From OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*:

In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

1. Conversions - when converting paper-based records to electronic systems;
2. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
3. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
   - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
4. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
   - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
5. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
6. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
7. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
   - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
8. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
   - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
9. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

Examples of Business Identifiable Information (BII):

- Financial information provided in response to requests for economic census data
- Business plans and marketing data provided to participate in trade development events
- Commercial and financial information collected as part of export enforcement actions
- Proprietary information provided in support of a grant application or related to a federal acquisition action
- Financial records collected as part of an investigation

From NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of PII*:

Context of Use

The context of use factor is related to the Fair Information Practices of Purpose Specification and Use Limitation. Context of use is defined as the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated. Examples of context include, but are not limited to, statistical analysis, eligibility for benefits, administration of benefits, research, tax administration, or law enforcement. Organizations should assess the context of use because it is important in understanding how the disclosure of data elements can potentially harm individuals and the organization. Organizations should also consider whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual. For example, law enforcement investigations could be compromised if the mere fact that information is being collected about a particular individual is disclosed.

The context of use factor may cause the same types of PII to be assigned different PII confidentiality impact levels in different instances. For example, suppose that an organization has three lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general - interest newsletter produced by the organization. The second list is people who have filed for retirement benefits, and the third list is individuals who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each of the three lists. Based on context of use only, the three lists are likely to merit impact levels of low, moderate, and high, respectively.

Organizations should categorize their PII by the PII confidentiality impact level.

All PII is not created equal. PII should be evaluated to determine its PII confidentiality impact level, which is different from the Federal Information Processing Standard (FIPS) Publication 199 confidentiality impact level, so that appropriate safeguards can be applied to the PII. The PII confidentiality impact level — low, moderate, or high — indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. Below is a list of factors an organization should consider when determining the PII confidentiality impact level. Each organization should decide which factors it will use for determining impact levels and then create and implement the appropriate policy, procedures, and controls. The following are examples of factors:

- Identifiability – Organizations should evaluate how easily PII can be used to identify specific individuals. For example, a SSN uniquely and directly identifies an individual, whereas a telephone area code identifies a set of people.

- Quantity of PII – Organizations should consider how many individuals can be identified from the PII. Breaches of 25 records and 25 million records may have different impacts. The PII confidentiality impact level should only be raised and not lowered based on this factor.
- Data Field Sensitivity – Organizations should evaluate the sensitivity of each individual PII data field. For example, an individual's SSN or financial account number is generally more sensitive than an individual's phone number or ZIP code. Organizations should also evaluate the sensitivity of the PII data fields when combined.
- Context of Use – Organizations should evaluate the context of use — the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The context of use may cause the same PII data elements to be assigned different PII confidentiality impact levels based on their use. For example, suppose that an organization has two lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general - interest newsletter produced by the organization, and the second list is people who work undercover in law enforcement. If the confidentiality of the lists is breached, the potential impacts to the affected individuals and to the organization are significantly different for each list.
- Obligations to Protect Confidentiality – An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance). For example, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII.
- Access to and Location of PII – Organizations may choose to take into consideration the nature of authorized access to and the location of PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported offsite, then there are more opportunities to compromise the confidentiality of the PII.