Information Sensitivity Leveling Standard

Background & Overview

All information held by (or on behalf of) the CFPB is assigned a Sensitivity level. The Sensitivity level determines important rules, guidelines and expectations around the storage, access, use, and disclosure of information. The CIO, or any other individual or committee to whom the CIO has delegated authority, is responsible for determining the appropriate Sensitivity level of information.

Given the complex and often subjective nature of sensitivity determination, this document does not attempt to provide detailed, prescriptive rules for assigning sensitivity levels. Rather, it is intended to guide the Bureau in the process of making those decisions. As such, it will continue to evolve as proscriptive rules are identified and guidelines evolve.

Limitations

Sensitivity levels under this Standard are not intended to either parallel or replace any categories of classified national security information (e.g. Classified, Secret, Top Secret).

Sensitivity levels under this Standard do not align with or have any direct bearing on whether a given piece of information would be released under a FOIA or Privacy Act request.[1]

Sensitivity levels under this Standard do not align with or have any direct bearing on whether a given piece of information constitutes a Record under the Federal Records Act.[2]

Sensitivity levels under this Standard do not align with or have any direct bearing on whether a given piece of information is classified under the Control Unclassified Information program.[3]

There is no direct correlation between the Sensitivity levels under this Standard and the security categorization of CFPB information systems under National Institute of Standards and Technology (NIST) publications or the Federal Information Security Management Act (FISMA).[4]

Determining Information Sensitivity Levels

All information received by the Bureau will be assigned a sensitivity level (Public, Low, Medium, or High). The sensitivity level can be based on a number of factors, but is primarily determined by:

[1] For additional information on FOIA, visit http://team.cfpb.local/wiki/index.php/FOIA.
[2] For additional information on Records, visit http://team.cfpb.local/wiki/index.php/Records_Management_Information_Center.
[3] For more details on Controlled Unclassified Information, see Executive Order 13556 available at http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information
[4] For additional information on Cybersecurity, including policies, processes, standards, and templates, visit http://team.cfpb.local/wiki/index.php/Cybersecurity.

- The authority under which the information was received
- Legal restrictions related to the information
- Any contractual restrictions, such as MOUs, non-disclosure agreements, contracts, *etc*.
- Presence and sensitivity of PII or Direct Identifiers, or level of re-identification risk
- The commercial sensitivity of the information
- Whether the information is available to the general public
- Bureau policy considerations arising from the content of the information

A. Public Information

Public Information is information which is available to the general public through sources other than the CFPB (e.g., other governmental bodies, universities, free publications, *etc*.).

Characteristics of Public Information

Is Not Public if:

- Includes raw data acquired through Enforcement or Supervisory authorities, or otherwise constitutes confidential investigative information, confidential supervisory information, or confidential consumer complaint information
- Contains Direct Identifiers of an individual who has not provided consent for its provision, use, or disclosure (e.g., SSN, address, full name, account numbers etc.), unless such Direct Identifiers are of public figures and have been made public as part of the content being acquired (such as journalists' bylines, names of business executives, individual images or audio/video files of public figures, etc.)
- Contains confidential, proprietary or commercially sensitive information
- Was made available to the public via illegal means (e.g. leaked documents)

Is Public if:

- Available to the general public by legal means with no restrictions regarding access or use

Sample Implications of Public Leveling

- Bureau employees, contractors, or consultants may be granted access without the need for additional approvals
- Information may generally be shared internally without restrictions
- May be exempted from data intake governance requirements; see *Public Information Intake Exception* for more details

Examples of Public Information

- Publicly released macroeconomic data such as employment statistics, GDP, etc.
- News articles from publicly available sources

B. Low Sensitivity Information

Low sensitivity information is generally information that is not generally available to the public, but which would not likely cause significant harm if misused.

Characteristics of Low Sensitivity Information

Is Not Low Sensitivity if:

- Includes raw data acquired through Enforcement or Supervisory authorities, or otherwise constitutes confidential investigative information, confidential supervisory information, or confidential consumer complaint information
- Contains Direct Identifiers of an individual who has not provided consent for its provision, use, or disclosure (e.g., SSN, address, full name, account numbers etc.), unless such Direct unless such Direct Identifiers are of public figures and have been made public as part of the content being acquired (such as journalists' bylines, names of business executives, individual images or audio/video files of public figures, etc.)
- Contains information which could cause significant harm to individuals if improperly used or disclosed (e.g. SSN, account numbers, etc.)
- Contains information which could cause significant harm to business entities if improperly used or disclosed (e.g. trade secrets)
- Received from a third party under contract or other agreement with significant restrictions regarding use, access, or disclosure

Is Low Sensitivity if:

- Is commercially available to the general public without material restrictions on access or use (e.g. magazine subscriptions)

May Be Low Sensitivity if it:

- Contains PII with low re-identification risk
- Contains Direct Identifiers of an individual who has provided explicit consent for its provision, use, or disclosure, assuming the information will be used in a manner consistent with the purpose for which the consent was provided
- Derived from information received through Enforcement or Supervisory authorities and through aggregation, source masking, or other techniques, does not reveal the identity of any consumer or business entity involved

Sample Implications of Low Sensitivity Leveling

- Bureau employees, contractors, or consultants may be granted access without the need for additional approvals
- Information may generally be shared internally without restrictions
- May be exempted from data intake governance requirements; see *Low Sensitivity Information Intake Exception* for more details

Examples of Low Sensitivity Information

- Purchased periodicals or industry reports that do not contain PII or trade secrets
- General Bureau-wide information that is intended to be available to all employees

C. Medium Sensitivity Information

Medium sensitivity information is generally information that is confidential, but that does not contain highly sensitive data such as Direct Identifiers concerning individuals or sensitive proprietary information concerning business entities.

Characteristics of Medium Sensitivity Information

Is Not Medium Sensitivity if:

- Includes raw data acquired through Enforcement or Supervisory authorities, or otherwise constitutes confidential investigative information, confidential supervisory information, or confidential consumer complaint information
- Contains Direct Identifiers of an individual who has not provided consent for its provision, use, or disclosure (e.g., SSN, address, full name, account numbers etc.), unless such Direct unless such Direct Identifiers are of public figures and have been made public as part of the content being acquired (such as journalists' bylines, names of business executives, individual images or audio/video files of public figures, etc.)
- Contains information which could cause significant harm to individuals if improperly used or disclosed (e.g. SSN, account numbers, etc.)
- Contains information which could cause significant harm to business entities if improperly used or disclosed (e.g. trade secrets)

May Be Medium Sensitivity if:

- Is commercially available with restrictions on access or use
- Poses a risk of re-identification, either on its own or when there is a reasonable expectation of re-identification when combined with other information
- Derived from information received through Enforcement or Supervisory authorities and through aggregation, source masking, or other techniques, does not reveal the identity of any source of data or of any consumer or business entity involved
- Certain types of confidential Bureau information (such as certain sensitive and pre-decisional documents)

Sample Implications of Medium Sensitivity Leveling

- Access may be granted to users with relevant roles
- Should be stored in a central, access-controlled location

Examples of Medium Sensitivity Information

- Commercially-available loan-level data that does not contain direct identifiers
- Procured data with significant contractual or MOU-based restrictions

D. High Sensitivity Information

High sensitivity information is information which carries with it a significant legal, reputational or financial risk to the Bureau, individuals and/or business entities, should it be improperly accessed, used, or disclosed.

Characteristics of High Sensitivity Information

Is High Sensitivity if:

- Includes raw data acquired through Enforcement or Supervisory authorities, or otherwise constitutes confidential investigative information, confidential supervisory information, or confidential consumer complaint information
- Contains Direct Identifiers of an individual who has not provided consent for its provision, use, or disclosure (e.g., SSN, address, full name, account numbers etc.), unless such Direct unless such Direct Identifiers are of public figures and have been made public as part of the content being acquired (such as journalists' bylines, names of business executives, individual images or audio/video files of public figures, etc.)
- Contains information which could cause significant harm to individuals if improperly used or disclosed (e.g. SSN, account numbers, etc.)
- Contains information which could cause significant harm to business entities if improperly used or disclosed (e.g. trade secrets)
- Otherwise deemed to carry a significant legal, reputational, operational or financial risk to the Bureau

Sample Implications of High Sensitivity Leveling

- To receive access, users must have a demonstrated business need
- Should be stored in a central, access-controlled location

Examples of High Sensitivity Information

- Raw Supervisory Exam information
- Raw Enforcement information
- Raw consumer complaint information
- CFPB employee names and home addresses when presented together

Sign & Date

This Standard shall become effective on September 30, 2014.

ASHWIN VASAN Digitally signed by ASHWIN VASAN
DN: c=US, o=U.S. Government, ou=Consumer Financial Protection Bureau, cn=ASHWIN VASAN, 0.9.2342.19200300.100.1.1=95581002465793
Date: 2014.09.30 21:27:07 -04'00'

Signature: _____ Date: _____

Ashwin Vasan, Chief Information Officer, Consumer Financial Protection Bureau