ.

Identity Governance Strategy

There are several activities and functional areas where a strong identity strategy is critical in the implementation, enforcement, monitoring, and auditing of individual security controls for access to digital and physical resources. Cybersecurity decision-makers and implementers can use best leverage Identity Governance and Administration (IGA) features and capabilities in the enterprise where security and risk are paramount in the overall security ecosystem.

Identity Governance capabilities and features include:

- Lifecycle Automation - employees, contractors, business partners, RPA/bots
- Identity Governance controls:
  - Role-based access control (RBAC) model
  - Policy model–suitability and separation of duties (SOD)
  - Risk model–user, application, policy, entitlement
- Account and Password Management
- Privileged Account Governance
- Application and Cloud Governance
- Centralized Application Access and Self-Service Fulfillment
- Access Certification, Auditing, and Reporting
- Advanced Identity Analytics

Supporting Framework Functions and Activities

Identity Governance and Administration (IGA) addresses key functions of security frameworks.

Identify – Identity Governance provides a comprehensive view of enterprise systems, people, assets, and data and the relationship or context related to cybersecurity risk for systems, assets, and data.

Protect – Identity Governance implements a model-based (Role, Attribute, Policies, Risk) approach to provisioning and access control, ensuring that access is authorized and appropriate and that only necessary access is granted to systems, assets, and data.

Detect – Identity Governance establishes the baseline of what a user's access should look like or which activities they can perform.

Recover - Identity Governance provides visibility, via Advanced Identity Analytics, into unauthorized access, overentitled, and risky user access to systems, assets, and data. Identity metadata provides contextual information and enriches security event analysis to validate and identify compromised or rogue users significantly reducing noise for security operations analysts.

Respond – provides business process automation and workflows to ensure that all access is authorized, appropriate, and suitable and removed when no longer valid or required.

Conclusion

The SailPoint Identity platform provides the enterprise secure and straightforward access and ensures that it is the right access. The platform allows the enterprise to define and govern access rights to minimize the risk associated with entitlement creep, orphaned accounts, and separation of duty and suitability policies. When properly implemented, the platform will provide visibility to "Who currently has access," "Who should have access," "Is the access suitable," and "How is the access being used for all systems, applications, and data everywhere – on-premises or in the cloud."

The SailPoint Identity platform:

- Provides the foundation for modern security architecture and frameworks
- Ensures appropriate access is granted timely and efficiently
- Initiates identity, application, or entitlement-based certifications
- Enriches security events with contextual identity information
- Uses continuous monitoring to gain insight into events and behaviors that move into and through an environment
- Leverages security orchestration automation and response (SOAR) technologies to auto-remediate events including automatically disabling or removing access from identities

To learn more about SailPoint identity solutions for state and local governments, please visit **www.sailpoint.com/identity-for/government.**

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

EB1345-2004