PIAs Provide Privacy Purview

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Final Draft for December 2009 CSI Alert

PIAs: Not A 70's Actress!

I am a huge proponent of privacy impact assessments (PIAs); basically risk assessments for privacy. Since the beginning of the current millennium I've been performing PIAs, and I use the term frequently. In fact, I use it so often I sometimes say "PIA" without first clearly defining the term. So, to remove all speculation, when you hear someone discussing a PIA, they are most likely not talking about a group of uniquely-named women, but they are more likely talking about a process to review the privacy concerns that exist within a specified scope, and then provide recommendations for how to address and mitigate, or more preferably remove, the privacy risks that are revealed through the process.

The Value Of PIAs

PIAs provide many benefits to an organization. They can be used to do things such as:

- Reveal the specific types of personal information items involved within the PIA scope. This helps tremendously with creating and maintaining a personal information inventory.
- Identify laws, regulations, industry standards, contractual and policy requirements for protecting personal information
- Show the data flows and paths for personal information, from collection, to storage, access, use, sharing, throughout the entire data lifecycle to retention and destruction.
- Highlight gaps in privacy practices, along with the information security practices used to protect personal information specifically and privacy in general.
- Determine the impacts of making changes to privacy policies on websites.
- Reveal the privacy vulnerabilities and threats that will exist as a result of a merger or divestiture.
- And many, many other types of situations that involve personal information.

PIAs can give organizations a view into the privacy posture within the entire enterprise, within specific applications, within information exchanges, within specific business operations, or within any scope you want to look at to determine the privacy risks. PIAs are important and effective exercises for all organizations that handle personal information of all kinds.

Examples: U.S. Government Agency PIAs

U.S. government agencies have had to do annual PIAs, and post the results publicly, for the past several years under the E-Government Act of 2002. If you review the posted PIA summaries posted at the many government agency sites, you will see a great variation in quality and quantity of information provided within them. Let's focus for now upon the Department of Homeland Security (DHS).

In the first half of 2007 the U.S. Department of Homeland Security (DHS) made available 14 PIA reports for projects that "collectively contain tens of millions of personal records concerning immigration and travel."[1] The PIAs went beyond the IT issues, as all PIAs should; they addressed the privacy impacts related to paper, spoken and other non-IT PII. These referenced DHS PIAs can serve as great case studies not only for establishing your own PIA processes, but also for your information security and privacy awareness and training programs.

PIA Results Get Attention And Spur Changes

Reviewing PIAs not only give you important information about the actions being done to preserve privacy and help to perform your own PIAs, they also help to demonstrate good privacy practices, reveal poor privacy practices, and demonstrate due diligence.

Starting in late June of this year I led a high-level PIA of the proposed consumer-to-utility portion of the U.S. utilities smart grid as part of volunteer work I'm doing for the NIST Smart Grid Privacy Subgroup to help them identify privacy concerns with the Smart Grid plans. A portion of that PIA report was published within "DRAFT NISTIR 7628: Smart Grid Cyber Security Strategy and Requirements" (See the full report at http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf). The first draft of the PIA report I provided to NIST in September was 22 pages long. However, after NIST got through doing their edits to make the report fit in with their full report of security and other issues, the amount included within the first draft of the NISTIR only 7 pages long. I am now working diligently to get not only the cut sections incorporated back into the report for the 2nd draft of the NISTIR, but also to include additional information about privacy concerns, proposed privacy standards, applicable laws and regulations that exist for data throughout the entire smart grid, and, hopefully, get included an idea I have and am promoting for establishing a privacy certification for organizations that are part of the smart grid.

Even though the full PIA was not included in the first draft of the NISTIR, and comprised a relatively small portion of the full NISTIR report, it definitely made an impact on some influential and powerful government leaders. In fact, when the NISTIR was released on September 24, 2009, U.S. Commerce Secretary Gary Locke included the following statements[2] within his prepared release about the smart grid:

- “*The major benefit provided by the Smart Grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles’ heel from a privacy viewpoint. Privacy advocates have raised serious concerns about the type and amount of billing and usage information flowing through the various entities of the Smart Grid…that could provide a detailed time-line of activities occurring inside the home.”*
- *“There is a lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility*

[1] For more information see http://www.gcn.com/online/vol1_no1/44880-1.html.

[2] For the full release containing the statements from Secretary Locke see http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf

> *companies, and supporting entities that will be involved with Smart Grid management and information collection and use which creates a very significant privacy risk that must be addressed.*"

Indeed, a well-constructed, comprehensive and effectively communicated PIA report will catch the attention of key leaders and decision-makers, as well as illuminate critical privacy issues.

Reasons To Do PIAs

In general, PIAs serve the great purpose of giving business leaders a view into the privacy practices of their organization. There are many more specific reasons for you to do PIAs within your organization. Here are just a few; I could go on for several pages.

Effective and consistently performed PIAs:

- Are increasingly legally required through growing numbers of laws, regulations, and contracts.
- Provide a way to establish and maintain a personal information inventory and personal information data flow diagrams.
- Clearly identify within the PIA scope:
    - The personal information that is collected
    - Why the personal information needs to be collected
    - The intended use of the collected information
    - With whom the information will be shared
    - The notice or opportunities for consent that are provided to individuals regarding the corresponding personal information about them and how that information is shared
    - How the information will be secured
- Provide information that allows you to prioritize your activities to most appropriately address privacy concerns.
- Reveal vulnerabilities that allow you to mitigate or eliminate them before bad things happen.
- Establish documentation that demonstrates you did everything you reasonably could to prevent those bad things when they happen any way, such as security incidents or privacy breaches.
- Help participants learn more about the business and how personal information is handled.
- Help identify ways to improve business processes to improve privacy.
- Help to build a program based upon mitigating privacy risk.
- Reveal gaps in current personal information controls and processes.
- Show where information security and privacy programs need updating to meet compliance as well as reduce risks.

I hope you seriously consider including PIAs into your information security and privacy compliance program. I've been addressing information security, privacy and compliance issues for over two decades, and I can tell you that PIAs are just as important for providing a revealing and valuable view of privacy risks and addressing compliance as information security risk assessments are for revealing security risks and meeting security requirements.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, The Privacy Professor ®, is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. See more about her services and awareness and training products at http://www.privacyguidance.com. She can be reached at rebeccaherold@rebeccaherold.com.