DEPARTMENT OF
INFORMATION TECHNOLOGY

Data Classification Methodology

Version 1.3

Document Approval and Revision Control

Author:	DOIT IT Security	Date : 3-30-10
Title:	Data Classification Methodology Version 1.3	
Signature:		
Approved by:	Michael Varney	Date : --
Title:	Director DOIT IT Security	
Signature:		
Reason for Revision:	Table of Contents added References to “Information” and “Information Systems” reviewed and edited for consistency and clarity where required Additional example added for Word Document. Hyperlinks to FIPS and NIST source reference documents added	

DOIT Data Classification Methodology
Version 1.3

Table of Contents

Section I	Purpose of Data Classification	Page 3
Section II	Role in the System Development Life cycle	Page 4
Section III	Linking Data Classification Levels to Minimum Security Control Levels	Page 4
Section IV	Data Classification Methodology	Page 4
Section V	Data Classification Process	Page 6
	Example One Example Two Example Three Example Four Example Five	Page 6 Page 8 Page 10 Page 11 Page 14
Appendix A-1	Security Categorization of Management and Support Information	Page 16
Appendix A-2	Security Categorization of Mission Based Information	Page 18
Appendix B	Data Classification Methodology References	Page 21

DOIT Data Classification Methodology
Version 1.3

Section I

Purpose of Data Classification - To establish protection profiles and assign control element settings for each category of data for which an agency is responsible. Security categorization is the basis for identifying an initial baseline set of security controls for the information and information systems.
Security categorization provides a vital step in integrating security into the state agency's business and information technology management functions, and establishes the foundation for security standardization amongst its information and information systems. Security categorization starts with the identification of what information and information systems support which government lines of business, as defined by the Federal Enterprise Architecture (FEA). Subsequent steps focus on the evaluation of the need for security in terms of confidentiality, integrity, and availability. The result is strong linkage between missions, information, and information systems with cost effective information security.

The results of system security categorization can and should be used by, or made available to, appropriate agency personnel to support agency activities including:

- Business Impact Analysis (BIA): Agency personnel should consider the cross-utilization of security categorization and BIA information in the performance of each activity. The common objectives shared by security categorization and business impact analysis initiatives provide opportunities for agencies to provide checks and balances to ensure consistency and accuracy of analytical results for information and each information system.
  Conflicting information and anomalous conditions, such as a low availability impact and a BIA three-hour recovery time objective, should trigger a reevaluation by the mission and data owners.
- Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA):, The security categorization that begins the security life cycle is a business-enabling activity directly feeding the enterprise architecture and CPIC processes for new investments, as well as migration and upgrade decisions. Specifically, the security categorization can provide a firm basis for justifying certain capital expenditures, and can also provide analytical input to avoid unnecessary investments.
- System Design: Understanding and designing the system architecture with varying information sensitivity levels in mind may assist in achieving economies of scale with security services and protection through common security zones within the enterprise. For example, an information system containing privacy information may be located in one security zone with other information systems containing similar sensitive information. Each zone may have varying levels of security. For instance, the more critical zones may require 3-factor authentication where the open area may only require normal access controls. This type of approach requires a solid understanding of an agency's information and data types gained through the security categorization process.
- Contingency and Disaster Recovery Planning: Contingency and disaster recovery planning personnel should review information systems that have multiple data types of varying impact levels, and consider grouping applications with similar information impact levels with sufficiently protected infrastructures. This approach ensures efficient application of the correct contingency and disaster protection security controls and avoids the over protection of lower impact information systems.
- Information Sharing and System Interconnection Agreements: Agency personnel should

utilize aggregated and individual security categorization information when assessing interagency connections. For example, knowing that information processed on a high impact information system is flowing to another agency's moderate impact information system should cause both agencies to evaluate the security categorization information, the implemented or resulting security controls, and the risk associated with interconnecting systems.

Section II

Role in the System Development Lifecycle - An initial security categorization should occur early in the agency's system development lifecycle (SDLC). The resulting security categorization would feed into security requirements identification (later to evolve into security controls) and other related activities such as privacy impact analysis or critical infrastructure analysis. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

Section III

Linking Data Classification Levels to Minimum Security Control Levels -NIST Special Publication 800-53 associates recommended minimum security controls with FIPS 199 low-impact, moderate-impact, and high-impact security categories. For each information system, the recommendation for minimum security controls from Special Publication 800-53 is intended to be used as a starting point for and input to the organization's risk analysis process. The risk analysis results are used to supplement the tailored baseline resulting in a set of agreed-upon controls documented in the security plan for the information system. While the FIPS 199 security categorization associates the operation of the information system with the potential impact on an organization's operations, assets, or individuals, the incorporation of refined threat and vulnerability information during the risk analysis facilitates supplementing the tailored baseline security controls to address organizational needs and tolerance for risk. The final, agreed-upon set of security controls are then documented with appropriate rationale in the security plan for the information system.

Section IV

Data Classification Methodology - The methodology presented here is adapted from the Federal Government's FISMA (Federal Information Security Management Act) information security framework and supporting FIPS (Federal Information Processing Standard) and NIST (National Institute of Standards and Technology) guides and publications.

Data is Classified on the Basis of Confidentiality, Integrity and Availability Impact Levels

As reflected in Table 1, FISMA and FIPS 199 define three security objectives for information and information systems.

Table 1: Information and Information System Security Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..."	A loss of *confidentiality* is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..."	A loss of *integrity* is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information..."	A loss of *availability* is the disruption of access to or use of information or an information system.

FIPS 199 defines three levels of *potential impact* on organizations or individuals in the event of a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization. Table 2 below provides FIPS 199 potential impact definitions.

Table 2: Potential Impact Levels

Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

The next table provides impact level definitions used in FISMA based data classification initiatives.

Table 3: Data Classification Impact Level Definitions

Security Objective	Potential Impact		
	LOW	MODERATE	HIGH

Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non- repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Data Classification Process – FISMA-based data classification has been streamlined by the publication of NIST 800-60 Volume 2 (from this point on referred to as Vol. 2). Data classification is a relatively straightforward process for users of this guide to locate specific pre-defined data classification categories that align with their information systems data types. Please see Appendix "A" for the detailed pre-defined data classification tables extracted from NIST 800-60. These tables cover most government information types and are separated into Management & Support and Mission based data types respectively.

The process consists of the following steps;

1) Information system owners review the pre-defined categories in Appendix A to locate matches for all information system data for which they are responsible.

2) They then review the detailed classification information in Vol. 2 for the particular data category to ensure their definition of the data matches the same definition in Vol. 2. The steps above are repeated for each identifiable type of data within the information system. If any data type within the system does not appear to fit into a pre-defined category then DOIT's IT Security Division will work with the information system owner to complete an analysis and classification of the data based on FIPS and NIST standards.

3) The data category is officially recorded for each data type processed or stored by the information system.

4) When all data types constituting the information system have been classified, then the security categorization of the information system will be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review. The Step 4 activities include the following: (i) review identified security categorizations for the aggregate of information types; (ii) determine the system security categorization by identifying the high water mark for each of the security objectives (confidentiality, integrity, availability) based on the aggregate of the information types; (iii) assign the overall information system impact level based on the highest impact level for the system security objectives; and (iv) document all security categorization determinations and decisions.

The following fictitious case studies provide complete examples of the data classification process described above:

Example One

An information system supporting the provision of electrical energy to the DOIT Data Centre contains the following data types:

a) Detailed electrical energy monitoring information
b) Inventory data related to backup electrical generating, UPS systems and related infrastructure devices

Step 1) The information owner reviews the predefined data categories in Appendix A and selects as a potential match. For data type (a) Detailed electrical energy monitoring information = Energy Supply (highlighted in Appendix A table A-2). For data type (b) Inventory data related to backup electrical generating, UPS systems and related infrastructure devices = Inventory Control (highlighted in Appendix A table A-1).
Step 2) The detailed classification information for the “Energy Supply” data type is accessed from Vol. 2, and reviewed to ensure that it properly describes the actual data type in the information system. The definition provided by Vol. 2 for “Energy Supply” is as follows;
D.7.1 Energy Supply Information Type
Energy Supply involves all activities devoted to ensuring the availability of an adequate supply of energy for the United States and its citizens. Energy Supply includes the sale and transportation of commodity fuels such as coal, oil, natural gas, and radioactive materials. This function also includes distributing and transferring power, electric generation, and/or storage located near the point of use.
This definition is deemed to be an accurate match.
For data type (b) the definition provided by Vol. 2 for “Inventory Control” is as follows;
C.3.4.2 Inventory Control Information Type
Inventory control refers to the tracking of information related to procured assets and resources with regards to quantity, quality, and location..
This definition is deemed to be an accurate match.
Step 3) and Step 4) consist of completing the table below:

Information System Name: Power Safe System - DOIT			
Business and Mission Supported: The Power Safe system provides real- time control and information supporting all backup electrical devices supporting the DOIT Data Center.			
Information Types			
Energy Supply	Sensor data monitoring backup power for the DOIT Data Center. This function includes control of distribution and transfer of power. The remote control capabilities can take action such as initiating necessary switching actions to alleviate an overloading power condition. The impacts to this information and the system may affect the installation’s critical infrastructures.		
Inventory Control	The Power Safe information system processes routine inventory information on all energy production, storage and monitoring devices.		
Identify Information Types	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

Energy Supply	L / L	L / M	L / M
	Disclosure of sensor information may impact the Data Center if indications & warnings of overall capability are provided to an unfriendly party.	Significant impacts or consequences may occur if unauthorized modification of information results in incorrect power system regulation or control actions.	Due to loss of availability, severe impact to the DOIT Data Center may result and may in-turn have overall catastrophic consequences for the facility's critical infrastructures.
Inventory Control	L	L	L
	Regardless of the ***moderate*** or ***high*** impact associated with unauthorized disclosure of some inventory control information, the provisional confidentiality impact level recommended for inventory control information is ***low***.	The provisional integrity impact level recommended for inventory control information is ***low***.	The provisional availability impact level recommended for inventory control information is ***low***.
Final System Categorization:	**Low**	**Moderate**	**Moderate**
	Overall Information System Impact: Moderate		

<u>Example Two</u>

An information system supporting the provision of Public Safety - Policing Services and contains the following data types:

a) Information regarding arrest warrants
b) Data related to current investigations

Step 1) The information owner reviews the predefined data categories in Appendix A and selects "Criminal Apprehension" as a potential match. For data type (a) in Appendix A table A-2. For data type (b) "Criminal Investigation and Surveillance" is selected as a potential match.

Step 2) The detailed classification information for the data type is accessed from Vol. 2, and reviewed to ensure that it properly describes the actual data types in the information system. The definition provided by Vol. 2 for "Criminal Apprehension" is as follows;

<u>D.16.1 Criminal Apprehension Information Type</u>

Criminal apprehension supports activities associated with the tracking and capture of groups or individuals believed to be responsible for committing Federal crimes.

This definition is deemed to be an accurate match.

For data type (b) the definition provided by Vol. 2 for "Criminal Investigation and Surveillance" is as follows:

<u>D.16.2 Criminal Investigation and Surveillance Information Type</u>

Criminal investigation and surveillance includes the collection of evidence required to determine responsibility for a crime and the monitoring and questioning of affected parties.

This definition is deemed to be an accurate match.

Step 3) and Step 4) consist of completing the table below:

Information System Name: Public Safety - Policing Services			
Business and Mission Supported: The Public Safety - Policing Services systems provides intelligence support to law enforcement agencies across the State of Connecticut			
Information Types			
Criminal Apprehension	The system provides details on outstanding arrest warrants, as well as historical demographic information on individuals		
Criminal Investigation and Surveillance	All information related to current investigations is available. Summary information of past investigations is also accessible.		
Identify Information Types	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Criminal Apprehension	L For most Federal law enforcement systems that support criminal apprehension activities, the harm that results from unauthorized disclosure will be limited. Therefore, the provisional confidentiality impact level recommended for criminal apprehension information is ***low***.	L For most Federal law enforcement systems that support criminal apprehension activities, the harm that results from unauthorized modification or destruction will be limited. Therefore, the provisional integrity impact level recommended for criminal apprehension information is ***low***.	M The provisional availability impact level recommended for most criminal apprehension information is ***moderate***
Criminal Investigation and Surveillance	M The provisional confidentiality impact level recommended for criminal investigation and surveillance information is ***moderate***.	M The provisional integrity impact level recommended for criminal investigation and surveillance information is ***moderate***.	M The provisional availability impact level recommended for criminal investigation and surveillance information is ***moderate***.
Final System Categorization:	**Moderate**	**Moderate**	**Moderate**
	Overall Information System Impact: Moderate		

Example Three

An information system supporting criminal justice administration contains the following data type:

a) Scheduling of court rooms and other related resources in support of judicial hearings

Step 1) The information owner reviews the predefined data categories in Appendix A and selects "Judicial Hearings "as a potential match for data type (a) above "The scheduling of court rooms and other related resources…"
Step 2) The detailed classification information for the "Judicial Hearings" data type is accessed from Vol. 2 and reviewed to ensure that it properly describes the actual data types in the information system. The definition provided by Vol. 2 for "Judicial Hearings" is as follows:*D.17.1 Judicial Hearings Information Type*
Judicial hearings include activities associated with conducting a hearing in a court of law to settle a dispute.
This definition is deemed to be an accurate match.
Step 3) and Step 4) consist of completing the table below:

Information System Name: Judicial Scheduling System			
Business and Mission Supported: The Judicial Scheduling System supports the provisioning and scheduling of all resources required for judicial hearings.			
Information Types			
Judicial Hearings	The system provides details on the scheduling of court rooms and other related personnel and required resources.		
Identify Information Types	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Judicial Hearings	M	L	L
	Given the consequences of unauthorized disclosure, the provisional confidentiality impact level recommended for judicial hearings information is ***moderate***.	Recommended Integrity Impact Level: The provisional integrity impact level recommended for judicial hearings information is ***low***.	Recommended Availability Impact Level: The provisional availability impact level recommended for judicial hearings information is ***low***.
Final System Categorization:	**M**	**L**	**L**
	Overall Information System Impact: Moderate		

<u>Example Four</u>

An information system supporting the provision of patient medical care and billing at a State Administered Hospital contains the following data types:

a) Patient Medical Records
b) Patient Billing Records
c) Inventory data related to routine hospital operations

Step 1) The information owner reviews the predefined data categories in Appendix A, and selects "Health Care Delivery Services" as a potential match.for data type (a). For data type b) "Health Care Administration" is selected as a potential match. For data type (c) "Inventory Control" is selected as a potential match.

Step 2) The detailed classification information for data type (a) is accessed from Vol. 2, and reviewed to ensure that it properly describes the actual data types in the information system. The definition provided by Vol. 2 for "Health Care Delivery Services" is as follows:
<u>D.14.4 Health Care Delivery Services Information Type</u>
Health Care Delivery Services provide and support the delivery of health care to its beneficiaries. The support includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation.
This definition is deemed to be an accurate match.
For data type (b) the definition provided by Vol. 2 for "Health Care Administration" is as follows:
<u>D.14.3 Health Care Administration Information Type</u>
Health Care Administration assures that federal health care resources are expended effectively to ensure quality, safety, and efficiency. This includes managing health care quality, cost, workload, utilization, and fraud/abuse efforts.
This definition is deemed to be an accurate match.
For data type c) the definition provided by Vol. 2 for "Inventory Control" is as follows:
<u>C.3.4.2 Inventory Control Information Type</u>
Inventory control refers to the tracking of information related to procured assets and resources with regard to quantity, quality, and location.
This definition is deemed to be an accurate match.
Step 3) and Step 4) consist of completing the table below:

Information System Name: Hospital Administration System			
Business and Mission Supported: The Hospital Administration System supports the provision of medical services to patients, as well as Hospital financial and administrative services.			
Information Types			
Health Care Delivery Services	Complete medical record information for all current and former patients.		
Health Care Administration	Provides billing and accounting services in support of all hospital activities.		
Inventory Control	Tracks all tangible hospital assets from acquisition to disposal.		
Identify Information Types	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Health Care Delivery Services	L	H	L
	The provisional confidentiality impact level recommended for disclosure of health care delivery services information is ***low***.	Because of the potential for the loss of human life, the provisional integrity impact level recommended for health care delivery services information is ***high***.	The provisional availability impact level recommended for health care delivery services information is ***low***.
Health Care Administration	L	M	L
	The provisional confidentiality impact level recommended for disclosure of Health Care Administration information is ***low***.	The provisional integrity impact level recommended for Health Care Administration information is ***Moderate***.	The provisional availability impact level recommended for Health Care Administration information is ***low***.
Inventory Control	L	L	L
	Regardless of the ***moderate*** or ***high*** impact associated with unauthorized disclosure of some inventory control information, the provisional confidentiality impact level recommended for inventory control information is ***low***.	The provisional integrity impact level recommended for inventory control information is ***low***.	The provisional availability impact level recommended for inventory control information is ***low***.
Final System Categorization:	**L**	**H**	**L**
	Overall Information System Impact: High		

Example Five

A word document consisting of a list of retired employees contains the following data types:

d) Employee Name
e) Employee Address
f) Monetary retirement benefits received to date

For the purposes of this example, we will assume the data contained in the document was exported from anther system that is the system of record for this data.

Step 1) The data owner reviews the predefined data categories in Appendix A, and selects "General Retirement and Disability" as a potential match for data types a, b, and c.

Step 2) The detailed classification information for the data type is accessed from Vol. 2, and reviewed to ensure that it properly describes the actual data types in the document. The definition provided by Vol. 2 for "General Retirement and Disability" is as follows:

D.15.1 General Retirement and Disability Information Type

> *General Retirement and Disability involves the development and management of retirement benefits, pensions, and income security for those who are retired or disabled.*

This definition is deemed to be an accurate match.

Step 3) and Step 4) consist of completing the table below:

Information System Name: Document Containing Retirement Benefit			
Business and Mission Supported: This document supports the provision and reporting of retirement benefits			
Information Types			
General Retirement and Disability	Retirement benefit information for retired employees is contained in this document.		
Identify Information Types	**Confidentiality Impact**	**Integrity Impact**	**Availability**
General Retirement	M	M	L

and Disability	The confidentiality impact recommended for general retirement and disability information is ***moderate***.	The provisional integrity impact level recommended for general retirement and disability information is ***moderate***.	The provisional availability impact level recommended for general retirement and disability information is ***moderate***. But, because this is not the authoritative source of this information, and the information can be readily retrieved from the system of record, the availability impact is likely, in reality, ***low***
Final Categorization	**M**	**M**	**L**
	Overall Impact: Moderate		

Appendix A

Table Appendix A-1 Security Categorization of Management and Support Information

	Confidentiality	Integrity	Availability
Controls and Oversight			
Corrective Action (Policy/Regulation)	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low[3]	Low	Low
Regulatory Development			
Policy and Guidance Development	Low	Low	Low
Public Comment Tracking	Low	Low	Low
Regulatory Creation	Low	Low	Low
Rule Publication	Low	Low	Low
Planning and Budgeting			
Budget Formulation	Low	Low	Low
Capital Planning	Low	Low	Low
Enterprise Architecture	Low	Low	Low
Strategic Planning	Low	Low	Low
Budget Execution	Low	Low	Low
Workforce Planning	Low	Low	Low
Management Improvement	Low	Low	Low
Budgeting & Performance Integration	Low	Low	Low
Tax and Fiscal Policy	Low	Low	Low
Internal Risk Management and Mitigation			
Contingency Planning	Moderate	Moderate	Moderate
Continuity of Operations	Moderate	Moderate	Moderate
	Confidentiality	Integrity	Availability
Service Recovery	Low	Low	Low
Revenue Collection			
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Federal Asset Sales	Low	Moderate	Low
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Product Outreach	Low	Low	Low
Public Relations	Low	Low	Low
Legislative Relations			

Legislation Tracking	Low	**Low**	Low
Legislation Testimony	Low	**Low**	Low
Proposal Development	Moderate	**Low**	Low
Congressional Liason Operations	Moderate	**Low**	Low
General Government			
Central Fiscal Operations4	Moderate	**Low**	Low
Legislative Functions	Low	**Low**	Low
Executive Functions5	Low	**Low**	Low
Central Property Management	Low6	**Low**	Low7
Central Personnel Management	Low	**Low**	Low
Taxation Management	Moderate	**Low**	Low
Central Records and Statistics Management	Moderate	**Low**	Low
Income Information	Moderate	**Moderate**	Moderate
Personal Identity and Authentication	Moderate	**Moderate**	Moderate
Entitlement Event Information	Moderate	**Moderate**	Moderate
Representative Payee Information	Moderate	**Moderate**	Moderate
General Information	Low	**Low**	Low
	Confidentiality	**Integrity**	Availability
Administrative Management			
Facilities, Fleet, and Equipment Mgmt	Low6	**Low7**	Low7
Help Desk Services	Low	**Low**	Low
Security Management	Moderate	**Moderate**	Low
Travel	Low	**Low**	Low
Workplace Policy Development and Management	Low	**Low**	Low
Financial Management			
Asset and Liability Management	Low	**Low**	Low
Reporting and Information	Low	**Moderate**	Low
Funds Control	Moderate	**Moderate**	Low
Accounting	Low	**Moderate**	Low
Payments	Low	**Moderate**	Low
Collections and Receivables	Low	**Moderate**	Low
Cost Accounting/ Performance Measurement	Low	**Moderate**	Low
Human Resource Management			
HR Strategy	Low	**Low**	Low
Staff Acquisition	Low	**Low**	Low
Organization and Position Management	Low	**Low**	Low
Compensation Management	Low	**Low**	Low
Benefits Management	Low	**Low**	Low
Employee Performance Management	Low	**Low**	Low
Employee Relations	Low	**Low**	Low

Labor Relations	Low	**Low**	Low
Separation Management	Low	**Low**	Low
Human Resources Development	Low	**Low**	Low
Supply Chain Management			
Goods Acquisition	Low	**Low**	Low
Inventory Control	Low	**Low**	Low
Logistics Management	Low	**Low**	Low
Services Acquisition	Low	**Low**	Low
Information & Technology Management			
System Development	Low	**Moderate**	Low
Lifecycle/Change Management	Low	**Moderate**	Low
System Maintenance	Low	**Moderate**	Low
IT Infrastructure Maintenance[10]	Low	**Low**	Low
Information System Security	Low	**Moderate**	Low
	Confidentiality	**Integrity**	Availability
Record Retention	Low	**Low**	Low
Information Management[11]	Low	**Moderate**	Low
System and Network Monitoring	Moderate	**Moderate**	Low
Information Sharing	N/A	**N/A**	N/A

Table Appendix A-2: Security Categorization of Mission Based Information

	Confidentiality	Integrity	Availability
Defense & National Security	**Nat'l Security**	**Nat'l Security**	**Nat'l Security**
Homeland Security			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	**High**	**High**	**High**
Catastrophic Defense	**High**	**High**	**High**
Executive Functions of the EO P[23]	**High**	**Moderate**	**High**
Intelligence Operations[24]	**High**	**High**	**High**
Disaster Management			
Disaster Monitoring and Prediction	Low	**High**	**High**
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	**Low**	**Low**	**Low**
Emergency Response	Low	**High**	**High**
	Confidentiality	**Integrity**	**Availability**
International Affairs and Commerce			
Foreign Affairs	**High**	**High**	Moderate

International Development and Humanitarian Aid	Moderate	Low	Low
Global Trade	High	High	High
Natural Resources			
Water Resource Management	Low	Low	Low
Conservation, Marine, and Land Management	Low	Low	Low
Recreational Resource Management and Tourism	Low	Low	Low
Agricultural Innovation and Services	Low	Low	Low
Energy			
Energy Supply	Low	Moderate	Moderate
Energy Conservation and Preparedness	Low	Low	Low
Energy Resource Management	Moderate	Low	Low
Energy Production	Low	Low	Low
Environmental Management			
Environmental Monitoring/ Forecasting	Low	Moderate	Low
Environmental Remediation	Moderate	Low	Low
Pollution Prevention And Control	Low	Low	Low
Economic Development			
Business and Industry Development	Low	Low	Low
Intellectual Property Protection	Low	Low	Low
Financial Sector Oversight	Moderate	Low	Low
Industry Sector Income Stabilization	Moderate	Low	Low
Community and Social Services			
Homeownership Promotion	Low	Low	Low
Community and Regional Development	Low	Low	Low
Social Services	Low	Low	Low
Postal Services	Low	Moderate	Moderate
Transportation			
Ground Transportation	Low	Low	Low
Water Transportation	Low	Low	Low
Air Transportation	Low	Low	Low
Space Operations	Low	High	High
Education			
Elementary, Secondary, and Vocational Education	Low	Low	Low
Higher Education	Low	Low	Low
Cultural & Historic Preservation	Low	Low	Low
Cultural & Historic Exhibition	Low	Low	Low
Workforce Management			
	Confidentiality	Integrity	Availability
Training and Employment	Low	Low	Low
Labor Rights Management	Low	Low	Low
Worker Safety	Low	Low	Low
Health			
Access to Care	Low	Moderate	Low

Population Health Management and Consumer Safety	Low	Moderate	Low
Health Care Administration	Low	Moderate	**Low**
Health Care Delivery Services	Low	**High**	Low
Health Care Research and Practitioner Education	**Low**	**Moderate**	**Low**
Income Security			
General Retirement and Disability	**Moderate**	Moderate	Moderate
Unemployment Compensation	Low	**Low**	**Low**
Housing Assistance	Low	**Low**	**Low**
Food and Nutrition Assistance	Low	**Low**	**Low**
Survivor Compensation	Low	**Low**	**Low**
Law Enforcement			
Criminal Apprehension	Low	Low	**Moderate**
Criminal Investigation and Surveillance	Moderate	Moderate	Moderate
Citizen Protection	Moderate	Moderate	Moderate
Leadership Protection	Moderate	Low	Low
Property Protection	Low	Low	Low
Substance Control	Moderate	Moderate	Moderate
Crime Prevention	Low	**Low**	Low
Trade Law Enforcement[27]	**Moderate**	Moderate	**Moderate**
Litigation and Judicial Activities			
Judicial Hearings	Moderate	**Low**	Low
Legal Defense	Moderate	High	Low
Legal Investigation	Moderate	Moderate	Moderate
Legal Prosecution and Litigation	Low	Moderate	Low
Resolution Facilitation	Moderate	**Low**	**Low**
Federal Correctional Activities			
Criminal Incarceration	**Low**	Moderate	Low
Criminal Rehabilitation	Low	**Low**	**Low**
General Science and Innovation			
Scientific and Technological Research and Innovation	Low	**Moderate**	**Low**
Space Exploration and Innovation	Low	**Moderate**	**Low**
Knowledge Creation and Management			
Research and Development	Low	**Moderate**	**Low**
General Purpose Data and Statistics	Low	**Low**	**Low**
Advising and Consulting	Low	**Low**	**Low**
Knowledge Dissemination	Low	Low	Low
	Confidentiality	Integrity	Availability
Regulatory Compliance and Enforcement			
Inspections and Auditing	Moderate	**Moderate**	**Low**
Standards Setting/ Reporting Guideline Development	**Low**	**Low**	**Low**
Permits and Licensing	Low	**Low**	**Low**
Public Goods Creation and Management			
Manufacturing	**Low**	**Low**	**Low**
Construction	Low	**Low**	**Low**

Public Resources, Facility, and Infrastructure Management	Low	Low	Low
Information Infrastructure Management	Low	Low	Low
Federal Financial Assistance			
Federal Grants (Non-State)	Low	Low	Low
Direct Transfers to Individuals	Low	Low	Low
Subsidies	Low	Low	Low
Tax Credits	Moderate	Low	Low
Credits and Insurance			
Direct Loans	Low	Low	Low
Loan Guarantees	Low	Low	Low
General Insurance	Low	Low	Low
Transfers to State/Local Governments			
Formula Grants	Low	Low	Low
Project/Competitive Grants	Low	Low	Low
Earmarked Grants	Low	Low	Low
State Loans	Low	Low	Low
Direct Services for Citizens			
Military Operations[28]	N/A	N/A	N/A
Civilian Operations[28]	N/A	N/A	N/A

Appendix B

Data Classification Methodology References

The following documents were utilized as original source material for this guide:

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NIST SP 800-30, Risk Management Guide for Information Technology Systems: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST Draft SP 800-39, Managing Risk from Information Systems: An Organization Perspective: http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf

NIST SP 800-53, Recommended Security Controls for Federal Information Systems Rev. 3: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

NIST SP 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf