CASE STUDY #1:

Are Privacy Impact Assessments (PIA) Useful as a Policy Tool?

DeBora King
CSIA 360 7980
Cybersecurity in Government Organizations (2172)
March 19, 2017

INTRODUCTION

The world of invasion of privacy hasn't changed much. In 2016, the Democratic National Committee (DNC) experienced email hacking by the Russians (Nakashima, 2016). Similarly, in 1972, five men physically broke into DNC offices – this was called the Watergate scandal (Maranzani, 2017). In both cases the offenders had the intent of gathering and exposing unauthorized information. The latter incident sparked concerns of government officials who saw the need to bring about the Privacy Act of 1974. With the increased use of technology, congress wanted to mitigate against abuses of power and protect the personal data of individuals. They wanted to implement regulation for the collection, maintenance, use, and dissemination of personal information by government agencies (DOJ, 2015). The Office of Management and Budget (OMB) is accountable to the Privacy Act. The act focuses of the following objectives: 1) to restrict disclosure of personally identifiable records maintained by agencies; 2) to grant individuals increased rights of access to agency records maintained on themselves; 3) to grant individuals the right to see amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete; and 4) to establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records. With the progression of technology, the E-Government Act of 2002 went into effect in order to protect personal identifiable information (PII) that the government contains in their records and systems (DOJ, 2014). Privacy Impact Assessments (PIA) is a requirement of Section 208 of the E-Government Act. This mandate supports that the procurement or development of new information technology by government agencies which encompass implementing or altering the collection, maintenance, or dissemination citizens' PII must have a PIA. The collection, storage, protection, and sharing of information by government owners and developers is a key component in developing a

PIA. In compliance with the E-Government Act, the government agency's PIA must be published and available publicly.

CONTENTS OF PRIVACY IMPACT ASSESSMENTS

The government is made up of many bureaucracies that include departments, independent agencies, independent regulatory commissions and government corporations (ThisNation.com, n.d.). The State Department's contents are as follows (United States Department of State, PIA Template Version 1.0, 4/2013):

1. Contact Information
2. System Information
    a. Date completed
    b. Name of system
    c. System acronym
    d. IT Asset Baseline (ITAB) number
    e. System description
        i. Scope
        ii. Purpose
        iii. Major functions
3. Characterization of the Information (first determining whether it contains PII)
    a. Elements of PII collected and maintained by the system and sources of that information
    b. How is information collected?
    c. Why is the information collected and maintained?
    d. How will information be checked for accuracy?

   e. What specific legal authorities, arrangements, and/or agreements define the collection of information?
   f. Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

4. Uses of Information
   a. Describe all uses of the information.
   b. What types of methods are used to analyze the data? What new information may be provided?
   c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.
   d. Are contractors involved in the uses of the PII?
   e. Describe the types of controls that may be in place to ensure that information is handled in accordance with the above users.
5. Retention
   a. How long is information retained?
   b. Discuss the risks associated with the duration that data is retained and how those risks are mitigated.
6. Internal Sharing and Disclosure
   a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?
   b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?
   c. Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

7. External Sharing and Disclosure
    a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?
    b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?
    c. Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.
8. Notice (it is determined whether PIA contains information covered by the Privacy Act)
    a. Is notice provided to the individual prior to collection of their information?
    b. Do individuals have the opportunity and/or right to decline to provide information?
    c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?
    d. Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.
9. Notification and Redress
    a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?
    b. Discuss the privacy risks associated with notification and redress and how those risks are mitigated.
10. Controls on Access
    a. What procedures are in place to determine which users may access the system and the extend of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?
    b. What privacy orientation of training for the systm is provided authorized users?

c. Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

b. Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

12. Security

a. What is the security assessment and authorization (A&A) status of the system?

The PIA content listed above by the State Department is an ideal guideline for many other agencies that may have little experience producing such documentation. Agencies that have PIAs similar to the format of the State Department (2013) include the Department of Interior (n.d.), the United States Department of Agriculture (2013), the Department of Health and Human Services (2017), the Department of Housing and Urban Development (2003), the Department of Transportation (2017), the Department of Education (2017), and the Department of Homeland Security (2015). The Treasury Department's PIA (2011) is along the same lines, and other agencies that collect a mass amount of PII and they assess how data is being used includes financial institutions, FedWire Securities Services, the Internal Revenue Service, Social Security Administration, Courts and Law Enforcement entities. The Department of Defense (n.d.) uses a thorough instruction form that includes the Department of Navy, Department of Air Force, and Department of Army. The Department of Justice (2012) also has an official guideline that outlines the Office of Privacy and Civil Liberties' role, what a PIA is, when it should be completed, who should prepare it and what the E-Government Act requires in preparing the documentation. Like many other agencies, the Department of Energy (n.d.) also uses a template and guidance. The Department of Commerce (n.d.) uses a PIA flowchart.

ANALYSIS OF PRIVACY IMPACT ASSESSMENTS

In this case study, we have examined what a PIA means and the rules and regulations that lead to the need for government transparency in the care and control of personal information. There are many resources that support government agencies in the preparation of PIA documents. But PIA documents alone are not effective tools for protecting personal information. PIA documentation couldn't stop over 67,000 federal security breaches in 2014 (Virtru, 2015). PIA documentation could not deter the Department of Veterans Affairs to be hacked, exposing servicemen and servicewomen's social security numbers, family information, disability ratings, medical information and birthdates. Although PIAs do not solve the entire problem of perils dealing with the maintenance and storage of citizen's personal information, the mandate does require a process to insure procedure and process are followed – perhaps in the process mitigating against data security breaches. PIAs also gives the public the ability to see what's happening with their own data. This helps with accountability because with information being public, individuals and organizations can advocate for how this data is handled should they object to any portion of the agency's documentation.

BEST PRACTICES

Best practices for federal government IT managers who are charged with preparing a PIA include the following:

- Determine if an when a PIA is required of the agency represented.
- Collaborating and communicating with key personnel and stakholders including legal counsel, record managers responsible for safeguarding data.
- Utilizing resources at other government agencies and reaching out to obtain helpful information from agencies with PIA experience.
- Following templates and guidelines outlined in the previous section. There are a vast amount of information available from many government agencies.

- It is important that personal information is updated accurate and handled properly. Having a team that insures this is vital to the maintenance and protection of PII.
- Following a lifecycle development helps the PIA documentation process, as many inquiries are answered by following such guidelines.
- Maintaining proper training, software audits, risk analysis in addition to mitigating against data breaches is another best practice that will be helpful to government IT managers.

References:

Nakashima, E. (2016, December 22). Cybersecurity firm finds evidence that Russian military unity was behind DNC hack. Retrieved from https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?utm_term=.5320cb03e42b

Maranzani, B. (2017, March 7). How Watergate changed America's intelligence laws. History. Retrieved from http://www.history.com/news/how-watergate-changed-americas-intelligence-laws

The United States Department of Justice. (2015). Overview of the Privacy Act of 1974. Retrieved from https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition

The United States Department of Justice. (2014, June 18). E-Government Act of 2002. Retrieved from https://www.justice.gov/opcl/e-government-act-2002

This Nation.com. (n.d.). The Realities of Bureaucracy. Retrieved from http://www.thisnation.com/textbook/bureaucracy-reality.html

United States Department of State privacy impact assessment (PIA) template version 1.0, 4/2013. Retrieved from https://www.state.gov/documents/organization/242249.pdf

Federal Personnel and Payroll System (FPPS) Major Application (MA) Department of the Interior privacy impact assessment. (n.d.) Retrieved from https://www.doi.gov/sites/doi.gov/files/migrated/ocio/information_assurance/privacy/upload/FPPS_FEB10.pdf

USDA privacy impact assessment. (2010, March). Revision: 1.2. Retrieved from https://www.usda.gov/sites/default/files/documents/ACFO_ACRWS_PIA.pdf

HHS.gov. (2017). Privacy impact assessment. Retrieved from https://www.hhs.gov/pia/

U.S. Department of Housing and Urban Development. (2003, September). Preliminary privacy impact assessment. Retrieved from https://portal.hud.gov/hudportal/HUD?src=/program_offices/officeofadministration/privacy_act/pia/pat

U.S. Department of Transportation. (2017). Privacy impact assessments. Retrieved from https://www.transportation.gov/individuals/privacy/privacy-impact-assessments

U.S. Department of Education. (2017). Privacy impact assessments. Retrieved from https://ed.gov/notices/pia/index.html#FSA

Department of Homeland Security. (2015, August 24). Privacy impact assessment. Retrieved from https://www.dhs.gov/privacy-impact-assessments

Bureau of Public Debt United States Department of the Treasury. (2011, September 30). TreasuryDirect Privacy Impact Assessment (PIA). Retrieved from https://www.treasurydirect.gov/TreasuryDirectPrivacyImpactAssessment.pdf

U.S. Department of Defense. (n.d.). DOD component privacy ampact assessments. Retrieved from http://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments/

Department of Justice. (2012, March). Privacy Impact Assessments official guidance. Retrieved from https://www.justice.gov/opcl/docs/2012-doj-pia-manual.pdf

Energy.gov. (n.d.). Privacy impact assessment template and guidance. Retrieved from https://energy.gov/cio/downloads/privacy-impact-assessment-template-and-guidance

Department of Commerce privacy impact assessment (PIA) flowchart. (n.d.). Retrieved from http://www.osec.doc.gov/opog/privacy/PIA%20Process%20final.pdf

Virtru. (2015, September 23). 5 data security challenges faced by government agencies and what they can do about it. Retrieved from https://www.virtru.com/blog/data-security/