NIST SP 800-53 Revision 4:

Implementing Essential Security Controls with Cyber-Ark® Solutions

May 2013

Table of Contents

EXECUTIVE SUMMARY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidance for the selection of security and privacy controls for federal information systems and organizations. Revision 4 is the most comprehensive update since the initial publication. This update was motivated principally by the expanding threat space and increasing sophistication of cyber attacks. Major changes include new security controls and control enhancements to address advanced persistent threats (APTs), insider threats, and system assurance; as well as technology trends such as mobile and cloud computing.

Cyber-Ark's solutions help federal agencies implement effective controls for privileged and administrative identities and access to sensitive information.

The recommended security controls in NIST SP 800-53 can help agencies to comply with applicable federal laws, regulations, and standards such as the Federal Information Security Management Act (FISMA). NIST SP 800-53 makes recommendations regarding a full range of controls. It specifically acknowledges that there are significant challenges to determining the most cost-effective, appropriate set of controls and implementing them in order to effectively mitigate risk.

Focusing on Targeted Accounts

Given the escalating threat landscape, a major focus area for many agencies will be improving the implementation of controls regarding privileged access. As with the previous version, Revision 4 includes an extensive array of controls that relate to protecting privileged accounts and strictly controlling and monitoring their use. Revision 4 puts even more emphasis on these shared, all-powerful accounts.

With extremely profuse access rights, privileged and administrative identities are basically the organization's "keys to the kingdom." As such, these types of accounts are prime targets for insider or external threat actors. In fact, APT-style attacks almost always exploit privileged credentials.

Protecting the "Keys to the Kingdom"

In most organizations today, typical IT environments are comprised of hundreds or thousands of servers, databases, virtual machines, network devices and applications, all controlled and managed by a variety of privileged and administrative identities such as:

- **Shared administrative accounts** – "super user" privileges often anonymously shared among IT staff. Examples include Windows Administrator, UNIX root, an Oracle SYS account, or Cisco Enable user. They can be used to modify system configurations, access entire databases, change security settings on network devices, gain control over applications, reconfigure audit logs, and so on.
- **Application and service accounts –** hard-coded, embedded credentials found in virtually every piece of hardware, software, and application within an organization, including virtual environments. These accounts typically have broad access rights to

underlying information.

- **Emergency accounts** – elevated privileges used to fix urgent problems, such as in cases of business continuity or disaster recovery. They are often called breakglass or fireIDs.

Inadequate security controls for privileged and administrative identities create significant risks for an organization; but these controls are often lacking. For example, without the benefit of a privileged account security solution, it is difficult to sufficiently monitor usage of privileged identities. With shared or generic accounts, systems do not usually track which individual users login in as administrators - merely that an administrative login occurred. Privileged account passwords can be more susceptible to compromise because they are typically changed less frequently than personal non-privileged accounts, if at all. As well, administrative or application accounts can often be impossible to disable due to the high potential for disruption to business. Moreover, manual processes to manage and update these accounts are prone to error and costly.

Organizations today also face a constant, growing need for secure, authorized access to their most sensitive information. Current trends such as the rise of mobile workforces and expanding use of service providers further increase the risks that sensitive information will fall into the wrong hands. Organizations must know exactly who is accessing and sharing confidential files, documents and reports, and balance availability with security.

Implementing Effective and Efficient Controls with Cyber-Ark® Solutions

To help agencies implement the necessary controls for managing the risks of privileged and administrative identities and access to sensitive information, Cyber-Ark solutions:

- **Manage and control access to all privileged accounts** - including automating password changes and rendering hard-coded application credentials invisible to all developers and administrators
- **Isolate, control and monitor privileged access** - to sensitive servers, databases or virtual machines
- **Provide a secure repository to protect sensitive information** - whether sharing it across the organization or transferring it to external parties

Pre-defined policies and workflows help streamline the implementation of controls.

Realizing Key Benefits

With Cyber-Ark's solutions, federal agencies can implement effective and efficient controls to:

- Control privileged activities and access to sensitive information
- Protect critical assets
    - Including operating systems, servers, databases, virtual machines, applications, firewalls, security systems, network devices, routers, and more
- Secure cloud environments
    - Control entire privileged access to all components within a private cloud
- Achieve consistent enforcement of policy across the entire organization
    - Replace ineffective and inefficient manual processes with reliable, automated

solutions
- Ensure comprehensive audit logging
    - Including tracking individual administrators' command-level activities
- Increase situational awareness and visibility over privileged users and sensitive documents
- Reduce overhead and increase productivity
    - Decrease or reassign staff to more productive work
- Detect advanced threats with real-time session monitoring of privileged access and activity
- Leverage existing investments
    - Streamlined integration with an organization's identity infrastructure including directories, provisioning, monitoring, security, and authentication systems
- Safeguard information using tamper-proof storage based on FIPS 140-2 validated cryptography

Addressing the Controls

The main NIST SP 800-53 Control families addressed by Cyber-Ark's solutions include:

Access Control

The Access Control family deals with managing and enforcing access rights, as well as authorizing and restricting access to information. It covers issues of account creation and assignment as well as when and how credentials should be used. Therefore, it contains many guidelines regarding the special care and attention that needs to be given to privileged accounts and their elevated access rights. For example, the Account Management control guidance states, *"Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access."*

For several of the controls in this family, Revision 4 adds specific control enhancements related to privileged access such as "Restrictions on use of shared groups/accounts," "Shared group account termination," and "Prohibit non-privileged users from executing privileged functions."

Cyber-Ark's solutions can be used to address the full set of access control recommendations as they relate to managing privileged and administrative identities including shared/group accounts, for meeting or even exceeding baseline requirements. This includes comprehensive privileged account lifecycle management, discovering and securing the accounts, enforcing access control policies, and auditing privileged access. Organizations can also control privileged sessions including who can initiate sessions and for how long, as well as restrict and monitor third-party access to the network.

For accessing sensitive information, the Access Control family specifies several controls regarding how information should be controlled, encrypted, accessed, and shared. Cyber-Ark provides a complete solution for storing and sharing sensitive information, whether inside the organization or with other entities.

Audit and Accountability

The Audit and Accountability family involves determining audit events and ensuring those events are adequately recorded and analyzed and the audit records are reliable and protected. The control "AU-3: Content of Audit Records" specifically addresses the requirement for individual accountability. It lists the required data for each audit record, and states that *"The information system generates audit records containing information that establishes what type of event and the identity of any individual associated with the event."*

Cyber-Ark's solutions helps organizations to meet the requirements of the Audit and Accountability family by providing extensive audit logging for events involving privileged accounts and access to sensitive information. Examples include logging the use of a privileged password or the transfer of a sensitive file, including the identity of the individual.

All Cyber-Ark logs are properly time-stamped, cryptographically protected and stored in the tamper-proof digital vault, referenced to a specific user in the system and stored for as long a period as required by the organization. Cyber-Ark products can also generate alerts on specific occurrences and feed into Security Information and Events (SIEM) products including HP ArcSight, McAfee ESM and RSA enVision.

Identification and Authentication

The Identification and Authentication family encompasses controls related to establishing and verifying the identity of users. The control "IA-2: Identification and Authentication (Organizational Users)" requires users be uniquely identified. The control asserts *"The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)."* It can be challenging to meet this requirement, especially for privileged generic accounts that are shared among the IT staff. Shared accounts diminish accountability and create vulnerabilities due to password knowledge. The control "IA-5 Authenticator Management" is concerned with the management and use of authenticators, such as passwords. The requirements include ensuring authenticator strength, defining their lifetime, updating them periodically, protecting them, and managing their revocation.

For privileged and administrative accounts, Cyber-Ark's solutions uniquely identify all users, including individual use of shared accounts. Complete lifecycle management for privileged account passwords is provided, helping organizations meet the authentication management requirements.

IA-5 Control Enhancement (7) addresses the key problem of hardcoded, clear-text passwords in applications, by requiring that "The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys." Cyber-Ark's solutions eliminate hard-coded passwords. They ensure periodic password refresh with no system downtime and provide enhanced secure authentication and a secure cache mechanism in the event of a network outage.

Confronting Advanced Threats

Revision 4 provides specific guidance regarding APTs and points out several key controls to consider. Cyber-Ark's solutions support the implementation of many of the recommendations applicable to APTs including:

- AC-6 (9) Auditing use of privileged functions
  - Cyber-Ark's solutions audit all access to privileged functions
- CM-5 (4) Dual Authorization
  - Cyber-Ark provides "Dual Control" which requires that an additional authorized administrative user approve requested actions before being granted, such as configuration changes
- SC-29 Heterogeneity
  - Cyber-Ark's products integrate with the full-range of diverse operating systems, applications, databases, security appliances, network devices, directories, virtual machines and storage found in today's IT environments
- SC-34 (3) Non-Modifiable Executable Programs
  - Cyber-Ark's technology uses hardware-based protection mechanisms

"Assurance" is another important aspect of defending against APTs as presented in Revision 4. It advises that as organizations become susceptible to APTs, increased levels of assurance may be required. A large number of controls related to assurance are clustered in the Systems and Services Acquisition (SA) family. With Revision 4, many of the SA controls have been added or expanded. Cyber-Ark can address many of the SA controls. The company provides proven technology that is certified by ICSA labs and FIPS 140-2 compliant. It was designed based on highly-acclaimed security engineering principles and best practices.

Overall, Cyber-Ark's solutions can help organizations to implement a wide-range of controls from each of the control families. The following sections in this document detail how Cyber-Ark's solutions address the controls of NIST SP 800-53 Rev. 4 and provide an overview of the product suites offered by Cyber-Ark.

ADDRESSING NIST SP 800-53 REV. 4 RECOMMENDATIONS

According to the NIST SP 800-53 Revision 4 recommendations, organizations determine security controls by first categorizing information systems as low-impact, moderate-impact or high-impact. Organizations are guided to select controls supplemented with control enhancements to attain "LOW", "MOD" or "HIGH" security baselines; and then tailor the controls to their own requirements, which may include additional control enhancements.

The table below describes how Cyber-Ark's solutions help organizations to implement the controls and control enhancements provided in NIST SP 800-53 Revision 4[1]. Cyber-Ark's solutions can be can be used to meet or exceed LOW, MOD or HIGH baselines. For each control family, the table lists the controls that can be addressed with Cyber-Ark's solutions and provides an explanation of how. Where applicable, some information on specific control enhancements is also provided.

No.	Control	How do Cyber-Ark's Solutions Help?
Family: ACCESS CONTROL		
AC-1	ACCESS CONTROL POLICY AND PROCEDURES Involves development of an access control policy as well as procedures to facilitate implementation of policy and associated controls including periodic reviews and updates.	With Cyber-Ark's solutions, organizations can consistently implement policy and procedures and effectively implement automated controls for privileged access and access to sensitive documents. Pre-defined policies and workflows help streamline implementation of controls, built-in audit-ready reports enable efficient reviews and flexible architecture and management environments provide support for updating controls.
AC-2	ACCOUNT MANAGEMENT Covers full range of activities related to managing accounts.	Cyber-Ark provides comprehensive solutions for automating all of the processes associated with privileged account lifecycle management. Identifying accounts is supported through the auto discovery function. Automatic discovery and provisioning of accounts ensures that even accounts hidden in services, scheduled tasks, application pools or local administrator

[1] Explanations of NIST SP 800-53 Rev. 4 recommendations are provided as general summary information only; federal agencies should refer to the complete text provided in the publication for the comprehensive control guidelines.

groups are discovered and managed securely according to organizational policy.

All account information is held within Cyber-Ark's patented digital vault. Assigning account managers is facilitated by the use of "safes" within the vault; group managers are provided with restricted access to account information for their particular workgroup. For establishing conditions for group or role membership, organizations can leverage the group structure already created in their LDAP database such as Active Directory. Granular account control for privileged identities is provided; in addition to group and role membership, additional privileges and attributes can be specified for individual accounts.

Through LDAP integration, any account changes – including creation, modification or removal – is automatically propagated to the account information held in the vault. Organizations can set up alerts for when users are transferred or terminated. All usage of privileged accounts is authorized and monitored. For example, before using their account, users must log in; all major authentication methods are supported including multi-factor. Further, "Dual Control" requires that an additional authorized user approve requested actions before being granted. All privileged access is recorded and audit logs protected in tamper-proof storage. Organizations can also do real-time monitoring of privileged sessions.

Reviewing accounts for compliance with account management requirements is securely enabled by allowing auditors to log in and access audit logs and usage reports, etc. without giving them access to account credentials. Cyber-Ark solutions also handle the requirement to reissue shared/group account credentials when individuals are removed from the group. The account administrator can be automatically notified

		when an individual is removed from a group in LDAP and immediately change the shared/group password or the system can be set up to issue a one-time password so that every time an account is used, the password is reissued. This control has many control enhancements all of which can be addressed by Cyber-Ark solutions for managing privileged accounts including: • Automated system account management • Removal of temporary/emergency accounts • Disable inactive accounts • Automated audit actions • Role-based schemes • Restrictions on use of shared/group accounts • Shared/group account credential termination • Usage conditions • Account monitoring/atypical usage • Disable accounts for high-risk individuals
AC-3	ACCESS ENFORCEMENT Deals with enforcing approved authorizations for logical access to information and system resources in accordance with policies.	Cyber-Ark's policy-based solutions help automatically enforce privileged access rights such that only authorized privileged users or applications can gain logical access to the information or system resources they are entitled to access. Many of the control enhancements can be supported by Cyber-Ark solutions such as: • Dual authorization • Mandatory access control • Discretionary access control • Security-relevant information • Role-based access control • Revocation of access authorizations
AC-5	SEPARATION OF DUTIES Involves defining the separation of duties of individuals and ensuring access authorizations support defined separation of duties.	The patented digital vault technology inherently supports separation of duties, allowing users to access only information that is relevant to them (files, privileged credentials etc.). The Vault is divided into safes that are accessed by users based on

		their specific permissions and without knowledge of the existence of other safes.
AC-6	LEAST PRIVILEGE Covers the concept of least privilege, which allows only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks.	With Cyber-Ark's solutions, organizations can restrict users and applications to only the necessary privileged access required to perform their assigned tasks, based on pre-defined policies. Workflows such as dual approval of password usage, email notifications and ticketing system integration for ticket validation and reasoning are just some of the many workflows that can be implemented to support least privilege. Many of the control enhancements can be addressed by Cyber-Ark solutions including: • Authorize access to security functions • Network access to privileged commands • Separate processing domains • Privileged accounts • Privileged access by non-organizational users • Review of user privileges • Privilege levels for code execution • Auditing use of privileged functions • Prohibit non-privileged users from executing privileged functions
AC-7 AC-8 AC-9 AC-10 AC-11	UNSUCCESSFUL LOGIN ATTEMPTS SYSTEM USE NOTIFICATION PREVIOUS LOGON (ACCESS) NOTIFICATION CONCURRENT SESSION CONTROL SESSION LOCK SECURITY ATTRIBUTES Deals with limiting the number of invalid logon attempts, displaying notifications before granting access, notifying user of date/time of last access,	Cyber-Ark's solutions support implementation of the following controls for the use of privileged accounts and access to sensitive documents within the Vault: • Unsuccessful Logon Attempts • System Use Notification • Previous Logon (Access Notification) • Concurrent Session Control • Session Lock • Security Attributes

AC-16	restricting the number of concurrent sessions, locking session after inactivity, and associating security attributes with information.	
AC-17 AC-18	REMOTE ACCESS WIRELESS ACCESS Call for establishing usage restrictions and authorizations for remote and wireless access.	Cyber-Ark's solutions enable secure remote access through a web portal or wirelessly from a mobile device – privileged users can access their privileged accounts to retrieve privileged credentials as well as request or approve workflows. Organizations can isolate and protect critical IT assets from potential endpoint malware and avoid exposing privileged credentials, for example to external or outsourced vendors.
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS Ensures terms and conditions are established for allowing authorized individuals to access external information systems or to process, store or transmit organization-controlled information using external information systems.	Cyber-Ark provides a central platform for secure file transfers between organizations.
AC-21	INFORMATION SHARING Applies to sharing information that is restricted in some manner (i.e. sensitive information) and is intended to facilitate information sharing in particular circumstances, including employing automated mechanisms to assist in making information sharing decisions.	To facilitate sharing of sensitive information with an organization's business partners, suppliers and subcontractors, Cyber-Ark provides a single platform enabling ad-hoc, manual or automated file transfer. The platform isolates sensitive data sent over the internet allowing organizations to securely and efficiently exchange sensitive information. The solution is available as an on-premise solution or as a cloud delivery model. Cyber-Ark's platform can help organizations to implement the control enhancements: • Automated decision support • Information search and retrieval
AC-24	ACCESS CONTROL	With Cyber-Ark's solutions, for each access

	DECISIONS Relates to establishing procedures for ensuring access control decisions are applied to each access request prior to access enforcement	request, the user is uniquely identified and their authorizations are validated (such as group membership in an LDAP directory) prior to granting access.
Family: IDENTIFICATION AND AUTHENTICATION		
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Covers development of an identification and authentication policy as well as procedures to facilitate implementation of policy and associated controls.	Cyber-Ark solutions help organizations to consistently implement identification and authentication policy and procedures and to effectively implement automated controls for privileged identities.
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Ensures that the information system **uniquely** identifies and authenticates organizational users (or processes acting on behalf of organizational users).	With Cyber-Ark solutions, every privileged user is uniquely identified in the system. The use of shared accounts is no longer anonymous and instead each individual privileged user is uniquely identified. Shared accounts such as Windows Administrator, UNIX root, an Oracle SYS account or Cisco Enable user are controlled by pre-defined granular access control. Cyber-Ark's solutions fully address the challenges of hard-coded, embedded credentials in applications, scripts or configuration files, and allow these highly sensitive identifiers to be centrally stored, audited and managed. Many of the control enhancements are directly applicable to the functionality of Cyber-Ark solutions including: • Network access to privileged accounts • Local access to privileged accounts • Group authentication • Network access to privileged accounts - separate device • Network access to privileged accounts - replay resistant • Acceptance of PIV credentials

IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION Requires the unique identification and authentication of devices before establishing a connection.	All of Cyber-Ark's products use highly secure, cryptographic methods for establishing connections between components and storing or transmitting information and are FIPS 140-2 compliant. For example, every connection to the digital vault, where all of the privileged account information is securely stored, has to be authenticated. It uses a strong two-way challenge and response authentication protocol (SRP). Cyber-Ark's solutions use unique secure application authentication methods for applications requesting credentials. This includes enforcing limitations like machine address, OS user, application path and run-time signature. Control enhancements supported by Cyber-Ark's solutions include: • Cryptographic bidirectional authentication • Dynamic address allocation • Device attestation
IA-4	IDENTIFIER MANAGEMENT Requires organization to manage information system identifiers.	Common device identifiers mentioned include MAC, IP addresses, or device-unique tokens. Cyber-Ark's solutions support authentication using passwords, RSA SecurID tokens, RADIUS, USB tokens (e.g. Aladdin's) or PKI digital certificates. Further, connections to the digital vault can be restricted by IP address.
IA-5	Authenticator Management Covers management of information system authenticators such as passwords and other types of authenticators.	Cyber-Ark's solutions support a variety of authentication methods for end users to access the digital vault, including: passwords, PKI, RADIUS, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions. The solutions provide automated privileged password management, including automatically changing passwords based on an organizationally-defined time-frame or when membership in a group changes. Complete lifecycle management for privileged account passwords helps organizations meet the full-range of requirements including

		ensuring password strength, defining their lifetime, updating them, and managing their revocation. Passwords are stored using the digital vault technology, which protects them from unauthorized disclosure and modification. And all passwords are also protected with strong encryption both in transit and at rest. For application passwords, Cyber-Ark solutions eliminate hard-coded, clear-text passwords and ensure periodic password refresh with no system downtime. The solutions provide enhanced secure authentication and a secure cache mechanism in the event of a network outage. Many of the control enhancements are supported including: • Password-based authentication • PKI-based authentication • Automated support for password strength determination • Protection of authenticators • No embedded unencrypted static authenticators • Hardware token-based authentication
IA-6	AUTHENTICATOR FEEDBACK Ensures information system obscures feedback of authentication information during authentication process	With Cyber-Ark's solutions, authentication information is obscured, for example by displaying asterisks when users input passwords.
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION Requires implementation of mechanisms for authentication to a cryptographic module that meets requirements of applicable federal laws, regulations, and standards, etc.	All of Cyber-Ark's products are FIPS-140-2 compliant.
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-	Cyber-Ark solutions uniquely identify any third-parties (e.g. contractors) provided with a

	ORGANIZATIONAL USERS) Ensures that the information system **uniquely** identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	privileged account and provide the ability to grant access without revealing any privileged passwords. Further, non-organizational users who remotely connect to the digital vault connect through a proxy so their session is encrypted and isolated from the internal network, mitigating third-party risks.
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION Ensures that organizations identify and authenticate services using security safeguards.	For authenticating services, the digital vault technology, is ICSA validated and designed to meet the highest security, audit and compliance requirements for managing App2App accounts. Cyber-Ark delivers a complete infrastructure to centralize the management of credentials to resources with a comprehensive set of abilities for managing service accounts.
IA-11	RE-AUTHENTICATION Requires users and devices to re-authenticate when requesting access under pre-defined circumstances.	With Cyber-Ark solutions, organizations can require re-authentication for privileged users or applications based on time-frames or when users request to initiate additional sessions.

Family: AUDIT AND ACCOUNTABILITY

Covers controls related to generating, protecting and reviewing audit records and ensuring accountability.

AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	Cyber-Ark's solutions enable organizations to effectively implement automated controls for generating, protecting and reviewing audit records. All privileged users and applications are uniquely identified and their activities logged ensuring full accountability for individuals regarding privileged actions and access to sensitive information. With Cyber-Ark's solutions, over 150 different types of audit events can be recorded. Some examples include: •Update Owner – tracks top-level ownership and administration over specific items in the vault •Add Group Member – tracks when users are added to groups which helps determine if a new member inadvertently gains over-wide access •Report Run – tracks when reports are run which is useful for proving that auditors were supplied with specific reports with a timestamp •CPM Reconcile Password – tracks when password changes were made outside of the vault which can detect potential malicious activity •Retrieve Password – tracks every time a user or application accesses a password in the vault Ensuring individual accountability is specifically addressed in the control, "AU-3 Content of Audit Records," which lists the required data for each audit record including the type of event and the identity of any individual associated with the event. This can be especially difficult for shared administrative accounts which typically log the use of the account without associating the use with an individual. Cyber-Ark's solutions track all
AU-2	AUDIT EVENTS	
AU-3	CONTENT OF AUDIT RECORDS	
AU-4	AUDIT STORAGE CAPACITY	
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	

AU-7	AUDIT REDUCTION AND REPORT GENERATION	administrative actions by individual users.
		
		Content of event logs can be configured to include information on user identifiers, event descriptions, success/fail indicators and more. Cyber-Ark's team can support the organization in identifying the important events and configuring the audit.
		
		When it comes to tracking privileged activity and access to sensitive information, Cyber-Ark's solutions help organizations to meet the full set of requirements of the audit control family based on extensive audit capabilities such as:
		• Records individual user identities for full accountability
		• Supports any audit storage size
		• Alerts on failures through the Notification Engine
		• Filters audit records by various parameters
		• Provides a complete range of built-in audit reports
		  ○ Examples: reports on entitlements, activity logs, provisioning/ deprovisioning and more
		• Delivers session recording for forensic analysis
		• Integrates with SIEM and event log systems including HP ArcSight, McAfee ESM, IBM/QRadar and RSA enVision for complete correlational analysis
		  ○ Support for Syslog and XSL schema
		• Time-stamps all logs synchronized to the vault clock
		  ○ NTP can be enabled if required
		• Protects audit information with cryptographic storage in a tamper-proof vault
		  ○ FIPS 140-2 certified
		• Supports any retention period as set by the organization
		• Can generate alerts on specific occurrences

AU-8	TIME STAMPS	
AU-9	PROTECTION OF AUDIT INFORMATION	
AU-10	NON-REPUDIATION	
AU-11	AUDIT RECORD RETENTION	
AU-12	AUDIT GENERATION	
AU-14	SESSION AUDIT	
AU-15	ALTERNATE AUDIT CAPABILITY	

Family: AWARENESS AND TRAINING

Contains controls for security awareness and training for end-users and personnel with assigned security roles and responsibilities.

AT-3	ROLE-BASED SECURITY TRAINING	Cyber-Ark provides comprehensive training courses — ranging from privileged account administration to applications development and can create specific programs to meet the unique needs of an organization.

Family: SECURITY ASSESSMENTS AND AUTHORIZATION

Includes controls for assessing and authorizing security controls including authorizing connections within and between systems and ensuring on-going assessments.

CA-3	SYSTEM INTERCONNECTIONS	Cyber-Ark's solutions support the authorization of system interconnections and internal system connections by providing secure control over connections of various applications throughout the infrastructure. For continuous monitoring, Cyber-Ark's solutions monitor privileged access and provide audit logs in real-time to SIEM solutions as well as security data analytics systems. Real-time monitoring of privileged sessions is also supported, providing details of all activity throughout a session and the ability to terminate a session.
CA-7	CONTINOUS MONITORING	
CA-9	INTERNAL SYSTEM CONNECTIONS	

Family: CONFIGURATION MANAGEMENT

Covers controls for managing the configuration of information systems.

CM-2	BASELINE CONFIGURATION	Configuration management ensures that critical assets including operating systems, servers, databases, virtual machines, applications, firewalls, security systems, network devices, routers, etc. are properly configured at all times. The ability to make configuration changes must be restricted to authorized privileged users. Cyber-Ark's solutions help maintain baseline configurations and support the implementation of oversight of configuration change control by ensuring that only authorized users can gain access to system configurations. All access is monitored and records retained. Organizations can effectively enforce access restrictions for change as required by organizational policy by controlling access to administrative passwords. "Dual Control" can specify that access to highly sensitive passwords or policies requires confirmation by one or more authorized users. As well, Cyber-Ark's solutions provide an audit record of which individual privileged users use administrative passwords to make configuration changes. Organizations can also monitor and record privileged sessions involving changes to configuration settings. Session approval workflows and DVR playback of recordings for review and analysis can be implemented. Cyber-Ark's solutions can control what privileged and elevated commands a user can access based on the "least privilege" principle.
CM-3	CONFIGURATION CHANGE CONTROL	
CM-5	ACCESS RESTRICTIONS FOR CHANGE	
CM-6	CONFIGURATION SETTINGS	
CM-7	LEAST FUNCTIONALITY	

Family: CONTINGENCY PLANNING

Covers controls involved with contingency planning.

CP-9	INFORMATION SYSTEM BACKUP	All Cyber-Ark products offer high availability, full disaster recovery capabilities and backup. Privileged credentials are always accessible and available for the requesting systems, even in network outages. Password versioning and reconciliation capabilities further enhance the criticality of being able to access systems with privileged credentials, based on enterprise policy. For sensitive information management, Cyber-Ark's platform helps to ensure that information is never lost, always protected and transmissions are always automatically resumed. The Vault can also be rebuilt based on guidelines.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	

Family: INCIDENT RESPONSE

Contains controls related to a comprehensive incident response program.

IR-5	INCIDENT MONITORING	Cyber-Ark's solutions provide the necessary logs and notifications for effective incident monitoring and reporting, including sending alerts through the Notification Engine and connecting to an SIEM, from vendors including HP ArcSight, McAfee ESM and RSA enVision.
IR-6	INCIDENT REPORTING	

Family: MAINTENANCE

Includes controls regarding information system maintenance.

MA-2	CONTROLLED MAINTENANCE	For maintenance, Cyber-Ark provides the ideal platform from which to securely provide external parties with access to key systems in closely monitored and controlled environments. Organizations can record and store every privileged session in the tamper-proof digital vault for 24/7 video surveillance of sensitive systems.
MA-4	NON-LOCAL MAINTENANCE	

Family: PLANNING

Covers controls for security planning.

PL-8	INFORMATION SECURITY ARCHITECTURE	Cyber-Ark's professional services consulting team includes top subject matter experts who can help organizations to architect secure and efficient solutions for managing and controlling privileged access and access to sensitive documents. The core functionality of Cyber-Ark's solutions includes centralized management of privileged identities and access to sensitive information.
PL-9	CENTRAL MANAGEMENT	

Family: PERSONNEL SECURITY

Contains controls related to personnel security.

PS-4	PERSONNEL TERMINATION	With Cyber-Ark's solutions, organizations can ensure that for privileged users, upon termination of individual employment, their access to privileged passwords is immediately disabled. All changes in the organization's

PS-5	PERSONNEL TRANSFER	LDAP directory (e.g. Active Directory) are immediately propagated to the digital vault. For personnel transfers, all modifications to an individual's access authorizations are also immediately propagated to the Vault. Further, organizations can proactively set up the use of one-time passwords which would ensure terminated or transferred users could not use previously issued passwords.

Family: RISK ASSESSMENT

Includes controls regarding risk assessment.

RA-5	VULNERABILITY SCANNING	Cyber-Ark's solutions help to protect the integrity of vulnerability scanning systems by ensuring that only those with authorized privileged credentials can gain access to these systems. As well, a detailed log is kept so that organizations will have a complete record of scan requests. Cyber-Ark integrates with leading vendors such as McAfee Vulnerability Manager, Qualys, and nCircle to enable deep, authenticated scans while continuing to protect the privileged credential needed to scan IT systems.

Family: SYSTEM AND SERVICES ACQUISITION

Contains controls for system and services acquisition.

SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	Cyber-Ark helps implement controls for system and services acquisition. The company fully supports its customers and enables complete life-cycle management of the product suites. Specifically: • All of the products come fully documented. • Cyber-Ark's products are highly acclaimed for their security engineering, including
SA-4	ACQUISITION PROCESS	
SA-5	INFORMATION SYSTEM DOCUMENTATION	
	SECURITY ENGINEERING	

SA-8	PRINCIPLES	layered protection, security architecture, security training for developers and much more. • The company provides configuration management, change tracking, and security updates. • The products have all been internally and field-tested and extensively used by hundreds of large customers, providing the highest security assurance. • Cyber-Ark has a 95% maintenance renewal rate. • To help ensure proper implementation and usage of the product suites, Cyber-Ark provides comprehensive training for users and administrators and offers additional support through professional services. • Cyber-Ark's products are validated d by ICSA Labs and FIPS 140-2 compliant. • Cyber-Ark's can provide customized development professional services.
SA-9	EXTERNAL INFORMATION SYSTEMS SERVICES	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	
SA-12	SUPPLY CHAIN PROTECTION	
SA-13	TRUSTWORTHINESS	
SA-16	DEVELOPER-PROVIDED TRAINING	
SA-18	TAMPER-RESISTANCE AND DETECTION	
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	

Family: SYSTEM AND COMMUNICATIONS PROTECTION

Includes controls regarding system and communications protection

SC-2	APPLICATION PARTITIONING	Cyber-Ark successfully addresses a wide-range of the requirements for system and communications protection, including transmission, architecture, cryptographic procedures and functions. Specifically, Cyber-Ark's solutions: • Separate the main Vault component from other components, isolating the main security function and ensuring application partitioning • Enable system components to reside on the internal network, helping to ensure protection from DoS attacks • Can block access to system components based on subnet or IP address • Ensure session authenticity by SSL verification between the main interface (PVWA) and the Vault and through use of the proprietary secure protocol (Vault
SC-3	SECURITY FUNCTION ISOLATION	
SC-5	DENIAL OF SERVICE PROTECTION	
SC-7	BOUNDARY PROTECTION	
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	
SC-10	NETWORK DISCONNECT	
SC-11	TRUSTED PATH	
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	

SC-13	CRYPTOGRAPHIC PROTECTION	Protocol)
		• Use FIPS 140-2 validated cryptography
		• Save database states and preserve consistency
		• Have been architected with the use of thin nodes, enhancing the overall security
		• Protect all information at rest with encryption in the Vault
		  ○ Encryption algorithms supported include AES-256, RSA-2048
		  ○ HSM integration
		• Support heterogeneous environments
		  ○ Integrate with the full-range of operating systems, applications, databases, security appliances, network devices, directories, virtual environments and storage
		• Are designed to run in virtualized environments enabling the use of virtualized techniques for concealment and misdirection
		• Enable information system partitioning; components can be set up to reside at diverse geographic locations
		• Employ hardware-based protection to ensure non-modifiable executable programs
		• Support distributed architecture
		• Facilitate process isolation through the use of "safes" within the vault, each safe is assigned a separate address space

SC-23	SESSION AUTHENTICITY	
SC-24	FAIL IN KNOWN STATE	
SC-25	THIN NODES	
SC-28	PROTECTION OF INFORMATION AT REST	
SC-29	HETEROGENEITY	
SC-30	CONCEALMENT AND MISDIRECTION	
SC-32	INFORMATION SYSTEM PARTITIONING	
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	
SC-36	DISTRIBUTED PROCESSING AND STORAGE	
SC-39	PROCESS ISOLATION	

Family: SYSTEM AND INFORMATION INTEGRITY

Includes controls related to system and information integrity.

SI-3	MALICIOUS CODE PROTECTION	Cyber-Ark helps organizations meet the requirements for system and information integrity through an internal components check. Cyber-Ark's Vault checks the internal Firewall, as well as the crypto functionality and other security functions. In case of failure, the system will stop its operation to ensure security and integrity. The Notification Engine enables error handling. All system information is encrypted and verified and the retention policy is configurable.
SI-4	INFORMATION SYSTEM MONITORING	
SI-6	SECURITY FUNCTION VERIFICATION	
SI-10	INFORMATION INPUT VALIDATION	
SI-11	ERROR HANDLING	
SI-12	INFORMATION HANDLING AND RETENTION	

CYBER-ARK'S SOLUTIONS OVERVIEW

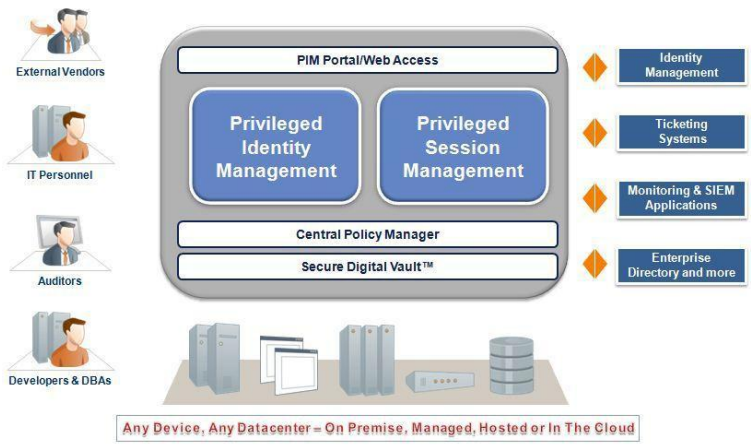
Based on Patented Digital Vault Technology

Cyber-Ark's solutions are based on unique and patented digital vault technology, which includes a FIPS 140-2 validated cryptographic module (with AES-256 encryption). Cyber-Ark's vaulting solutions create safe havens – distinct areas for storing, protecting and sharing the most critical business information. Cyber-Ark's approach is much like that of a physical vault at a bank. Regardless of the overall network "neighborhood" it is in, the Cyber-Ark vault is extremely secure.

Cyber-Ark's digital vault technology is ICSA certified and designed to meet the highest security requirements, providing numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection. At the same time, Cyber-Ark's unique approach makes information readily accessible – eliminating the traditional tradeoff between accessibility and security.

Integrated Suite for Managing and Monitoring Privileged Accounts

Cyber-Ark's Privileged Identity Management (PIM) and Privileged Session Management (PSM) suites comprise an integrated, full lifecycle solution for centrally managing privileged and shared identities, privileged sessions, as well as embedded passwords found in applications and scripts.



Privileged Identity Management (PIM) Suite

The PIM Suite is a unified policy-based solution that secures, manages and enforces policies and workflows for accessing privileged and shared accounts across the data center, whether on-premise, off-premise or in the cloud. The PIM Suite includes the following products:

- **Enterprise Password Vault® (EPV):** enables organizations to secure and manage all types of privileged accounts, creating a tamper-proof log for reporting purposes. EPV integrates with other leading security products and offers proven scalability and robustness for managing hundreds of thousands of servers, databases, network devices, virtual machines and more.

- **Application Identity Manager™ (AIM):** addresses the challenges of hard-coded, embedded credentials and encryption keys. It eliminates the need to store embedded credentials in applications, scripts or configuration files, allowing highly sensitive passwords to be centrally stored, audited and managed. Only trusted applications have access to these credentials and no downtime is experienced when replacing them. A secure local cache ensures credentials are always available, even in network outages.
- **On-Demand Privileges Manager™ (OPM):** is a unified solution for managing and monitoring superusers and privileged accounts. Usage of accounts such as 'root' users on UNIX is no longer anonymous and can now be controlled by pre-defined granular access control, where both the command itself and the output are recorded. OPV also dramatically improves productivity and security in Windows environments by implementing a 'least privilege' policy on desktops and servers.

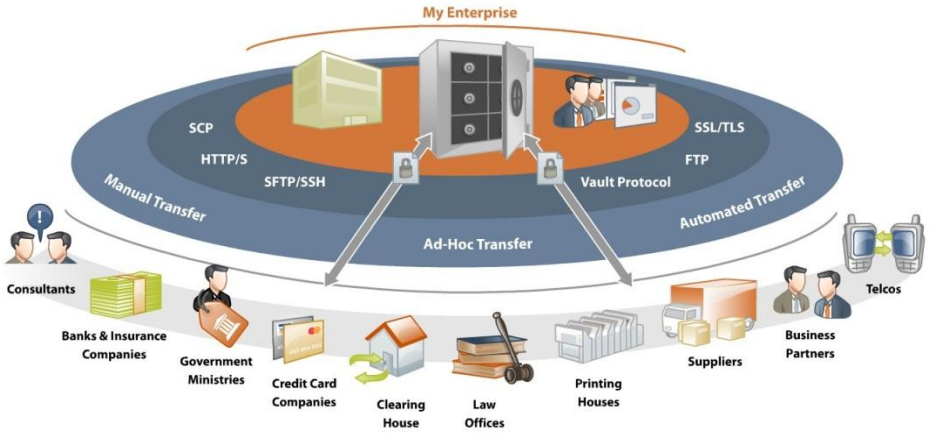
Privileged Session Management (PSM) Suite

To complement Cyber-Ark's PIM Suite, the PSM Suite proactively protects privileged sessions, especially remote or third party access. It provides a central point of control for protecting systems accessed by privileged users and accounts, allowing organizations to isolate, control and monitor all privileged activity across the data center. This includes isolating and protecting critical IT assets from potential endpoint malware, mitigating the risk of exposing privileged credentials.

With the PSM suite, organizations gain full visibility of privileged activity. Real-time monitoring helps detect any malicious, command-level activity and includes the ability to intervene with and terminate a privileged session. The PSM suite also enables root-cause analysis for rapid remediation and provides video recorded session playbacks to be used as evidence in audits and reviews.

Sensitive Information Management (SIM) Suite

The SIM is a secure repository platform for managing, sharing, and protecting critical information across the enterprise and when transferring it outside the enterprise. The SIM suite ensures that only authorized personnel can access sensitive files and prevents IT or other unauthorized personnel from opening them. The SIM suite includes:



- **Sensitive Document Vault:** provides a highly secure central storage with granular access control, segregation of duties and extensive monitoring capabilities for storing and sharing files.
- **Inter-Business Vault® (IBV)**: isolates sensitive data sent over the internet allowing organizations to securely and efficiently exchange sensitive information with business partners, suppliers and subcontractors using ad-hoc, manual or automated file transfer on a single platform. The Inter-Business Vault® solution is available as an on-premise solution or as a cloud delivery model.

CONCLUSION

Federal agencies are required by law to comply with the Federal Information Security Management Act (FISMA), which references the NIST SP 800-53 Recommendations. The long-awaited Revision 4 represents the first major review of the Recommendations in almost four years. These changes have important ramifications for agencies that need to be FISMA compliant.

A primary driver for updating the NIST Recommendations was to help organizations confront advanced persistent threats (APTs). Many controls and control enhancements were added to address APTs, including increased requirements for securing privileged accounts.

Privileged accounts are specifically targeted by APTs because they enable broad access to critical assets. When a privileged account is compromised, the attacker has the power to gain access to a vast amount of data, and their activity can be extremely hard to detect. The release of Revision 4 will prompt many agencies to focus on improving the security of privileged accounts.

Cyber-Ark's solutions can help agencies to effectively and efficiently meet the full range of requirements regarding privileged accounts. The solutions are enterprise-proven in large and mid-sized government and commercial organizations. Cyber-Ark is the trusted expert in privileged account security and compliance.