



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

December 29, 2011

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Kevin Neyland 
Deputy Administrator, Office of Information and Regulatory Affairs

SUBJECT: Model Privacy Impact Assessment for Agency Use of Third-Party
Websites and Applications

On June 25, 2010, OMB issued Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications. The memorandum requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites or applications to engage with the public. Among other requirements, the memorandum asks agencies to prepare an adapted Privacy Impact Assessment (PIA) that is tailored to address the specific functions of a third-party website or application that is being used.

To facilitate agency use of third-party websites and applications, OMB has worked with the CIO Council's Privacy Committee to develop a model PIA reflecting the requirements for an adapted PIA. You are requested to use the attached model PIA when preparing an adapted PIA before engaging the public through third-party websites and applications. The introduction to the model PIA provides additional context for agencies completing an adapted PIA, and the eight sections in the model are aligned with Section 4(a)(i-viii) of M-10-23.

If you have any questions regarding the model PIA or Memorandum M-10-23—or wish to discuss possible deviations from the model PIA—please contact OMB at privacy-oir@omb.eop.gov.

MODEL PRIVACY IMPACT ASSESSMENT FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS

This document does not create, modify, or interpret any laws, regulations, or OMB policies. When Federal agencies have questions about OMB guidance, they may contact OMB at privacy-oira@omb.eop.gov.

Contents

Introduction

SECTION 1.0 – SPECIFIC PURPOSE OF THE AGENCY’S USE OF A THIRD-PARTY WEBSITE OR APPLICATION

1.1 – What is the specific purpose of the agency’s use of the third-party website or application and how does that use fit with the agency’s broader mission?

1.2 – Is the agency’s use of the third-party website or application consistent with all applicable laws, regulations, and policies?

SECTION 2.0 – ANY PII THAT IS LIKELY TO BECOME AVAILABLE TO THE AGENCY THROUGH THE USE OF THE THIRD-PARTY WEBSITE OR APPLICATION

2.1 – What PII will be made available to the agency?

2.2 – What are the sources of the PII?

2.3 – Do the agency’s activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

SECTION 3.0 – THE AGENCY’S INTENDED OR EXPECTED USE OF THE PII

3.1 – Generally, how will the agency use the PII described in Section 2.0?

3.2 – Provide specific examples of the types of uses to which PII may be subject.

SECTION 4.0 – SHARING OR DISCLOSURE OF PII

4.1 – With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

4.2 – What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

SECTION 5.0 – MAINTENANCE AND RETENTION OF PII

5.1 – How will the agency maintain the PII, and for how long?

5.2 – Was the retention period established to minimize privacy risk?

SECTION 6.0 – HOW THE AGENCY WILL SECURE PII

6.1 – Will the agency’s privacy and security officials coordinate to develop methods of securing PII?

SECTION 7.0 – IDENTIFICATION AND MITIGATION OF OTHER PRIVACY RISKS

Section 7.1 – What other privacy risks exist, and how will the agency mitigate those risks?

SECTION 8.0 – CREATION OR MODIFICATION OF A SYSTEM OF RECORDS

Section 8.1 – Will the agency’s activities create or modify a “system of records” under the Privacy Act of 1974?

Introduction

On June 25, 2010, OMB issued Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*.¹ The memorandum requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites or applications to engage with the public. Among other requirements, the memorandum asks agencies to prepare an adapted Privacy Impact Assessment (PIA) that is tailored to address the specific functions of a third-party website or application that is being used. According to the memorandum, the PIA should describe:

- i. the specific purpose of the agency's use of the third-party website or application;
- ii. any PII that is likely to become available to the agency through public use of the third-party website or application;
- iii. the agency's intended or expected use of PII;
- iv. with whom the agency will share PII;
- v. whether and how the agency will maintain PII, and for how long;
- vi. how the agency will secure PII that it uses or maintains;
- vii. what other privacy risks exist and how the agency will mitigate those risks; and
- viii. whether the agency's activities will create or modify a "system of records" under the Privacy Act.

An agency may prepare one PIA to cover multiple websites or applications that are functionally comparable, as long as the agency's practices are substantially similar across each website and application. For example, one PIA may be sufficient to cover an agency's use of multiple social media websites where limited PII is made available to the agency, but none is collected, shared, or maintained. However, if an agency's use of a website or application raises distinct privacy risks, the agency should prepare a PIA that is exclusive to that website or application.

Agencies should consult the memorandum for the full details of the PIA requirement.

Since the release of the memorandum, agencies have been taking steps to comply with the new requirements. In that time, OMB has received only a few requests for clarification. However, because the memorandum issued new requirements that pertain

¹ OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

to agencies' use of new technologies, agencies may benefit from general guidance on the adapted PIA process for third-party websites and applications.

This document – a “model PIA” – provides some tips and examples to help agencies prepare high-quality PIAs for third-party websites and applications. The model does not institute new OMB requirements or modify existing OMB requirements, including those in Memorandum M-10-23. Agencies seeking to understand OMB policies should refer to official OMB memoranda; this document may be consulted as an additional resource.

In using a model PIA, agencies should recognize that all model language is merely illustrative. While a model can serve as a general resource, agencies should not simply adopt the examples in this document for use in the PIA. Rather, agencies should perform a specific, tailored analysis of their use of a website or application, according to the instructions in Memorandum M-10-23. A successful PIA will include greater specificity than is possible in a model of this kind.

Finally, a model PIA for third-party websites and applications cannot function as a static template. As agencies gain experience performing PIAs for their use of these technologies, they are encouraged to contact OMB with suggestions for improving the model. Periodic updates will be considered, as appropriate. As always, OMB stands ready to assist agencies in complying with OMB policies and ensuring that privacy is fully protected across the Federal Government.

SECTION 1.0 – SPECIFIC PURPOSE OF THE AGENCY’S USE OF A THIRD-PARTY WEBSITE OR APPLICATION

1.1 – What is the specific purpose of the agency’s use of the third-party website or application, and how does that use fit with the agency’s broader mission?

The agency should use plain language to disclose the purpose(s) of its use of the third-party websites or applications. The agency’s description should provide enough detail to allow the reader to gain a full understanding of the agency’s purpose(s), while avoiding overly technical jargon.

The purpose(s) of agencies’ use of third-party websites and applications may differ, depending on each agency’s specific mission. An agency may use these technologies to facilitate public dialogue, to provide information about or from the agency, or to improve customer service. These technologies may help an agency make its information and services more widely available. The agency should explain each of its purpose(s) in the context of its specific mission.

1.2 – Is the agency’s use of the third-party website or application consistent with all applicable laws, regulations, and policies?

The President’s January 21, 2009 memorandum on *Transparency and Open Government*² and the OMB Director’s December 8, 2009 *Open Government Directive*³ call on Federal departments and agencies to harness new technologies to engage with the public. These documents may serve as the primary policies underlying the agency’s efforts to use the third-party websites or applications.

The agency should make clear that it will comply with all applicable laws, regulations, and policies, in particular those pertaining to privacy, accessibility, information security, and records management. The agency may wish to provide examples showing how it will comply with these policies. Finally, the agency should indicate that it will work with its counsel to ensure that its use of third-party websites and applications remains compliant.

² President Barack Obama, Memorandum on *Transparency and Open Government* (January 21, 2009), available at <http://www.gpoaccess.gov/presdocs/2009/DCPD200900010.pdf>.

³ OMB Memorandum M-10-06, *Open Government Directive* (December 8, 2009), available at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.

SECTION 2.0 – ANY PII THAT IS LIKELY TO BECOME AVAILABLE TO THE AGENCY THROUGH THE USE OF THE THIRD-PARTY WEBSITE OR APPLICATION

2.1 – What PII will be made available to the agency?

With the degree of variation between third-party websites and applications, it would be impossible to provide a definitive model. Instead, we have provided a few general examples to show the kinds of issues that should be addressed in a PIA. As always, answers should be tailored to address the specific websites and applications being used.

Registration: Many third-party websites or applications request personally identifiable information (PII)⁴ at the time of registration. The process will vary across third-party websites or applications and often users can provide more than is required for registration. For example, users can provide such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown. Agencies should make clear whether they will have access to this information and whether users can take steps to limit agencies' access.

Submission: An individual can make information available to agencies when he or she provides, submits, communicates, links, posts, or associates PII while using the third-party website or application. This can include such activities as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions. Individuals who have accounts with third-party websites or applications may transmit PII through the system during the sign-up/log-on transaction or during subsequent interactions. If PII is posted in a public area or sent to the agency in connection with the transaction of public business, it may become a Federal record.

Association: Even when individuals do not actively post or submit information, they can potentially make PII available to the agency by “associating” themselves with the websites or applications. Such acts of association may include activities commonly referred to as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions. It is also important to recognize that these activities may make information about a user more widely available than is immediately obvious to the user. For example, a user may post information on one third-party website or application that then may be linked to a different third-party website or application, even without the user's knowledge or consent.

⁴ The term “PII,” as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

Accounts: Even individuals who do not have an account with a third-party website or application may make PII available to agencies if certain functions of the website or application are available to individuals without an account. For example, users may transmit PII through the system by commenting on images or videos, or otherwise submitting information. Agencies should make clear whether they will have access to this information and whether users can take steps to limit agencies' access.

2.2 – What are the sources of the PII?

Users may be required to submit PII to the third-party websites or applications at the time of registration. This information is collected and maintained by the third-party websites or applications, but it is also available to the agency in many circumstances. In addition, whenever individuals engage in transactions on the third-party website or application, they may make information available to agencies.

It is important to recognize that the agency may gain access to information in ways that are not obvious to users. For example, in some circumstances the agency may have access to information that an individual communicates to another individual, if the activity is somehow connected with the agency's page or profile.

2.3 – Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

The agency should refer to the April 7, 2010 OMB memorandum entitled, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*⁵ to determine whether the PRA will apply. This determination should be briefly explained.

SECTION 3.0 – THE AGENCY'S INTENDED OR EXPECTED USE OF THE PII

3.1 – Generally, how will the agency use the PII described in Section 2.0?

Once the agency has identified the PII that is likely to be made available through the use of a third-party website or application, the agency should determine whether it will use the PII for any purpose. This is a key decision point in the development of a PIA for a third-party website or application. When an agency makes this determination, it should involve more than a statement of the agency's expectations. The agency will need to address the potential uses of any PII that is likely to become available to the agency. In the event that the agency decides to change these uses after the publication of the PIA, the agency may need to revise their assessment.

In cases where the agency will *not* use any PII, the agency may use a single comprehensive PIA to cover multiple websites or applications. For example, an agency

⁵ OMB Memorandum, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act* (April 7, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/infogeg/SocialMediaGuidance_04072010.pdf

with multiple pages on a social media website may use a single PIA to cover all the pages if none of the PII made available on those pages is used by the agency. Likewise, multiple applications with similar uses may be covered by a single PIA, provided that the privacy, security, and retention issues are sufficiently comparable.

In cases where the agency *will* likely use PII, the agency should consider both current uses of PII made available through third-party websites or applications, as well as potential future uses of the PII. This will provide the public with notice of the agency's future actions, and will prepare the agency to identify and address the full range of privacy risks. For all potential uses of PII, agencies should consider alternative approaches that might help to mitigate these risks. For example, the agency may provide users with the option to use an official agency website in lieu of a third-party website.

3.2 – Provide specific examples of the types of uses to which PII may be subject.

Given the high degree of variation among third-party websites and applications, it would be impossible to provide a definitive model. Instead, we have provided a few general examples to show the kinds of issues that should be addressed in a PIA. As always, answers should be tailored to address the specific websites and applications being used.

Public interaction/open government activities: This could include surveys, contests, or message boards that provide a forum for the public to comment on the agency's activities.

Recruitment and/or employee outreach: In order to recruit and hire from the widest possible pool of candidates, the agency may consider using third-party websites or applications to attract new hires or to inform or receive feedback from current employees.

Participation in agency programs or systems: The agency may consider using third-party websites or applications in order to facilitate access to programs or systems. The agency should consider and address whether this use will result in the PII being combined, matched, or otherwise used in concert with PII that is already maintained by the agency.

Web measurement and/or customization: The agency may use third-party websites or applications to conduct measurement and analysis of web usage, or to customize the user's experience. Whenever the agency uses web measurement or customization technologies, the agency should consult the June 25, 2010 OMB memorandum, *Guidance for Online Use of Web Measurement and Customization Technologies*.⁶

SECTION 4.0 – SHARING OR DISCLOSURE OF PII

⁶ OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf

4.1 – With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

The agency should describe all the entities to which any PII may be disclosed, and explain the specific authority for each type of disclosure. In addition, the agency should explain how any disclosure will comply with applicable laws, regulations, and policies. The agency should describe any expected dissemination activities and discuss any circumstances in which PII is likely to be disclosed through the agency’s activities.

4.2 – What safeguards will be in place to prevent expansion of uses beyond those authorized under law and described in this PIA?

The agency should describe the safeguards that are established to ensure that PII is used only as permitted by law. In addition, the agency should describe the safeguards that are established to ensure that the agency’s uses of PII do not exceed or differ from the precise uses described in the PIA.

SECTION 5.0 – MAINTENANCE AND RETENTION OF PII

5.1 – How will the agency maintain the PII, and for how long?

The agency should describe how it will maintain PII and precisely how long PII will be retained. In addition to conventional retention methods, such as inclusion in a system of records, the agency should explain any less formal methods that it may adopt. For example, if agency decides to copy individual comments into a document or database, the agency should make that clear.

5.2 – Was the retention period established to minimize privacy risk?

Retention standards and requirements should be officially established for any PII that is maintained by the agency, in compliance with applicable laws, regulations, and policies. The agency should describe these standards and explain why they were adopted.

SECTION 6.0 – HOW THE AGENCY WILL SECURE PII

6.1 – Will the agency’s privacy and security officials coordinate to develop methods of securing PII?

The agency should consult the government-wide policies that pertain to information security, such as those of NIST, OMB, and the CIO Council. For example, NIST recommends that organizations take steps to protect their PII, including the following:

Encourage close coordination among chief privacy officers, senior agency officials for privacy, chief information officers, chief

information security officers, and legal counsel when addressing issues related to PII. To protect the confidentiality of PII effectively, organizations need a comprehensive understanding of their information systems, information security, privacy, and legal requirements. Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with the organization's legal counsel and privacy officer since the laws, regulations, and other mandates are often complex and may change over time.

Also, new technical security controls may be needed to implement and enforce new security policies that are adopted. Close coordination of the organization's technical and legal experts helps to prevent incidents that could result in the compromise and misuse of PII by ensuring proper interpretation and implementation of requirements. ”⁷

The CIO Council also recommends that the agency's privacy and security components work together to protect PII in such uses: “The decision to authorize access to social media websites is a business decision, and comes from a risk management process made by the management team with inputs from all players, including the CIO, CISO, Office of General Counsel (OGC), privacy official and the mission owner.”⁸

The agency should use plain language to describe the basic methods that it will use to secure any PII that it uses or maintains. In particular, the agency should describe how it will limit access to the PII, whether and how it will use encryption or other technical methods of securing the PII, and what steps it will take to reduce the volume of PII to the minimum necessary to accomplish the agency's purposes.

SECTION 7.0 – IDENTIFICATION AND MITIGATION OF OTHER PRIVACY RISKS

Section 7.1 – What other privacy risks exist, and how will the agency mitigate those risks?

With the degree of variation between third-party websites and applications, it would be impossible to provide a definitive model. Instead, we have provided a few general examples to show the kinds of issues that should be addressed in a PIA. As always, answers should be tailored to address the specific websites and applications being used.

⁷ NIST ITL Bulletin April 2010 GUIDE TO PROTECTING PERSONALLY IDENTIFIABLE INFORMATION

⁸ CIO COUNCIL - Guidelines for Secure Use of Social Media by Federal Departments and Agencies Version 1.0 September 2009

Disclosure of PII by users. When interacting with the agency or others on a third-party website, PII that users share or disclose may become available to other users or any individuals with access to the site. In order to mitigate the risks of disclosure, the agency may choose to delete or hide comments or other user interactions when a user's sensitive information is included. The agency's employees and contractors should be trained and instructed not to solicit sensitive information when interacting with users on behalf of the agency. Where possible, the agency should also provide appropriate notice to users on the third-party site itself, warning individuals to avoid sharing or disclosing any sensitive PII when interacting with the agency on the site.

Third-party advertising and tracking. A third-party website may display advertising or other special communications on behalf of other businesses or organizations. If the user clicks on the advertisement or reads the communication to learn about the advertised product or service, the user's PII may be shared by the website operator with the advertiser. The user's actions may also initiate tracking technology (e.g., "cookies," "web bugs," "beacons"), enabling the website operator or advertiser to create or develop a history or profile of the user's activities. In addition, where possible, the agency should provide appropriate notice to users on the third-party website itself, warning them about the privacy issues raised by such advertising and tracking technology.

Spam, unsolicited communications, spyware, and other threats. Users may receive spam or other unsolicited or fraudulent communications from a third party as a result of their interactions with the agency on the website. To avoid harm, users should be wary of responding to such communications, particularly those that may solicit the user's personal information. Users should also avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded. These unsolicited links and applications can contain unwanted tracking technology as well as computer viruses or other malicious payloads that can pose a variety of risks to the user. Where possible, the agency should provide warnings about these risks in a notice to users on the third-party website itself.

Accounts or pages that misrepresent agency authority or affiliation. Certain accounts or pages on the website may not be officially authorized by, or affiliated with, the agency, even if they use official insignia or otherwise appear to represent the agency or the Federal Government. Interacting with such unauthorized accounts or pages may expose users to many of the privacy or security risks described above. The agency should make every reasonable effort to label or identify its account or page in ways that would help users distinguish it from any unauthorized accounts or pages. The agency should also, where appropriate, inform the website operator about any unofficial accounts or pages purporting to represent the agency, seek their removal, and warn users about such accounts or pages. In addition, the agency's account or page should explain that the agency does not own, operate, or control the host website, and should provide users with a direct link to the agency's official website.

External links and embedded third-party applications. If the agency posts a link that leads to a third-party website or any other location that is not part of an official

government domain, the agency should provide notice to the user to explain that users are being directed to a nongovernment website that may have different privacy policies (and risks) from those of the agency's own official website. Likewise, if the agency incorporates or embeds a third-party application, separate from any applications that may be incorporated or embedded by the website operator itself, the agency should disclose and explain the nature or extent, if any, of the third party's involvement in the agency's use of the application(s). The agency should also describe the use of these application(s) in the agency's own privacy policy.

Monitoring future requirements and future technology. In addition to the measures described above, the agency should establish and maintain procedures to identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations, or policies. The agency should also monitor new technologies, consider new risks that may emerge, and look for new approaches to protecting privacy.

Monitoring the third-party website's privacy policies. The agency should make clear that they have examined the third-party website's privacy policy and have determined that the website is appropriate for the agency's use. To the extent practicable, the agency should monitor any changes to the third party's privacy policies and periodically reassess the risks.

SECTION 8.0 – CREATION OR MODIFICATION OF A SYSTEM OF RECORDS

Section 8.1 – Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

The agency should determine whether its use of the third-party website or application will involve any records that are subject to the requirements in the Privacy Act of 1974. This determination will depend on a careful evaluation of the agency's activities. For general guidance on the applicability of the Privacy Act, agencies may consult OMB guidance, as well as the Department of Justice's *Overview of the Privacy Act of 1974* (2010 ed.) (U.S. Department of Justice, Office of Privacy and Civil Liberties).