Excerpts from the Pending Paper – Protecting Sensitive data on State Networks

The workflow for determining information sensitivity is based on the NIST 800-60 standards, which if examined address many of the current data type's agencies need to consider. This process is enhanced at Phase 3 with a geo-political reality check that takes non-tangible issues into account by allowing for a feedback loop for certain items that required a weighted response (e.g. Governors personal email account may be considered moderate, due to political implications of message traffic if released to the public). Figure 1 provides the general work flow for determining sensitivity:

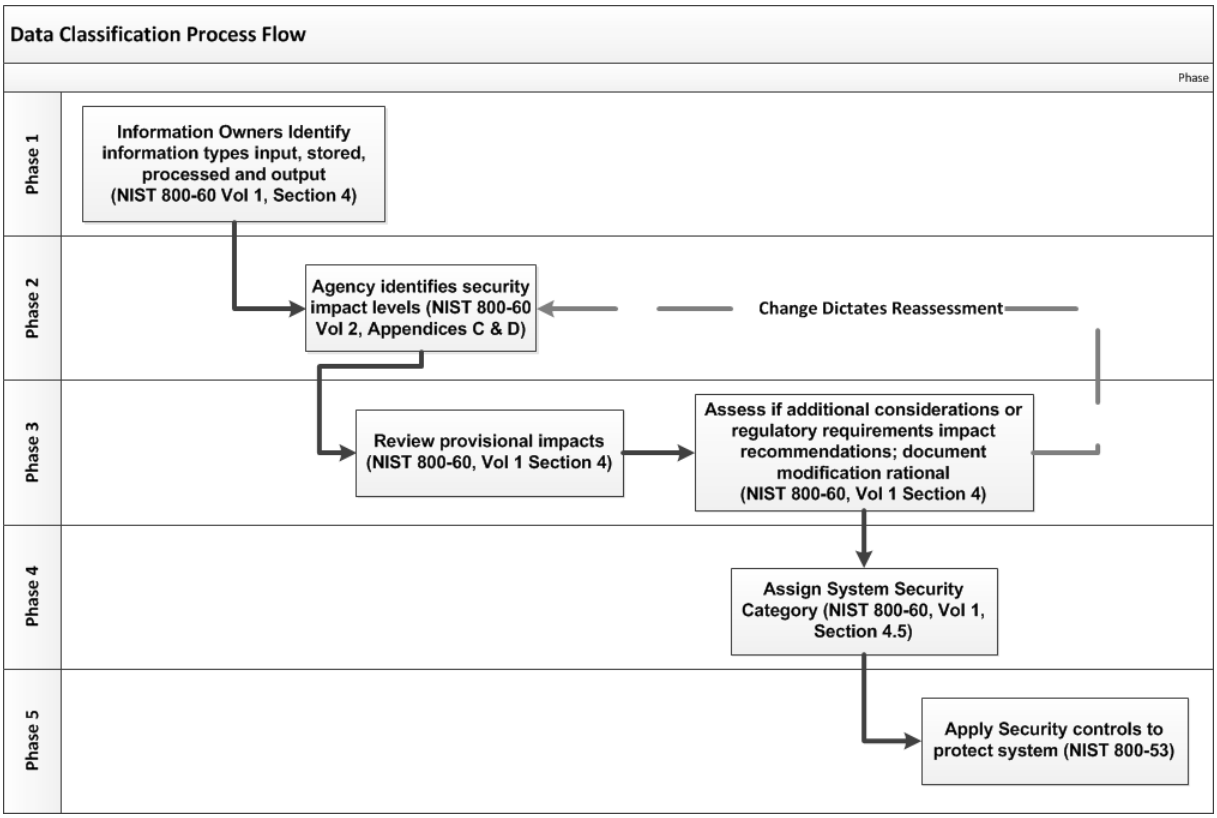

Figure 1. Data Classification Determination Workflow [5]

In order to use the workflow, one must understand the categories expressed in the Security Objective which are designated a security risk impact rating of Low, Moderate, or High across the three traditional security categories of Confidentiality, Integrity, and Availability, see table 1.

Table 1. Categorization of Information Sensitivity

Security Objective	Potential Impact Level		
	Low	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protection personal privacy, and proprietary information	Unauthorized disclosure could have a ***limited*** adverse impact on operations, assets, or individuals	Unauthorized disclosure would be expected to have a ***serious*** impact on operations, assets, or individuals	Unauthorized disclosure would be expected to have a ***serious or catastrophic*** impact on operations, assets, or individuals
Integrity Guarding against improper information modification or destruction including ensuring information non-repudiation and authenticity	Unauthorized modification or destruction could be expected to have a ***limited*** adverse impact on operations, assets, or individuals	Unauthorized modification or destruction is expected to have a ***serious*** adverse impact on operations, assets, or individuals	Unauthorized modification or destruction is expected to have a ***serious or catastrophic*** adverse impact on operations, assets, or individuals
Availability Ensuring timely and reliable access to and use of information	Access disruption could be expected to have a ***limited*** adverse impact on operations, assets, or individuals	Access disruption could be expected to have a ***serious*** adverse impact on operations, assets, or individuals	Access disruption could be expected to have a ***serious or catastrophic*** adverse impact on operations, assets, or individuals

Source: FIPS 199 [23]

However, the NIST guidelines do not do a good job helping what the definition of Low, Moderate, and High really mean. So upon research I was able to cross-correlate these to FIPS 199 definitions of Limited, Serious, and Catastrophic. Those well-defined definitions are provided below in Table 2.

Table 2. Risk Impact Definitions

Impact Rating	Definition Factors
Limited (Low)	(1) Causes a noticeable reduction in mission execution capability (2) Results in minor damage to an organizational asset(s) (3) Results in minor financial loss (4) Results in minor harm to individuals (including loss of privacy)
Serious (Moderate)	(1) Causes significant degradation in mission execution capability (2) Results in significant damage to organization asset(s) (3) Results in significant financial loss (4) Results in significant harm to individuals that is not expected to result in serious life threating injuries or loss of life
Catastrophic (High)	(1) Loss of ability to execute one or more primary mission functions (2) Results in major damage to organizational assets (3) Results in major financial losses (4) Results in catastrophic harm to individuals involving serious life threating injury or loss of life

Source: FIPS 199 [23]

Applying the Workflow with NIST 800-60 and FIPS 199 to determine the true risk rating for data. There is where the rubber meets the road so to speak. Below is an excerpt from the formula application and it demonstrates the non-standard scenarios (3) that shows the classification officer overriding the standard recommended risk sub-category due to a local consideration, causing the data to be protected at a higher overall classification.

This method requires that each data source be evaluated using a matrix considering Confidentiality, Integrity, and Availability (CIA) against the rating of Low, Moderate, and High to determine the highest watermark of risk for a given source. Using this method a formula of:

Security Category (SC) High Watermark = (Confidentiality Impact), (Integrity Impact), Availability Impact) [23]

Examples:

(1) A agency Human Resource Management system that contains salaries and payroll data is evaluated as: ***HR System Data***: (Confidentiality **Moderate**), (Integrity **Moderate**), Availability **Low**) = SC (***Moderate***)

(2) A Law Enforcement Intelligence platform system that contains intelligence planning and operations data is evaluated as: Law Enforcement Intel System: Confidentiality **High**), (Integrity **High**), Availability **High**) = SC (***High***)

(3) A Repository system of Information Technology Security Controls for IT Operations is evaluated as: Confidentiality ~~**Low**~~ **{Moderate}**), (Integrity **Moderate**), Availability ~~**Low**~~ **{Moderate}**) = SC (***Moderate***). *Note: Using the principles of Sensitive information discussed latter in this paper, the example shows the agency appropriately assigning a higher level of risk during Phase 3 of the assessment process to the unauthorized exposure of IT security controls, raising the level to Moderate.*

Once this has been determined for all potential data sets, the next step is to map that to the systems in which the data is processed. This will be address in detail in the final paper.