	Department of Human Services Online Directives Information System	Index: Effective: Review:	POL1917 09/20/2014 11/02/2019

SUBJECT: DHS Information Security Policies

Vulnerability & Risk Assessment Policy

POLICY

This policy establishes the Enterprise Risk Management Policy, for managing risk associated with information assets, information leakage, and network vulnerabilities. The Risk Management Policy and associated plans, augment DHS mission, by proactively identifying threats and vulnerabilities, which can result in consequences (impact).

Authority

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

References

- Centers for Medicare & Medicaid Services' Catalog of Minimum Acceptable Risk Controls for Exchanges
- 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 800-39 "Managing Risk from Information Systems: An Organizational Perspective" April 2008
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-115 "Technical Guide to Information Security Testing and Assessment" September 2008
- Georgia Technology Authority Enterprise Information Security Policy
- United States Internal Revenue Service Publication 1075 "Tax Information Security Guidelines for Federal, State and Local Agencies

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

Vulnerability - a hardware, software, or firmware weakness, or design deficiency, that leaves a system open to assault, harm, or unauthorized exploitation, either externally or internally,

thereby resulting in unacceptable risk of information compromise, information alteration, or service denial.

Risk Assessment - The identification, evaluation, and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk.

Responsibilities

DHS shall adopt the Risk Management principles established in NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems," as the official policy for this domain. The following subsections outline the Risk Management 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.

- **RA-1 Risk Assessment Procedures:** DHS shall
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for assessing risks to 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 vulnerability and risk assessment procedures shall be performed at least **annually**.
- **RA-3 Risk Assessment**
    1. Conduct a risk assessment (RA) to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits. The responsibility for conducting the assessment on a period basis is formally assigned to the DHS CISO and/or appointed DHS Information Security management personnel.
    2. Document the risk assessment results in a Risk Assessment Report.
    3. Review the risk assessment results at least **annually.**
    4. Disseminate risk assessment results to designated agency officials.
    5. Update the Risk Assessment Report at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions affecting the security state of the system.
- **RA-5 Vulnerability Scanning**
    1. Conduct vulnerability scans on the information system and hosted applications at least **monthly** and when new vulnerabilities potentially affecting the system/applications are identified and reported.
    2. Employ enterprise vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards that:
        a) Enumerating platforms, software flaws, and improper configurations

b) Formatting checklists and test procedures.
c) Measuring vulnerability impact.

3. Analyzes vulnerability scan reports and results from security control assessments.
4. Remediate legitimate vulnerabilities based on the organizational assessment of risk.
5. Share the information obtained from the vulnerability scanning process and security control assessments with SOs and ISOs throughout the GETS environment to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).

History
None