

INFORMATION TECHNOLOGY SECURITY POLICY

2400.25

5.0 TECHNICAL POLICIES

5.1 Identification and Authentication

Authentication is the process of establishing confidence in user identities electronically presented to an information system. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual. Authentication focuses on confirming an individual's identity, based on the reliability of the individual's credentials.

Authentication of user identities is accomplished using passwords, tokens, PKI certificates, key cards, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and its attendant SP 800-73 and SP 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication. When information systems are accessed through local interfaces and contained within a controlled environment with physical access controls, the risk of using passwords as opposed to other forms of authentication, are somewhat mitigated. Thus, passwords that meet NIST SP 800-63 level 2 password requirements used locally in an environment with adequate physical access controls can be used in FIPS 199/SP 800-53 moderate-impact systems.

HUD Policy

- a. Program Offices/System Owners shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support access control, least privilege, and system integrity in accordance with FIPS 201, Personal Identity Verification for Federal Employees and Contractors. For high-impact systems, the system shall employ multifactor authentication mechanisms.
- b. HUD users shall not share identification or authentication materials of any kind; nor shall any HUD user allow any other person to operate any HUD system by employing the user's identity.
- c. All user authentication materials shall be treated as sensitive material and shall carry a level of sensitivity as high as the most sensitive data to which that user is granted access using that authenticator.
- d. The system ISSO shall ensure that USERIDs are disabled after a period of inactivity of no more than 90 days. For systems rated moderate to high, the system shall do this automatically.
- e. Program Offices/System Owners shall ensure that user access is reviewed once a year.

5.1.1 E-Authentication

To successfully implement a government service electronically (or e-government), federal agencies must determine the required level of assurance in the authentication for each transaction. This is

accomplished through a risk assessment for each transaction.

The OMB has defined four levels of assurance in terms of the consequences for authentication errors and misuse of credentials. NIST has published technical guidance for federal agencies to support the ability of individuals to remotely authenticate to a federal system at different assurance levels.

HUD Policy

- a. Program Offices/System Owners of IT systems that require authentication controls over the Internet between outside parties and HUD, the IT system shall utilize authentication mechanisms in accordance with NIST SP 800-63, Electronic Authentication Guide.
- b. Program Offices/System Owners shall at a minimum comply with the following authentication requirements depending on system sensitivity in accordance with NIST SP 800-63: Low-impact systems must comply with the requirements for level 1 authentication systems Moderate-impact systems must comply with the requirements for level 2 authentication systems High-impact systems must comply with the requirements for level 3 authentication systems

5.1.2 Device and Application Authentication

Multi-tier systems can use middle- and back-end systems to connect to legacy systems and databases. In certain situations, this connection takes place using a generic ID and password that may contain full system privileges. Compromise of these IDs/Passwords can result in system misuse.

Networks that do not use device authentication are open to intrusions by attackers who have access to their physical location. Shared media networks and dynamic protocols, like Dynamic Host Configuration Protocol (DHCP), are susceptible to attacks from anyone with physical access to a network connection (e.g., network wall outlet). The attacker can plug in the device and start using it to capture packets of data or to start scanning the network for vulnerable systems. To ensure that only approved devices can connect to the network and that approved applications can connect to back-end systems, the authenticators need to be protected from unauthorized disclosure and use.

The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses), an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP]), or a Radius server with EAP-Transport Layer Security (TLS) authentication to identify and authenticate devices on local and/or wide area networks (WAN).

HUD Policy

- a. Program Offices/System Owners must use an IT Security Office-approved procedure, mechanism, or protocol to secure authenticators used for application, host, or device authentication.

5.1.3 Passwords

A password is a secret that a claimant memorizes and uses to authenticate the claimant's identity. Passwords are typically character strings.

Strong passwords have a minimum of eight alphanumeric characters with at least one uppercase letter, one lowercase letter, one digit, and one special character. Strong passwords do not have common words or permutations of the user name.

HUD Policy

- a. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.
- b. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce the appropriate frequency for changing passwords; but in no case shall the frequency be less often than every 90 days.
- c. Users shall not share personal passwords.
- d. Users shall select strong passwords and not reuse old passwords.
- e. Use of group passwords shall be limited to situations dictated by operational necessity or those critical for mission accomplishment. Use of a group USERID and password must be approved by the appropriate Authorizing Official.
- f. In those systems where user identity is authenticated by password, the system shall ensure that users cannot reuse a password for at least eight iterations.
- g. In those systems where user identity is authenticated by password, the system shall ensure that passwords are not displayed when entered.
- h. In those systems where user identity is authenticated by password, the system shall protect passwords from unauthorized disclosure and modification when stored and transmitted.
- i. System administrators shall replace all default passwords provided by the vendor.
- j. In those systems where user identity is authenticated by password, the system ISSO shall develop and implement administrative procedures for initial password distribution, for lost/compromised passwords, and for revoking passwords.

The use of a password by more than one individual is discouraged throughout HUD; however, it is recognized that in certain circumstances (e.g., operation of crisis management or operations centers, watch teams, and other duty personnel) may require the use of group USERIDs and passwords.

5.2 Access Control

Users are responsible for protecting all HUD information to which they are granted access. Access controls restrict access to system objects, such as files, directories, and devices based upon the identity of the user or the group to which the user belongs. The purpose of access controls is to protect against the unauthorized disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. Automated systems are vulnerable to fraudulent or malicious activity by individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual acting alone from engaging in such fraudulent or malicious behavior. The Principle of Least Privilege states that a user should only be able to access the system resources needed to fulfill the user's job responsibilities.

HUD Policy

- a. Program Offices/System Owners shall ensure that their information systems implement access control measures to provide protection from

unauthorized alteration, loss, unavailability, or disclosure of information.

b. Program Offices/System Owners shall ensure that their information systems rated moderate to high, use an automated mechanism to support management of information system accounts. For information systems rated high, the automated mechanism shall track account creation, disabling, and termination to support audit of such actions and, as required, notify appropriate individuals.

c. Program Offices/System Owners shall ensure that access control follows the principle of least privilege and separation of duties and shall require that a user use unique identifiers on a system.

d. ISSOs shall ensure that temporary and emergency accounts are properly authorized and maintained. For systems rated high, these accounts shall be automatically disabled after 48 hours.

e. ISSOs shall ensure that guest/anonymous accounts are not used.

f. Program Offices/System Owners shall identify specific user actions, which can be performed on the information system without identification and authentication. For systems rated moderate to high, actions to be performed without identification and authentication will be permitted only to the extent necessary to accomplish mission objectives.

5.2.1 Automatic Account Lockout

Program Offices/System Owners shall configure each IT system to lock any user account immediately and automatically following a specified number of consecutive failed logon attempts, in such a way that:

* As long as the account remains locked, no logon of any kind will be permitted to that account, including the user to whom the account is assigned.

* The manual intervention of an appropriate security administrator is required to unlock the account.

HUD Policy

a. Program Offices/System Owners shall ensure that their information systems implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three within a thirty-minute period.

b. Program Offices/System Owners shall ensure their information systems are configured to lock out a user account after three consecutive failed logon attempts.

5.2.2 Logon and Session Security

Program Offices/System Owners shall configure each IT system to deactivate any user session immediately and automatically following a specified period of inactivity, in such a way that will require the user to re-authenticate the user's identity before resuming interaction with the system.

Systems that provide the user at logon with information concerning the last connection and possible unsuccessful attempts provide the agency with another layer of defense by enlisting users in identifying and reporting unusual activity.

Highly sensitive systems should limit the number of sessions that a user can have active to prevent possible unauthorized disclosure, modification, and/or destruction of sensitive information.

HUD Policy

a. Program Offices/System Owners of systems that have been rated moderate or high shall ensure their systems time out user sessions after ten minutes of inactivity.

b. For systems rated high, the Program Offices/System Owners shall ensure that the system does not allow concurrent sessions.

5.2.3 Warning Banner

Successful prosecution of unauthorized access to HUD systems requires that users be notified prior to their entry into the systems that the data in the system is owned by HUD and that activities on the system are subject to monitoring. All multi-user computer systems will display a warning message when a user attempts to access the system, and prior to actually logging into a system, informing users that equipment is the property of the government, that the use of government property is for the conduct of government business only, and that the use of government equipment is subject to monitoring. Privacy Laws have explicit requirements to notify users about HUD's privacy policy prior to granting access to a system.

HUD Policy

- a. The CISO shall provide a standard notification message for HUD systems that warns unauthorized users that they have accessed a U.S. Government system and can be punished. The wording shall also warn authorized users that they are subject to monitoring and recording and that use of the system indicates consent to such monitoring and recording.
- b. IT systems internal to the HUD network shall display a warning banner stipulated by the HUD CISO and the Privacy Officer, when applicable. The warning banner shall require users to click through, indicating acknowledgment, prior to granting access to the system.
- c. IT systems accessible to the public shall provide both a security and privacy statement approved by the CISO and the Privacy Officer at every entry point. The statement shall include a description of the authorized uses of the system.

5.3 Audit and Accountability

Audit trails maintain a record of system application and user activity. In conjunction with the appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and application flaws.

Audit trails may be used as support for regular system operations or as a kind of insurance policy, or both. As an insurance policy, audit trails are maintained but are not used unless needed (e.g., after a system outage or suspected compromise). As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

Audit trails help accomplish several security-related objectives, including individual accountability, event reconstruction, intrusion detection, and problem analysis.

Information systems that store or process personally identifiable information, personal health-related information, or financial information have specific audit requirements under the Privacy Act, Health Insurance Portability and Accountability Act, and the Sarbanes-Oxley Act.

HUD Policy

- a. Program Offices/System Owners shall ensure that audit trails are sufficient in detail to facilitate the reconstruction of events if a system is compromised or if a malfunction occurs or is suspected. Audit trails shall include auditable events as specified in the system security plan and be reviewed accordingly. The audit trail shall contain at least the following information:

Type of event

Identity of the user, application, and device that triggered the event

The component of the information system (e.g., software component and hardware component) where the event occurred

Time and date of the event

Outcome (success or failure) of the event

For systems rated moderate to high, the audit function shall have the capability of providing more detailed information for audit events identified by type, location, or subject. For systems rated high, the system shall provide the capability for centralized management of audit records.

b. Program Offices/System Owners shall ensure that their audit trails and audit logs are protected from unauthorized modification, access, or destruction while online and during offline storage.

c. Program Offices/System Owners shall ensure that audit logs are recorded and retained in accordance with HUD records retention policies, but in no case shall the frequency be less than once a year for systems rated moderate to high.

d. Program Offices/System Owners shall develop and implement a process to periodically review audit records for inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report findings to the appropriate officials. For systems rated moderate or high, the Program Offices/System Owners shall employ an automated mechanism to facilitate the review of audit records. Audit records related to activities of users with significant information systems roles and responsibilities shall be reviewed more frequently.

e. Program Offices/System Owners shall ensure that the system allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

f. Program Offices/System Owners shall ensure that the system alerts the appropriate officials in the event of an audit failure or when audit capacity is close to being reached.

g. Program Offices/System Owners shall make a risk-based decision on which one of the following actions the system should take in the event of an audit failure or when audit capacity is being reached:

Shutdown the system

Overwrite the oldest audit records

Stop generating audit records

h. Program Offices/System Owners of information systems that have been rated moderate or high shall that utilize audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered. Program Offices/System Owners of high-impact systems shall ensure the system provides the capability to automatically process audit records for events of interest based upon selectable, even criteria.

i. Program Offices/System Owners shall use automated mechanisms to integrate their audit procedures into HUD's incident response capability for systems rated moderate to high, which provides for centralized audit monitoring, analysis, and reporting.

j. Program Offices/System Owners shall ensure that information systems under their purview provide time stamps for use in audit record generation. The time stamps shall be generated using internal information system clocks that are synchronized system wide.

5.4 Network Security

5.4.1 Remote Access and Dial-In

Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public

access. HUD restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network [VPN] technology). HUD permits remote access for privileged functions (e.g., maintenance ports and system and device administration) only for compelling operational needs and during emergencies.

HUD Policy

- a. The Deputy CIO for IT Operations shall provide remote access mechanisms that are centrally managed, monitored, and protected by strong authentication. The mechanisms shall have the capability to provide strong cryptographic mechanisms for authentication and protection of sensitive information during transmission. For access to systems rated moderate or high, the session shall be encrypted and access shall be managed through a managed access control point.
- b. Program Offices/System Owners shall authorize and approve remote access methods for systems under their purview. The remote access methods shall only use mechanisms authorized by the Deputy CIO for IT Operations.
- c. ISSOs shall authorize in writing users requiring remote access, including remote access for privileged functions.
- d. Remote access administrators shall not add users to remote access mechanisms without written approval from the ISSO.

5.4.2 Network Security Monitoring

The increasingly important role of automated information system networks in government has fueled the need for more secure systems. Intrusion detection systems are gaining widespread recognition as important tools that improve computer network security. Although firewalls have traditionally been the first line of defense against would-be attackers, intrusion detection devices, working with firewalls, are becoming more popular for network security.

HUD Policy

- a. The CSIRC shall use automated tools and mechanisms to monitor HUD's networks for security events.
- b. The CISO, in coordination with IT Operations, shall select and implement intrusion detection and monitoring tools for HUD in accordance with NIST SP 800-31, Intrusion Detection Systems. The tools shall be part of a system-wide intrusion detection system that uses common protocols and supports near-real-time analysis of events in support of system-level attacks.
- c. The CISO, in conjunction with the Deputy CIO for IT Operations, shall select and implement vulnerability scanning tools and techniques to scan information systems for vulnerabilities every month or when significant new vulnerabilities affecting HUD's infrastructure are identified and reported on systems rated low and moderate. Systems rated high shall be scanned once a week. For high-impact systems, the tools shall include the capability to update the list of vulnerabilities scanned. The list shall be updated every six months or when significant new vulnerabilities affecting the system are identified and reported.
- d. The CISO, in conjunction with the Deputy CIO for IT Operations, shall perform annual penetration testing on network components.

5.4.3 Network Connectivity

Within HUD, boundary protection of IT resources is accomplished by the installation and operation of controlled interfaces (e.g., proxies, gateways, routers, firewall, and encrypted tunnels). Controlled interfaces, when used in concert with a variety of

additional security controls (e.g., intrusion detection systems, personnel background checks, security guards, data encryption, and physical security barriers), provide an added level of assurance that unauthorized personnel will be unable to access departmental automated systems.

By tracking and controlling data, deciding whether to pass, drop, reject, or encrypt the data, controlled interfaces have proven to be an effective means of securing a network.

HUD Policy

- a. The Deputy CIO for IT Operations shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
- b. Program Offices/System Owners shall ensure that interconnections between sensitive IT systems under their purview and IT systems not controlled by HUD are established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network.
- c. The Deputy CIO for IT Operations shall ensure controlled interfaces are configured to prohibit any protocol or service that is not explicitly permitted. For high-impact systems, the Deputy CIO for IT Operations shall review and eliminate any unnecessary functions, ports, protocols, or services once a year.
- d. The Deputy CIO for IT Operations shall ensure that a failure of the controlled interfaces does not result in any unauthorized release of information outside the information system boundary.
- e. The Deputy CIO for IT Operations shall ensure that there is no public access to HUD's internal networks except as appropriately mediated through a proxy server.
- f. The Deputy CIO for IT Operations shall ensure that alternate processing sites provide the same level of protection for network connections as the primary site.
- g. The CISO shall establish connection criteria for allowing portable or mobile information systems access to HUD's networks.
- h. The Deputy CIO for IT Operations shall ensure that portable or mobile information systems are not allowed access to HUD's networks without written approval and only after the devices meet the connection criteria established by the CISO.

5.4.4 Internet Security

The Internet is an excellent medium to publish and transmit information, thus providing substantial gains in productivity. Since the Internet is an open network available to everyone, including hackers and attackers, HUD must strike a balance that provides Internet connectivity to its constituents while maintaining an appropriate level of security.

HUD Policy

- a. The Deputy CIO for IT Operations shall ensure that any direct connection of HUD networks to the Internet or to extranets occurs through controlled interfaces that have been certified and accredited.
- b. The Deputy CIO for IT Operations shall ensure that publicly accessible information system components (e.g., public web servers) reside on separate sub-networks with separate physical network interfaces.
- c. HUD employees or contractors shall not download or install mobile code (e.g., ActiveX or JavaScript) that has not been approved by the CISO.
- d. The Deputy CIO for IT Operations shall ensure that controlled

interfaces protecting the network perimeter filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks.

e. The Deputy CIO for IT Operations shall ensure that publicly accessible information systems protect the integrity of the information and applications available to the public.

5.4.5 Personal Email Accounts

Personal email accounts often reside on insecure networks where they are subject to compromise, interception, and computer viruses.

HUD Policy

a. HUD employees or contractors shall not transmit sensitive HUD information to any personal email account that is not authorized to receive it.

b. HUD employees or contractors shall not access personal email accounts from internal HUD networks or with HUD-provided equipment.

5.5 Cryptography

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy. There are two basic types of cryptography:

1. Secret key systems-also called symmetric systems
2. Public key systems-also called asymmetric systems

In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

Refer to NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government, for more in-depth information on cryptography.

A digital signature is an electronic analogue of a written signature. The digital signature can be used to prove to a recipient or third party that the originator did in fact sign the message (i.e., the message originators cannot repudiate the message). Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system depends on maintaining the secrecy of users' private keys.

Encryption can be used to do, but is not limited to, the following:

- * Encrypt data while in storage (e.g., hard drives, diskettes, and tapes)
- * Encrypt data while in transmission
- * Encrypt individual files for transmission over an unsecured medium
- * Encrypt email messages
- * Guarantee the integrity of a file or message, and detect any modifications
- * Provide the legally binding equivalent of a hand signature in digital form
- * Support non-repudiation
- * Support authentication, including strong authentication
- * Support electronic financial transactions, including electronic funds transfers, automated teller machine transactions, cash cards, gift cards, and credit cards
- * Provide copyright protection (e.g., for DVDs)

5.5.1 Encryption

The FIPS 199 security category (for integrity and confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms.

HUD Policy

a. Program Offices/Systems Owners shall identify IT systems transmitting or storing sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

Products using triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-1 or FIPS 140-2. (All new systems should use AES because it is expected that triple DES will be phased out.)

Secure Sockets Layer Version 3.0 (SSL3.0) or Transport Layer Security Version 1.0 (TLS1.0)

National Security Agency (NSA) Type 2 or Type 1 encryption

b. The CISO and Deputy CIO for IT Operations shall ensure cryptographic key establishment and management is done in accordance with NIST SP 800-56, Recommendation on Key Establishment Schemes, and NIST SP 800-57, Recommendation on Key Management.

c. Program Offices/Systems Owners of systems rated moderate or high shall use encryption to implement the following controls:

Remote access

Wireless access

Cryptographic module authentication

Transmission integrity and confidentiality

d. Program Offices/System Owners and users shall ensure information rated moderate or high residing on portable or mobile systems use FIPS 140-1 or 140-2-approved encryption to protect information.

5.5.2 Public Key Infrastructure

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA).

HUD Policy

a. The CISO, in conjunction with the Deputy CIO for IT Operations, shall select and implement a PKI for HUD in accordance with NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure.

b. The CISO, in conjunction with the Deputy CIO for IT Operations, shall establish HUD's root CA and operate under an approved certificate policy and certificate practice statement. Any additional CAs within HUD must be subordinate to the HUD root.

c. Program Offices wishing to establish their own CA shall request approval from the CISO, be a subordinate to the HUD root, and operate under an approved certificate policy and certificate practices statement.

d. The CISO shall cross-certify the HUD root CA with the Federal Bridge. The certificate policies and practice statements of CAs subordinate to the HUD root must comply with the Federal Bridge Certificate Policy.

e. The CISO shall perform a yearly compliance audit of the root CA and all subordinate CAs.

f. The CISO, in conjunction with the Deputy CIO for IT Operations,

shall ensure that HUD's PKI can support the requirements for E-authentication in accordance with NIST SP-800-63, Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology.

g. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure that HUD's PKI can support the requirements for personal identification verification in accordance with NIST FIPS 201, Personal Identity Verification for Federal Employees and Contractors and Draft SP 800-73, Integrated Circuit Card for Personal Identity Verification.

5.5.3 Public Key/Private Key

A public key/private key pair is generated using the PKI. The user retains the private key. The issuing CA signs the public key, creating a public key certificate. These certificates are used by the PKI to validate a public key. Public key/private keys can be used in a public key cryptographic system to encrypt data. They also can be used to create digital signatures.

HUD Policy

a. The CISO, in conjunction with the Deputy CIO for IT Operations, shall ensure separate public/private key pairs are used for encryption and digital signature.

b. Users shall not disclose or allow the use of their private keys. If a user shares his or her private key, the user is accountable for all transactions signed with the user's private key.

c. Users shall be responsible for the security of their private keys.

5.6 Malicious Code Protection

Malicious code includes all and any programs (including macros and scripts) that are deliberately coded to cause an unexpected, and unwanted, event on a user's workstation. Malicious code includes viruses, worms, logic bombs, Trojan horses, web bugs, and in some cases "spyware."

Malicious code can be introduced several ways (e.g., email, file downloads, and web surfing). It can destroy the integrity and confidentiality of data and systems.

HUD Policy

a. The Deputy CIO for IT Operations shall implement a defense-in-depth strategy that:

Installs and centrally manages antivirus software at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device. The software shall be configured to check all files automatically on access, downloads, and email.

Installs updates to antivirus software and signature files at each critical information entry point (e.g., firewalls, email servers, and remote-access servers) and at each workstation, server, and mobile computing device promptly without requiring that end users specifically request the update.

Configures the software to prevent users from disabling it or modifying configuration settings.

Installs security patches to servers and desktops promptly.

Automatically forwards alerts generated by anti-virus software to HUD's intrusion detection system.

b. The Deputy CIO for IT Operations shall implement appropriate file/protocol/content filtering to protect data and networks against malicious code in accordance with HUD's Internet usage policy.

c. The Deputy CIO for IT Operations shall install and centrally manage spam and spyware protection mechanisms at each critical

information entry point (e.g., firewalls, email servers, and remote-access servers) and at workstations, servers, and mobile computing devices connected to the network. The mechanism shall have the capability for automatic updates.

5.7 Miscellaneous

The following section addresses security requirements that did not belong to any other subcategory. Some of these requirements might apply to specific technologies. Examples of such technologies include video and audio conferencing and Voice over Internet Protocol (VoIP).

HUD Policy

- a. Program Offices/System Owners of systems that have been rated moderate or high and use collaborative computing resources, like audio and video conferencing and electronic white boards, shall ensure that the collaborative computing resources cannot be activated remotely and provide explicit indication of use to the local user.
- b. Program Offices/System Owners wishing to use VOIP in information systems under their purview must obtain approval from the CISO and Deputy CIO for IT Operations and follow the guidance in NIST SP 800-58, Security Considerations for VoIP Systems.