	Department of Human Services Online Directives Information System	Index:	POL1913
		Effective:	09/20/2014
		Review:	11/02/2019

SUBJECT: DHS Information Security Policies

System and Communications Protection Policy

POLICY

This policy establishes the Enterprise System and Communications Protection Policy for managing risks from vulnerable system configurations, denial of service, data communication and transfer through the establishment of an effective System and Communications Protection program. The system and communications protection program helps DHS implement security best practices with regard to system configuration, data communication and transfer.

Authority

1. United States Department of Commerce National Institute of Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services

References:

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013
- System and Communications Protection Control Family, August 2009
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Manager” October 2006
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-41“Guidelines on Firewalls and Firewall Policy” September 2009
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-77 “Guide to IPsec VPNs” December 2005
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-56A “Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” March 2007
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-63 “Electronic Authentication Guideline” April 2006.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-28 “Guidelines on Active Content and Mobile Code” March 2008

- United States Department of Commerce Nation Institute of Standards and Technology (NIST) Special Publication 800-45 Version 2
- United States Department of Health and Human Services Office for Civil Rights "HIPAA Administrative Simplification, 164.312 Technical Safeguards"
- United States Department of Commerce Nation Institute of Standards and Technology (NIST) "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule"
- Unites States Department of Commerce National Institute of Standards and Technology (NIST) Special Publication 800-122
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Catalog of Minimum Acceptable Risk Controls for Exchanges

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information, not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions

None

Responsibilities

DHS shall adopt the System and Communications Protection principles established in NIST SP 800-53 "System and Communications Protection," Control Family guidelines, as the official policy for this domain. The following subsections outline the System and Communications Protection standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- **SC-1 System and Communications Protection Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing system and communications protection controls and preventing unauthorized access to and dissemination of IT resources and information systems and data on the basis of business and security requirements.
    2. Periodic reviews of this policy shall be performed and documented **at least within every three years**, or **when there is a significant change**.
    3. Periodic review of system and communication protection procedures shall be performed **at least annually**.
- **SC-2 Application Partitioning**

DHS information systems are designed and configured to separate user functionality (including user interface services) from information system management functionality (e.g., functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access).

- **SC-4 Information in Shared Resources**
    1. DHS information systems are configured to prevent unauthorized and unintended information transfer via shared system resources. This includes, but is not limited to:
        a) Ensuring that any previous information or content for use on the information system is made unavailable upon the allocation of the resource to all subjects, and is carried out through the implementation of safeguards,
        b) Configuring the information system's object reuse features to delete information when no longer needed,
        c) Preventing core dumps in the event of system failure,
        d) Appropriate backup and media storage.
- **SC-5 Denial of Service Protection**
  DHS information systems protect against or limit the effects of denial of service attacks via automated, technically implemented controls, and network services.
- **SC-7 Boundary Protection**
    1. The information system is configured to monitor and control communications:
        a) At the external boundary of the system
        b) At key internal boundaries within the system
    2. Subnetworks for publicly accessible system components that are physically and logically separated from internal agency networks are implemented.
    3. Public access into the organization's internal networks is prevented by the information system, except as appropriately mediated by managed interfaces employing boundary protection devices.
    4. The agency limits the number of external network connections to the information systems.
    5. A secure managed interface (VPN) is used for each external telecommunication service.
        a) Security controls must be employed as needed to protect the confidentiality and integrity of the information being transmitted.
    6. A traffic flow policy for each managed interface has been established by the agency and is implemented by agency third party service providers.
        a) Each exception to the traffic flow policy must be documented with a supporting mission/business need and the duration of that need.

b) Exceptions to the traffic flow policy must be reviewed, at a minimum, **annually**.
c) Traffic flow policy exceptions that are no longer supported by an explicit mission/business need must be removed.

7. The confidentiality and integrity of the information being transmitted across each interface is enforced.

- **SC-8 Transmission Confidentiality and Integrity**
  1. The confidentiality and integrity of transmitted information from information systems is protected.
  2. FIPS 140-2 compliant cryptographic mechanisms are utilized to prevent unauthorized disclosure of FTI and other sensitive data, and to detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN).
  3. All agency personnel are responsible for ensuring the confidentiality and integrity of sensitive data to include, but is not limited to, Federal Tax Information, Social Security Administration data, Centers for Medicare and Medicaid data, PII, etc.
- **SC-10 Network Disconnect**
  The agency terminates network connections associated with a communications session at the end of the session or after **15 minutes** of inactivity.
- **SC-12 Cryptographic Key Establishment and Management**
  DHS has established and manages cryptographic keys for required cryptography employed within the information system by using manual procedures or automated mechanisms with supporting manual procedures, when cryptographic protection is required and the information system is not covered by an enterprise solution.
- **SC-13 Cryptographic Protection**
  DHS employs at a minimum, FIPS 140-2 cryptographic mechanisms to protect agency information systems and sensitive data.
- **SC-15 Collaborative Computing Devices**
  1. Remote activation of collaborative computing devices (e.g., networked white boards, cameras, microphones) is prohibited.
  2. An explicit indication of use to users is provided in the event that collaborative computing devices activate.
     a) Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.
- **SC-17 Public Key Infrastructure Certificates**
  DHS issues public key infrastructure or obtains public key infrastructure certificates from approved service providers.
- **SC-18 Mobile Code**

1. Acceptable and unacceptable mobile code and mobile code technologies is defined and restricted appropriately.
2. Usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies are enforced.
3. The use of mobile code within the information systems

- **SC-19 Voice over Internet Protocol**
  1. Usage restrictions and implementation guidance is established for Voice over Internet Protocol (VoIP) technologies which highlight the potential to cause damage to the information system if used maliciously.
  2. The use of VoIP within company information systems authorized, monitored, and controlled.
- **SC-23 Session Authenticity**
  1. DHS provides mechanisms to protect the authenticity of communications sessions for company information systems.
     a) Mechanisms include but are not limited to the following:
        i. Security services based on IPsec
        ii. VPN
        iii. TLS
        iv. DNS
        v. SSH
        vi. SSL
        vii. Digital signatures
        viii. Digital certificates
        ix. Digital time stamping
        x. Approved encryption requirements and technology (i.e. FIPS 140-2)
- **SC-28 Protection of Information at Rest**
  The information system protects the confidentiality and integrity of information at rest (i.e., the state of information when it is located on a secondary storage device within an information system).

History
None