	Department of Human Services Online Directives Information System	Index:	POL1914
		Effective:	09/20/2014
		Review:	11/02/2019

SUBJECT: DHS Information Security Policies

System and Information Integrity Policy

POLICY

This policy establishes the Enterprise System and Information Integrity Policy, for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. The system and information integrity program helps DHS implement security best practices with regard to system configuration, security, and error handling.

Authority

1. Unites 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
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-83 “Guide to Malware Incident Prevention and Handling” November 2005
- Georgia Technology Authority Enterprise Information Security Policy
- 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

Information Integrity - Assurance that the data being accessed or read has neither been tampered with, nor been altered or damaged through a system error, since the time of the last authorized access.

System Integrity – The state of a system where it is performing its intended functions without being degraded or impaired by changes or disruptions in its internal or external environments.

Responsibilities

DHS shall adopt the System and Information Integrity principles established in NIST SP 800-53 "System and Information Integrity," Control Family guidelines, as the official policy for this domain. The following subsections outline the System and Information Integrity standards that constitute this 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 to the standards documented.

- **SI-1 System and Information Integrity Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing system and information integrity for IT resources and information systems 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 access control procedures shall be performed at least **annually**.
- **SI-2 Flaw Remediation**
    1. DHS shall identify, report, and correct information system flaws.
    2. Software updates related to flaw remediation, (including patches, services packs, and hot fixes) must be tested before installation for effectiveness and potential side effects on DHS information systems.
        a) The software code for all patches, service packs, hot fixes, etc., must be verified before testing or installation.
        b) All remediation changes must be tested on non-production systems prior to implementation on all agency-standard IT products and configurations in order to reduce or eliminate the following:
            - Unintended consequences
            - Alteration of security settings

- Enabling of default user accounts that had been disabled
- Resetting of default passwords for user accounts
- Enabling of services and functions that had been disabled
- Non-security changes, such as new functionality

3. Vulnerabilities and remediation actions must be prioritized, and their priority order must be based on the individual vulnerability criticality or severity ratings.
    a) Priorities must be established based on the source's assessment of severity or criticality as high, moderate/medium, or low.
4. A database of remediation efforts that need to be applied to the organization's IT resources must be created and maintained.
    a) Vulnerability remediation must be monitored.
5. Flaw remediation must be and is into the organizational configuration management process.
    a) Existing change management procedures must be used for testing low priority remediation efforts, and when possible, for testing patches and configuration modifications for moderate/medium priority vulnerabilities.
6. The flaw remediation process must be centrally managed.

- **SI-3 Malicious Code Protection**
    1. Malicious code protection mechanisms must be employed at information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
    2. Malicious code protection mechanisms (including signature definitions) must be updated whenever new releases are available and in accordance with agency-wide configuration management policy, procedures, and standards.
    3. Standard malicious code protection software deployed on all information systems must be configured to adhere to the following:
        a) Ensure that continuous, weekly, and real-time scanning for malicious code on files from external sources at endpoint and network entry/exit points as files are downloaded, opened, or executed.
        b) Ensure that malicious code protection software allows users to manually perform scans on their workstation and removable media.
        c) Malicious code protection software must be updated concurrently with releases of updates provided by the vendor of the software.
        d) Configure malicious code protection mechanisms to block at gateways and quarantine at host, validate quarantined code before releasing to user, clean quarantined malware as appropriate.

4. The following elements must be addressed during vendor and product selection and when tuning the malicious code protection software:
    a) The receipt of false positives during malicious code detection and eradication.
    b) The resulting potential impact on the availability of the information.
5. Malicious code protection mechanisms must be centrally managed.

- **SI-4 Information System Monitoring**
    1. Events on the information systems must be monitored in accordance with defined monitoring objectives and information system attacks must be detected
        a) Attacks and indicators of potential attacks must be detected.
    2. Unauthorized use of information systems and access local, network, and remote connections must be identified.
    3. Monitoring devices must be deployed at ad hoc locations within the system to track the following:
        a) Specific types of transactions of interest to the Agency,
        b) The impact of security changes to the information and information systems
    4. DHS shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to DHS operations, assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.
    5. Information system monitoring information shall be provided to designated agency officials as needed. Additionally, designated agency officials shall be notified of detected suspicious events and they shall take necessary actions to address suspicious events.
    6. The information system must be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions including, but not limited to:
        a) Internal traffic that indicates the presence of malicious code within an information system or propagating among system components
        b) The unauthorized export of information
        c) Attack signatures
        d) Signaling to an external information system
        e) Localized, targeted, and network-wide events
    7. Automated tools must be employed to support near real-time analysis of events.
    8. Host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) are employed and maintained on information systems that receive, process, store, or transmit sensitive data.
- **SI-5 Security Alerts, Advisories, and Directives**

1. DHS shall receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.
2. Internal security alerts, advisories, and directives must be generated, as deemed necessary.
3. Security alerts, advisories, and directives must be disseminated to DHS personnel
    a) Information system and security personnel shall check for security alerts, advisories, and directives on an ongoing basis.
4. Security directives must be implemented in accordance with established time frames, or the issuing organization must be notified of the degree of noncompliance.

- **SI-8 Spam Protection:**
    1. Spam protection mechanisms must be employed at information systems entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
    2. Spam protection mechanisms (including signature definitions) must be updated when new releases are available.
        a) Updates are implemented in accordance with DHS configuration management policy and procedures
- **SI-10 Information Input Validation:**
    1. The information system must be configured to check the validity of information inputs.
        a) The checks for input validation must be verified as part of system testing
- **SI-11 Error Handling**
    1. Error messages generated by the information system must provide information necessary for corrective actions without revealing sensitive information (e.g., account numbers, social security numbers, etc.) or potentially harmful information in error logs and administrative messages that could be exploited by adversaries.
        a) Error messages revealed to users must not include file pathnames or system architecture information.
        b) Alert error messages revealed to the administrator must include file pathnames or system architecture information and must be written to the application's error log and audit trail.
    2. The information system must be configured to reveal error messages only authorized personnel.
        a) System error messages must be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel).
- **SI-12 Information Handling and Retention**

DHS shall handle and retain both information within and output from the information system in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements.

- **SI-16 Memory Protection**
  DHS shall implement safeguards to protect the memory for all information systems from unauthorized code execution.

History
None