CYBER SECURITY STANDARD

Standard Identifier:	CSS2018-001
Standard Name:	Remote Access Authentication
Version:	DRAFT Version 1.0
Cyber Security Framework Alignment:	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. *Mapped to: NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20*
Strategic Alignment:	☐ Cyber Risk ☐ Cyber Outreach ☒ Cyber Protection ☐ Cyber Operations
Standard Summary:	Require multifactor authentication for remote access to State technology resources.
Standard Details:	Advanced or multifactor authentication is required for all remote access originating from outside the State's networks. This requirement includes both users and administrators, as well as third-party access for support or maintenance. This standard is limited to individual users or host-based access and does not include site-to-site VPN connections.
Exceptions Procedure:	Exception requests will be processed through CSO@WV.GOV and provided to the appropriate approval authority for consideration. All requests must include • Reason for exemption • Identity of user/host/system(s) being exempted • Length of exemption needed (determined by reason) • Type of data being accessed • Network and/or system being accessed
Attachment:	NIST 800-53 AC 17, 19, 20

AC-17

Remote Access

The organization: Documents allowed methods of remote access to the information system; Establishes usage restrictions and implementation guidance for each allowed remote access method; Monitors for unauthorized remote access to the information system; Authorizes remote access to the information system prior to connection; and Enforces requirements for remote connections to the information system.

This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.

The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.

The information system routes all remote accesses through a limited number of managed access control points.

Related control: SC-7.

The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

The organization monitors for unauthorized remote connections to the information system [Assignment: organization-defined frequency], and takes appropriate action if an unauthorized connection is discovered.

The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

The organization ensures that remote sessions for accessing [Assignment: organization-defined list of security functions and security-relevant information] employ [Assignment: organization-defined additional security measures] and are audited.

Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.

The organization disables [Assignment: organization-defined networking protocols within the information system deemed to be nonsecure] except for explicitly identified components in support of specific operational requirements.

The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

AC-19

Access Control for Mobile Devices

The organization: Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; Monitors for unauthorized connections of mobile devices to organizational information systems; Enforces requirements for the connection of mobile devices to organizational information systems; Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and Applies [Assignment: organization-defined inspection and preventative measures] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

The organization restricts the use of writable, removable media in organizational information systems.

The organization prohibits the use of personally owned, removable media in organizational information systems.

The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

The organization: Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s); and Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information: \ - Connection of unclassified mobile devices to classified information systems is prohibited; - Connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s); - Use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and - Mobile devices and the information stored on those devices are subject to random reviews/inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.

AC-20

Use of External Information Systems

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: Access the information system from the external information systems; and Process, store, and/or transmit organization-controlled information using the external information systems.

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government. This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access

authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: Can verify the implementation of required security controls on the external system as specified in the organizations information security policy and security plan; or Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.