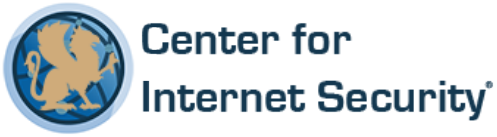
Toward A Privacy Impact Assessment (PIA)

Companion to the

CIS Critical Security Controls *Version 6.0*



October 2015

Table of Contents

A Privacy Impact Assessment (PIA) for the CIS Critical Security Controls

Introduction

An effective posture of enterprise cybersecurity need not, and, indeed, should not compromise individual privacy. Many laws, regulations, guidelines, and recommendations exist to safeguard privacy, and enterprises will, in many cases, adapt their existing policies on privacy as they apply the Center for Internet Security Critical Security Controls for Cyber Defense Version 6.0

At a minimum, use of the CIS Controls should conform to the general principles embodied in the *Fair Information Practice principles* (FIPs) [1] and in *Privacy by Design.*[2] All enterprises that apply the CIS Controls should undertake – and make available to stakeholders – privacy impact assessments of relevant systems to ensure that appropriate protections are in place as the CIS Controls are implemented. Every enterprise should also regularly review these assessments as material changes to its cybersecurity posture are adopted. The aim is to assess and mitigate the major potential privacy risks associated with implementing specific CIS Controls as well as evaluate the overall impact of the Controls on individual privacy.

To assist enterprises in efforts to conduct a privacy impact assessment when implementing the CIS Controls and to contribute to the establishment of a more general reference standard for privacy and the Controls, CIS will convene technical and privacy experts to review each Control and offer recommendations for best practice.

The following framework will help guide this effort and provide a possible outline for a Privacy Impact Assessment.

Privacy Impact Assessment of the CIS Critical Security Controls

I. Overview

Outline the purpose of each Control and provide justification for any actual or potential intersection with privacy-sensitive information.

---

[1] See http://www.dhs.gov/publication/fair-information-practice-principles-fipps, and http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[2] See https://www.privacybydesign.ca. The approach discussed in this Annex draws heavily on public sector approaches in the United States, but can be adapted for any jurisdiction.

- Where possible, identify how technologies, procedures, and data flows are used to implement the Control. Provide a brief description of how the Control generally collects and stores information. Identify the type of data collected by the Control and the kinds of information that can be derived from this data. In discussing how the Control might collect and use PII, include a typical transaction that details the life cycle of that PII from collection to disposal.
- Describe the measures necessary to protect privacy data and mitigate any risks of unauthorized access or inadvertent disclosure of the data. The aim here is not to list every possible risk to privacy, but rather, to provide a holistic view of the risks to privacy that could arise from implementation of the Control.
- Describe any potential ad-hoc or routine information sharing that will result from the implementation of the Control both within the enterprise and with external sharing partners. Also describe how such external sharing is compatible with the original collection of the information, and what agreements would need to be in place to support this sharing.

II. Authorities

Identify the legal authorities or enterprise policies that would permit or, conversely, limit or prohibit the collection or use of information by the Control.

- List the statutory and regulatory authorities that would govern operation of the Control, including the authorities to collect the information identified above. Explain how the statutory and regulatory authorities permit or would limit collection and use of the information or govern geographic storage requirements. If the Control would conceivably collect Personally Identifiable Information (PII), also identify the specific statutory authority that would permit such collection.
- Would the responsible office of an enterprise be able to rely on authorities of another parent organization, subsidiary, partner or agency?
- Might the information collected by the Control be received from a foreign user, organization or government? If so, do any international agreement, contract, privacy policy or memorandum of understanding exist to support or otherwise govern this collection?

III. Characterizing Control-Related Information

Identify the type of data the Control collects, uses, disseminates, or maintains.

- For each Control, identify both the categories of technology sources, logs, or individuals from whom information would be collected, and, for each category, list any potential PII, that might be gathered, used, or stored to support the Control.
    - Relevant information here includes (but is not limited to): name; date of birth; mailing address; telephone numbers; social security number; e-mail address; mother's maiden name; medical records locators; bank account

numbers; health plan beneficiaries; any other account numbers; certificates or other license numbers; vehicle identifiers, including license plates; marriage records; civil or criminal history information; medical records; device identifiers and serial numbers; education records; biometric identifiers; photographic facial images; or any other unique identifying number or characteristic.

- If the output of the Control, or system on which it operates, creates new information from data collected (for example, a scoring, analysis, or report), this might this new information have privacy implications? If so, perform the same above analysis on the newly created information.
- If the Control uses information from commercial sources or publicly available data to enrich other data collected, explain how this information might be used.
    - Commercial data includes information from data aggregators (such as Lexis Nexis, threat feeds, or malware databases), or from social networking sources where the information was originally collected by a private organization.
    - Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.
    - Identify scenarios with this enriched data might derive data that could have privacy implications. If so, perform the same above analysis on the newly created information.
- Identify and discuss the privacy risks for Control information and explain how they are mitigated. Specific risks may be inherent in the sources or methods of collection.
- Consider the following Fair Information Practice principles (FIPs):
    - *Principle of Purpose Specification:* Explain how the collection of PII by the Control links to the cybersecurity needs of the enterprise.
    - *Principle of Minimization:* Is the PII data directly relevant and necessary to accomplish the specific purposes of the Control?
    - *Principle of Individual Participation:* Does the Control, to the extent possible and practical, collect PII directly from individuals?

IV. Uses of Control-Related Information

Describe the Control's use of PII or privacy protected data. Describe how and why the Control uses this data.

- List likely uses of the information collected or maintained, both internal and external to the enterprise. Explain how and why different data elements will be used. If Social Security numbers are collected for any reason, for example, describe why such collection is necessary and how such information would be used. Describe types of procedures and protections to be in place to ensure that information is handled appropriately, and policies that need to be in place to provide user notification.

- Does the Control make use of technology to conduct electronic searches, queries, or analyses in a database to discover or locate a predictive pattern or an anomaly? If so, describe what results would be achieved and if there would be possibility of privacy implications.
- Some Controls require the processing of large amounts of information in response to user inquiry or programmed functions. The Controls may help identify data that were previously not identifiable and may generate the need for additional research by analysts or other employees. Some Controls are designed to perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.
- Discuss the results generated by the uses described above, including link analysis, scoring, or other analyses. These results may be generated electronically by the information system, or manually through review by an analyst. Would these results potentially have privacy implications?
- Are there other offices or departments within or connected to the enterprise that would receive any data generated? Would there be privacy implications to their use or collection of this data?
- Consider the following FIPs:
    - *Principle of Transparency:* Is the PIA and related policies clear about the uses of information generated by the Control?
    - *Principle of Use Limitation*: Is the use of information contained in the system relevant to the mission of the Control?

V. Security

Complete a security plan for the information system(s) supporting the Control.

- Is there appropriate guidance when implementing the Control to ensure that appropriate physical, personnel, IT, and other safeguards are in place to protect privacy protected data flowing to and generated from the Control?
- Consider the following Fair Information Practice principle:
    - *Principle of Security*: Is the security appropriate and proportionate to the protected data?

VI. Notice

Identify if any notice to individuals must be put in place regarding implementation of the Control, PII collected, the right to consent to uses of information, and the right to decline to provide information (if practicable).

- Define how the enterprise might require notice to individuals prior to the collection of information.
- Enterprises often provide written or oral notice to employees, customers, shareholders, and other stakeholders before they collect information from

individuals. In the U.S. government, that notice may include a posted privacy policy, a Privacy Act statement, a Privacy Impact Assessment, or a Statement of Records Notice (SORN) published in the *U.S. Federal Register*. For private companies, collecting information from consumers, publicly available privacy policies are used. Describe what notice might be relevant to individuals whose information might be collected by the Control.

- If notice might not, or cannot be provided, define if one is required or how it can be mitigated. For certain law enforcement operations, notice may not be appropriate – enterprises would then explain how providing direct notice to the individual at the time of collection would undermine a law enforcement mission.
- Discuss how the notice provided corresponds to the purpose of the Control and the declared uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how implementation of the Control mitigates the risks associated with potentially insufficient notice and opportunity to decline or consent.
- Consider the following FIPs:
    - *Principle of Transparency*: Will this Control allow sufficient notice to be provided to individuals?
    - *Principle of Use Limitation:* Is the information used only for the purpose for which notice was provided either directly to individuals or through a public notice? What procedures can be put in place to ensure that information is used only for the purpose articulated in the notice?
    - *Principle of Individual Participation*: Will the enterprise be required to provide notice to individuals regarding redress, including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

VII. Data Retention

Will there be a requirement to develop a records retention policy, subject to approval by the appropriate enterprise authorities (e.g., management, Board), to govern information gathered and generated by the Control?

- Consider the following FIPs below to assist in providing a response:
    - *Principle of Minimization:* Does the Control have the capacity to use only the information necessary for declared purposes? Would the Control be able to manage PII retained only for as long as necessary and relevant to fulfill the specified purposes?
    - *Principle of Data Quality and Integrity:* Does the PIA describe policies and procedures required by an organization for how PII is purged once it is determined to be no longer relevant and necessary?

VIII. Information Sharing

Describe the scope of the information sharing within and external to the enterprise that could be required to support the Control. External sharing encompasses sharing with other businesses, vendors, private sector groups, or federal, state, local, tribal, and territorial government, as well as with governments or official agencies of other countries.

- For state or local government agencies, or private sector organizations list the general types that might be applicable for the Control, rather than the specific names.
- Describe any agreements that might be required for an organization to conduct information sharing as part of normal enterprise operations.
- Discuss the privacy risks associated with the sharing of information outside of the enterprise. How can those risks be mitigated?
- Discuss how the sharing of information is compatible with the stated purpose and use of the original collection for the Control.

IX. Redress

Enterprises should have in place procedures for individuals to seek redress if they believe their PII may have been improperly or inadvertently disclosed or misused through implementation of the Controls. These procedures may include allowing them to file complaints about what data is collected or how it's used.

- Consider the following issue that falls under the FIP principle of *Individual Participation*:
    - Can a mechanism be applied by which an individual can prevent PII obtained for one purpose from being used for other purposes without the individual's knowledge?

X. Auditing and Accountability

Describe what technical and policy based safeguards and security measures might be needed to support the Control. Include an examination of technical and policy safeguards, such as information sharing protocols, special access restrictions, and other controls.

- Discuss whether the Control allows for self-audits, permits third party audits, or allows real time or forensic reviews by appropriate oversight agencies.
- Do the IT systems supporting the Control have automated tools to indicate when information is possibly being misused?
- Describe what requirements for privacy training should be provided to users either generally or specifically relevant to the Control, including information handling procedures and sensitivity of information. Discuss how individuals who have access to PII collected or generated by the Control should be trained to appropriately handle that information.

- Discuss the types of processes and procedures necessary to review and approve information sharing agreements, new uses of Control information, and new access to Control information by other parties.