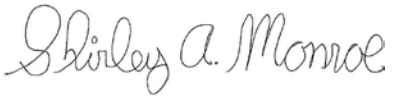
COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF HUMAN SERVICES, INSURANCE, AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Remote Access Control**	Number: **STD-ENSS035**
Domain: **Security**	Category:
Date Issued: **12/04/2013**	Issued By Direction Of:
Date Revised: **03/26/2015**	 Shirley A. Monroe, Dir of Division of Technical Engineering

Abstract:

The purpose of this standard is to describe the department's remote access requirements to state and federal agencies.

DHS organization employs Virtual Private Networks (VPNs) and dedicated direct access to allow remote user access to DHS's internal network. VPN services are generally accessible through internet using encrypted tunnels to enhance confidentiality and integrity over remote connections. Remote access controls apply to information systems other than public web servers or systems designed for public access. While using remote connections, comprehensive security requirements are needed to protect DHS information resources. Some of the key activities to be performed to improve remote access security include:

- Authentication
- Authorization
- Encryption
- Audit Logging and Monitoring

Separate logical and physical segments are designed to ensure security requirements are met between these network services.

General:

This Standard addresses how remote access to DHS information and information systems is controlled; including the identification, authorization and authentication of users, programs and processes that access DHS information resources through various type of remote connections (e.g., VPN, Dial-in). This standard also addresses compliance with DHS, federal and Commonwealth of Pennsylvania (COPA) requirements.

Standard:

Authentication:

Remote access to DHS IT infrastructure should implement, at a minimum, the following authentication procedures:

- Multi-factor authentication (e.g., “soft” cryptographic tokens, “hard” cryptographic tokens, SSL Certificates using PKIs and domain passwords)
- Encrypted and shared cryptographic keys (e.g., 3DES with IPsec) shall be established for gateway-to-gateway and client-to-gateway VPN sessions
- Authentication credentials shall be passed in an encrypted format
- Authentication credentials shall be at rest in an encrypted format
- Use of a Completely Automated Public Turing test (CAPTCHA) type solutions to determine whether or not the user is human and prevent automation of user authentication
- Maintain a session expiration of 15 minutes.

The authentication for remote access passwords shall not traverse the network in clear text and must meet minimum password strength requirements, as documented in approved security policies, procedures and standards, provided in the CoPA Detailed Windows Password Policy, RFD-SEC007A.

Authorization

Prior to connection, system owners shall enforce requirements to authorize remote access to the DHS Information System:

- Users who remotely access DHS internal network or system shall be uniquely identifiable and would be authorized with pre-approved access based on their job functions.
- Periodic review of remote system account shall be performed following guidance provided in the User Identity and Access Management Policy (POL-SEC012).
- DHS organization shall authorize the execution of privileged commands and access to security-relevant information via remote access only for administrative accounts.
- Rationale for privileged commands remotely executed shall be documented.
- DHS shall perform a quarterly review of unauthorized remote connections to the information system

In addition, rules set shall be required for remote access systems such that only authorized parties can access authorized segments and ports of the DHS internal network as outlined in the Network Security Policy (POL SEC007).

Encryption

DHS information system shall implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Remote access solution shall use the guidance provided by the DHS’s Cryptography Policy (POL-SEC002) for data at rest and in motion.

Audit Logging and Monitoring

DHS information system administrators, with input from logging and monitoring administrators shall enable logging and audit capabilities (e.g., sign-on, activity, connections) and disable the ability to automate authentication on the client server for remote access, including remote administration.

DHS information resources shall meet the following minimum requirements to avoid security incidents and effectively log and monitor remote access activities:

- Audit logs of remote access activities shall be maintained and reviewed periodically for after-the-fact investigations as outlined in the Security Audit Logging Policy (POL-SEC009).

- DHS information system administrators shall have authorization to enable/disable audit logging capabilities
- Audit logs shall be integrated with DHS SIEM solutions when applicable.
- Automated monitoring and control of remote access sessions shall be in place to detect unauthorized attempts and ensure ongoing compliance by auditing remote user's connection activities.
- Security related activities on critical devices shall be logged, supporting the remote access environment (e.g., VPN servers, routers, firewalls)
- A centralized reporting solution, such as syslog, shall be used for capturing related audit logs. (refer to the Audit Log Review Standard for additional details)
- Use of IDSs for protecting VPN access points shall be considered (IDS shall be placed behind the VPN termination point).

Exemption from This Standard:

Any exemption to comply with this standard should be discussed with the Department's Chief Information Security Officer (CISO).

Refresh Schedule:

All standards and referenced documents identified in this standard will be subject to periodic review and possible revision annually or upon request by the DHS Information Technology Standards Team.

References:

1. ITB-PRV001: Commonwealth of Pennsylvania Electronic Information Privacy Policy
2. ITB-SEC010: Virtual Private Network Standards
3. POL-SEC002: Cryptography Policy
4. POL-SEC007: Network Security Policy
5. POL-SEC009: Security Audit Logging Policy
6. POL-SEC012: User Identity and Access Management Policy
7. NIST SP800-124: Guidelines for managing and Securing Mobile Devices in the Enterprise

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
07/18/2013	1.0	Initial draft	Mathieu Saury
12/04/2013	1.0	Sign-Off	Robert Myers
03/26/2015	1.1	Reviewed for accuracy per policy, made cosmetic changes (DPW to DHS)	Pamela Skelton