provided under the sub-heading "Special Factors Affecting [Security Objective] Impact Determination."

Appendices C.2 and C.3 identify information elements and contexts that may result in variances from the basic impact level assignment. For example, some systems process information the compromise of which affect national security, critical infrastructures, or key national assets. Impacts associated with such systems are either outside the scope of this document (i.e., national security information) or may need to be adjusted upward based on the more severe consequences of compromises.

Many of the information types are also lifecycle-dependent. That is, information that requires protection at one stage in system development or operational use of the information is publicly accessible at a later stage or following some event. For example, information that has confidentiality attributes during the period that an agency is using it to make a decision may be public knowledge once the decision has been made (e.g., financial/budgetary information used during development of requests for proposals in procurement actions).

Table C-2: Type-based Impacts for Federal Information and Information Systems

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**

[3] The confidentiality impact assigned to the Program Monitoring Information Type may necessitate the highest confidentiality impact of the information types processed by the system.

Security Categorization of Management and Support Information

	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 Operations[4]	Moderate	**Low**	**Low**
Legislative Functions	**Low**	**Low**	Low
Executive Functions[5]	**Low**	**Low**	**Low**
Central Property Management	Low[6]	**Low**	Low[7]
Central Personnel Management	Low	Low	Low
Taxation Management	Moderate	Low	Low
Central Records and Statistics Management	Moderate	**Low**	**Low**
Income Information[8]	**Moderate**	Moderate	Moderate
Personal Identity and Authentication[8]	Moderate	Moderate	Moderate
Entitlement Event Information[8]	**Moderate**	Moderate	Moderate
Representative Payee Information[8]	**Moderate**	Moderate	Moderate
General Information[9]	Low	Low	Low

[4] Tax-related functions are associated with the Taxation Management information type.

[5] The OMB Business Reference Model "Executive Function has been expanded to include general agency executive functions as well as Executive Office of the President (EOP) functions. Strictly EOP executive functions are treated in Appendix D, Examples of Impact Determination for Mission-Based Information and Information Systems.

[6] High where safety of major critical infrastructure components or key national assets is at stake.

[7] Moderate or High in emergency situations where time-critical processes affecting human safety or major assets are involved.

[8] The identified information types are not a derivative of OMB's Business Reference Model and were added to address privacy information.

[9] The OMB Business Reference Model does not include a General Information information type. This information type was added as a catch-all information type. As such, agencies may use this to identify additional information types not defined in the BRM and assign impact levels.

Security Categorization of Management and Support Information

	Confidentiality	Integrity	Availability
Administrative Management			
Facilities, Fleet, and Equipment Mgmt	Low[6]	Low[7]	Low[7]
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**

[10] The confidentiality impact assigned to the IT Infrastructure Maintenance Information Type may necessitate the highest confidentiality impact of the information types processed by the system.

Security Categorization of Management and Support Information

	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

C.2 Rationale and Factors for Services Delivery Support Information

Services delivery support functions provide the critical policy, programmatic, and managerial foundation to support Federal government operations. Security objectives and impact levels for service delivery support information and systems are generally determined by the natures of the supported direct services and constituencies being supported. If a system stores, processes, or communicates *national security* information, it is defined as a *national security system*, and is outside the scope of this guideline.[12] Service delivery support activities are defined in this section.

C.2.1 Controls and Oversight

Controls and Oversight information is used to ensure that the operations and programs of the Federal government and its external business partners comply with applicable laws and regulations and prevent waste, fraud, and abuse.

C.2.1.1 Corrective Action Information Type

Corrective Action involves the enforcement functions necessary to remedy programs that have been found non-compliant with a given law, regulation, or policy. The recommended security categorization for the corrective action information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of corrective action information on the ability of responsible agencies to remedy internal or external programs that have been found non-compliant with a given law, regulation, or policy. Unauthorized disclosure of most corrective action information should have only a limited adverse effect on agency operations, assets, or individuals.

[11] The confidentiality impact assigned to the Information Management Information Type may necessitate the highest confidentiality impact of the information types processed by the system.

[12] A *national security system* is any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a routine administrative or business applications system used for applications such as payroll, finance, logistics, and personnel management); or (ii) that processes classified information.