DHHS Information Technology (IT) Security Reporting Standard

Issue Date: October 1, 2013
Effective Date: October 1, 2013
Revised Date:

Number: DHHS-2013-001-D

1.0 Purpose and Objectives

The purpose of the Nebraska Department of Health and Human Services (DHHS) Security Reporting Standard is to provide DHHS leadership with appropriate information in a consistent format to support their fact-based decision making and allocation of future funding. Consistent reporting standards will also help to ensure that DHHS information security controls are consistent across the enterprise, meet all necessary regulations and requirements, and are appropriate for the level of risks facing DHHS and its information assets. Formal reporting helps keep the information security mission consistent, well understood and continually progressing as planned.

2.0 Scope

The following standard and recurring reports are required to be produced by the DHHS Information Security Officer (ISO):

1. Information Security Strategic Plan for DHHS
2. Information Security Annual Report
3. System Security Plans
4. Safeguard Activity Report (SAR) for Federal Tax Information (FTI)
5. Safeguard Procedures Report (SPR) for FTI
6. Plan of Actions and Milestones (POA&M)

These reports will reflect the current and planned state of information security at DHHS.

3.0 Reports and Standards

3.1 Information Security Strategic Plan

It is impossible to eliminate or mitigate all information security risks. DHHS, like all organizations, has limited funding to apply towards information technology and security. Proper planning is critical to ensure the most appropriate projects are funded by DHHS. Information Security planning is no exception. Planning for information protection will be given the same level of executive scrutiny at DHHS as planning for information technology changes. This plan shall be updated and published on an annual basis, and should include a 5-year projection of planned technology implementation and forecasted costs. It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to DHHS information resources. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall DHHS and Information Systems and Technology (IS&T) Strategic planning process.

Contents of the Strategic Plan:

1. Summary of the state of information security, mission, scope, and guiding principles
2. Analysis of the current and planned technology and infrastructure design for DHHS, and the corresponding changes required for Information Security to stay aligned with these plans.
3. Summary of the overall DHHS Information Risks Assessments and current risk levels. Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks.
4. Assessment of the current information security posture related to the future targeted posture, identified gaps, and high-level timeline necessary to close or mitigate those gaps.
5. Summary of the Policies, Standards, and Procedures for DHHS Information Security, and projected changes necessary to stay current and relevant.
6. Summary of the Information Security Education and Awareness Program, progress, and timeline of events.
7. Summary of Disaster Recovery and Business Continuity activity and plans.
8. Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect DHHS Information Security.
9. Proposed five year timeline of events
10. Line item cost projections for all information security activity is itemized by:
    a. Steady State Investments: The costs for current care and maintenance of the information security program.
    b. Risk Management and Mitigation: The line item expenses necessary to mitigate or resolve security risks for DHHS, in a prioritized order.
    c. Future Technology: The line item expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats to DHHS information.
    d. Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

3.2 Information Security Annual Report

The Information Security Annual report is intended to be an executive-level report for DHHS senior-level officials. Its purpose is to ensure that senior officials at DHHS have appropriate exposure to information security risks and activity. The report will be provided to the DHHS CIO within one month after the end of the fiscal year.

Contents of this report:

1. State of the information security summary
2. Summary of the security maturity level at start of year, and at end of year
3. Summary of reviews, assessments, inspections, and security tests, and key findings
4. Summary of security risks identified, mitigated, remediated or accepted this past year
5. Summary of the past year's threats and vulnerabilities identified and addressed
6. Summary of security incidents from the past year, including costs and impacts from those incidents
7. Summary of successful blocks, thwarted attempts, disabled viruses and worms, and other successes from the Information Security Program
8. Summary of the Information Security Education and Awareness activity for the year
9. Summary of completed activity and projects, initiatives underway, and strategic plans and upcoming activity
10. Summary of information security expenses for the year, categorized by key strategic areas.

3.3 System Security Plan

DHHS information assets have become increasingly more difficult to protect due to advances in technology such as easy-to-use high-level query languages, the use of personal computers, the accelerating use of the Internet and other networks, as well as universal familiarity with data processing. Because new technology is too often adopted before protective measures are developed, these factors have resulted in increased vulnerability of information and information systems. Without a corresponding growth in good information security practices, such advances could result in a higher likelihood of inadvertent or deliberate corruption of DHHS information assets and even the loss of the public's trust in DHHS' integrity and credibility.

The *DHHS System Security Plan (SSP)* provides an overview of the security requirements of the DHHS information system including all DHHS in-house or commercially developed and maintained systems and installations and to all external business partner systems and installations operated by, or on behalf of DHHS. The SSP describes the controls in place or planned for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system.

IS&T will work with the ISO to maintain an SSP incorporating each major system managing Highly Restricted or Confidential information and used to process DHHS business.

DHHS is required to develop or update the SSP in response to each of the following events:

- New system
- Major system modification
- Increase in security risks / exposure
- Increase of overall system security level
- Serious security violation(s)
- Every three years (minimum) for an operational system

The content of the SSP must include:

1. System name and title, description and scope of system including each all in-house or commercially developed system and installations included in the SSP.
2. Responsible organization: Name and contact information for business area responsible for the systems defined in the SSP. Decision authority for business functionality and business risks.
3. Key Contacts: Name and contact information for personnel who can address system characteristics and operation. IS&T maintenance personnel for the system, applications, and infrastructure.
4. System operation status and description of the Business Process, including a description of the function and purpose of the systems included in the SSP.
5. Description or diagram of system inputs, processing, and outputs. Describe information flow and how information is handled. Include the information classification for all information processed, accessed, or exposed.
6. System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners.
7. Applicable laws, regulations, or compliance requirements - list any laws, regulations, or specific standards, guidelines that specify requirements for the Confidentiality, Integrity, or Availability of information in the system.
8. Review of security controls and assessment results that have been conducted within the past three years.
9. Information Security Risk Assessment which includes identification of potential threat/vulnerabilities in the information system, analysis of planned or actual security controls, and potential impacts on operations, assets, or individuals.

3.4 Safeguard Activity Report (SAR) and Safeguard Procedures Report (SPR) for FTI information

DHHS shall submit an SAR and an SPR document which meets all IRS requirements as defined in IRS Publication 1075 and using the templates developed by the IRS Office of Safeguards, downloaded from IRS.GOV. The SAR shall be prepared on an annual basis. The SAR is a collection of information required by the IRS for handling of FTI and much of the content is taken from other reports and formatted to meet IRS requirements.

The SPR shall be prepared whenever significant changes occur in the DHHS Security Program, or every six (6) years. Significant changes would include, but are not limited to, new computer equipment, systems, or applications (hardware or software); new facilities; and organizational changes such as movement to a consolidated data center from an embedded IT operation. The SPR is a record of how FTI is received and processed by DHHS, and states how the confidentiality, integrity, and availability of FTI is secured.

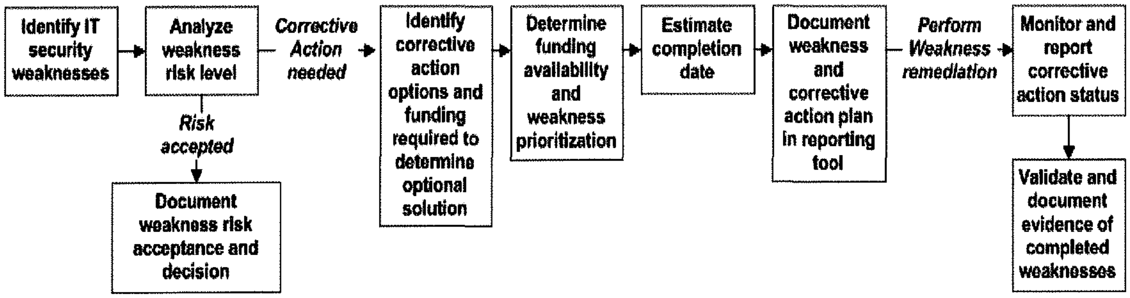
3.5 Plan of Action and Milestones Report (POA&M)

The POA&M report is a result from a monthly management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The DHHS Information Security POA&M process will be used to facilitate the remediation of DHHS Information Security and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions
- Defining roles, responsibilities, and accountabilities for weakness resolution
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources
- Ensuring appropriate progress and priorities are continually addressed
- Informing decision makers

The POA&M process provides significant benefits to DHHS. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, a POA&M must be continually monitored and diligently updated. The ISO is responsible for maintaining the POA&M and for providing monthly updates to the IS&T Management team.

Weakness Remediation and Corrective Action Planning Process


Identify IT security weaknesses
Analyze weakness risk level
Corrective Action needed
Risk accepted
Document weakness risk acceptance and decision
Identify corrective action options and funding required to determine optional solution
Determine funding availability and weakness prioritization
Estimate completion date
Document weakness and corrective action plan in reporting tool
Perform Weakness remediation
Monitor and report corrective action status
Validate and document evidence of completed weaknesses

The contents of the POA&M must meet all requirements as established by the IRS, Centers for Medicare and Medicaid Services, or other governing agency. DHHS POA&M will include the following content:

- Source – Identifies the audit, review, or procedure which identified this action item
- ID – Identification tracking number of this action item
- Project/Task – Defines the project, task objective and goals of the action item
- Key Content and Description – Narrative describing the key elements of the action item
- Key Milestones – Lists each measurable activity required to complete the action item
- Milestone Status – Lists the status of each milestone (Open, Completed, Assigned, In Progress)
- Target or Completion Date – Expected date each milestone will be completed
- Responsible Party – List of individuals or support unit assigned to address the action item

4.0 Revision History

Legal Review – 09-23-2013
Policy Approved – 09-30-2013

Signature:

Eric Henrichsen **Date:** 9/30/2013

Eric Henrichsen

Information System & Technology Administrator

Nebraska Department of Health & Human Services