WHITE PAPER

Can We Ensure That Open Data is Useful AND Secure?

DeBora King

CSIA 360 7980

Cybersecurity in Government Organizations (2172)

March 26, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

The purpose of this white paper is to address concerns for the planned conversion from controlled distribution of highly valuable datasets that are in high demand. Currently the information is in DVD form obtained through the Government Printing Office. The objective is to convert the data to an Open Data delivery method via the Data.Gov portal website. First, we must address the laws, regulations and policy requirements for agencies to identify, publish, and collect information. This document will also highlight the benefits of Open Data in the public and private sector. The following items will be addressed to alleviate concerns insuring businesses and academic institutions are able to access datasets for their intended purpose: 1) confidentiality/privacy (ensuring proper redaction); 2) data integrity; 3) data authenticity; 4) availability (reliability) of the Open Data service (website); and 5) non-repudiation of datasets. Also, best practices with datasets for each of these items while using the Open Data distribution method will be provided.

OPEN DATA LAWS, REGULATIONS & POLICIES

Laws, regulations and policies help government agencies build their framework. For example, the Privacy act of 1974 mandates that agencies show their systems records to the public in the Federal Register (Department of Justice, 2015); under the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), it is mandated that information supplied under the pledge of confidentiality shall be used for its intended purposes (Schildkraut, 2003); and the Family Educational Rights and Privacy Act (FERPA) protects the privacy of students' educational records (U.S. Department of Education, n.d.). The following guidelines for federal agencies will address open data policy and will help determine what data should be

public, how to make data public and how to implement policy according to the executive branch's Open Data/Open government policies making data available via Data.Gov.

What Should be Public

Proactive and reactive disclosure of some government agency information is necessary in keeping with the following policies: Right-to-Know Act of 1986 (EPA, n.d.), Freedom of Information Act (FOIA) of 2007 (U.S. Department of State, n.d.), and state public records laws. Proactive disclosure is having information readily available online, and reactive disclosure is when a request is made and the agency responds. Data accessed by the public must be continually updated and improved according to policy. The key to insuring legal right to government information is strongly building on law and policy to support and defend public access. A specific goal to bridge government and community helps the objective of Open Data, such as enhancing the good of citizenship, heightened transparency of government, and increased accountability, efficiency, community involvement and economic growth. An inventory of the data should be determined and made public. Appointing an oversight person(s) will ensure perpetual maintenance and accuracy. Prioritization of datasets must be established prior to publication, and sensitive data information must be safeguarded (Sunlight Foundation, 2012).

How to Make Data Public

The following resources are excellent tools to follow government law and policy:

1) **The Open Data Handbook** is an excellent tool. The guide is defined as "discusses the legal, social and technical aspects of Open Data" (Open Data Handbook, n.d.).
2) Although not a direct statement of government policy, **The Power of Information** (Mayo and Steinberg, 2007) is a helpful resource. It discusses changes in the use and

availability of information, the importance of the changes, challenges facing government, it explores new opportunities, defines improved access to public sector information, and the protection of public interest.

3) The **8 Principles of Open Government Data** (Opengovdata.org, n.d.) outlines considerations, many derivative of items from White House M-13-13 (2013), about the way data should be made public as follows:
    a. **Complete** – Data made available that is not limited to privacy, security and/or privilege.
    b. **Primary -** the granularity of data and that it must be collected at the source.
    c. **Timely** – supports quick availability in the preservation of the data's value.
    d. **Accessible** – reaching the broadest audience for the broadest purposes.
    e. **Machine Processable** – reasonably formatting for ease of accessibility.
    f. **Non-discriminatory** – access to all free of identification requirements, such as registration.
    g. **Non-proprietary** – free of exclusive control.
    h. **License-free** – copyright, patent, trademark, trade security regulation does not apply (with the exception of privacy, security or privilege restrictions).
4) **Open Government Data: The Book** (2014) focuses on civic hacking and government data, the creation of GovTrack.us, applications for open government, legal history of open government, principals of open government data, case studies, paradoxes in open government, and gives examples of policy language.

How to Implement Policy

Creating an oversite authority to facilitate following regulations and guidelines will help maintain reliability and data standards. This authority may also be responsible for ensuring data quality and conduct the review and maintenance of any changes or new policies (Sunlight Foundation, 2012).

BENEFITS OF OPEN DATA

The Open Data policy brings about many benefits to the general public whether in the community or business. In this section are examples of how government provided Open data is being used to benefit these entities.

Benefits in Advocacy for Quality Education

Sandra Moscoso is a Washington, DC resident who was looking for a way to gather information about what services were available in surrounding public schools, including if the school had a librarian. Not only was she interested for her two children, but she also wanted the convenience to be available to all DC parents. So, Moscoso worked to get the District of Columbia to make their public-school data more accessible to the public. In 2013, Moscoso's advocacy efforts earned her an OpenGov Champion award from the Sunlight Foundation, an open government advocacy group. Now the Capitol Hill Public School Parent Organization (CHPSPO), created through Moscoso's project, holds the school selection process to a higher standard (Quigg, 2014).

Benefits in Business Accountability and the Community

Cities like San Francisco and New York have open data availability that gives Yelp the ability to include information about a restaurant's health inspection. This gives businesses in these cities the ability to 'up their game' in the restaurant business. Restaurants with

the healthiest inspection reports have the potential of drawing more clientele, and people in the community are given choices for a better dining experience (Quigg, 2014).

Benefits in the Political Process

Seattle, Washington's King County Open Data application had 236,000 views from the public on election night in 2012. This was during a highly-contested race. They even had sophisticated charts about the 90 races that was available via online and mobile devices. Given the number of public views, this availability during the election process was quite popular (Quigg, 2014).

Benefits in Transportation

Recreation boaters are able to obtain information about water hazard and moorage because of Oregon's Marine Board. The board switched out its printed seasonal maps for dynamic digital maps obtained from Oregon's open data portal. Another positive is that the information is updated every 24 hours which gives boaters timely access to accurate information (Quigg, 2014).

SECURITY ISSUES & BEST PRACTICES

To address security issues, this chart outlines how the usefulness of Open Data can be impacted and best practices that can be implemented to address these issues in keeping with federal policies.

CONCERNS	SECURITY ISSUES	BEST PRACTICES
Confidentiality	• Privacy (ensuring proper redaction) • Compliance • Administrative, technical, and physical measures must be taken to ensure confidentiality of the data	• Federal Information Security Management Act (FSMA) has been tasked by NIST to develop standards, guidelines and minimum information security requirements (NIST, 2016).

	• Prevention against unauthorized access	• FIPS PUB 199 has recommendations for low potential impact of confidentiality, integrity and availability. • When data errors, inaccuracies, and/or discrepancies are discovered they should be reported, addressed, and corrected in a timely manner. This will insure accuracy, reliability, and completeness of the data. • Audit (across agencies, if necessary)
Data Integrity	• Discovery of data errors, inaccuracies and/or discrepancies of the data that is collected.	
Availability	• (reliability) of the Open Data service (website)	
Data Authenticity	• Methods of data transfer should be secured.	• Identify what files need to be received and the method that will be used for an adequate level of encryption. Determine if the transfer is one-way or two-way. • Refer to NIST SP 800-47.
Non-repudiation of data sets	• Trust in government agency data at stake.	• Identifiable source of data upload, download and transfer must always be verifiable. • Insure Open datasets cannot be denied of their authenticity. • Refer to FIPS 140-2.

References:

Department of Justice. (2015). Privacy act of 1974. Retrieved from https://www.justice.gov/opcl/privacy-act-1974

Schildkraut, J. (2003, March 26). Confidentiality information protection and statistical efficiency act of 2002. U.S. Bureau of Labor Statistics. Retrieved from https://www.bls.gov/opub/mlr/cwc/confidentiality-information-protection-and-statistical-efficiency-act-of-2002.pdf

Sunlight Foundation. (2012). Open data policy guidelines. Retrieved from https://sunlightfoundation.com/opendataguidelines/

EPA. (n.d.). Emergency planning and community right-to-know-act (EPCRA). Retrieved from https://www.epa.gov/epcra

U.S. Department of State. (n.d.). The Freedom of Information Act. Retrieved from https://foia.state.gov/Learn/FOIA.aspx

Open Data Handbook. (n.d.). The open data handbook. Retrieved from http://opendatahandbook.org/guide/en/

Mayo, E. and Steinberg, T. (2007, June). The Power of Information. Retrieved from http://www.opsi.gov.uk/advice/poi/power-of-information-review.pdf

Opengovdata.org. (n.d.). The annotated 8 principles of open government data. Retrieved from https://opengovdata.org/

Burwell, S., VanRoekel, S., Park, T., Mancini, D. (2013, May 9). Open data policy – managing information as an asset. M-13-13 Memorandum for the heads of executive departments and agencies. Executive office of the President, Office of Management and Budget. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf

Burwell, S. (2014, February 14). Guidance for providing and using administrative data for statistical purposes. M-14-06 Memorandum for the heads of executive departments and agencies. Executive office of the President, Office of Management and Budget. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-06.pdf

Tauberer, J. (2014). Open government data: the book. Retrieved from https://opengovdata.io/2014/civic-hacking/

Quigg, B. (2014, February 14). The citizen benefits of open data. Retrieved from Socrata. https://socrata.com/blog/citizen-benefits-open-data/

National Institute of Standards and Technology (NIST). (2016). Security categorization. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/categorization.html

Federal Information Processing Standards Publication (FIPS 199. (2014, February). Standards for security categorization of federal information and information systems. Retrieved from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Grace, T., Hash, J., Peck, S., Smith, J., Korow-Dicks, K. (2002, August). Security guide for interconnecting information technology systems. National Institute of Standards and Technology (NIST). Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf