**Cybersecurity in Government Organizations**

**CSIA 360**

**Maria Chaudhry**

**Dated: 10/15/2017**

# Paper #1: Can we ensure that Open Data is useful AND secure?

# Introduction

Open Data means data available publicly and public have access and could use or reuse it. Federal agencies circulate their open data to promote efficiency, involvement, and association for the public to view. There are some regulatory agencies those monitor how public is using the open data. According to first open data law passed by President Obama, all federal agencies require to publish their spending data through USASpending.gov. This helps the public to keep an eye that their tax money is not wasting by the federal agencies. Open data makes the federal agencies operation more efficient and transparent. Open format and machine-readable are standards that are required policies incorporated in the open data initiative. Executive branch always ensure privacy and confidentiality.

There are three types of open data called Infrastructural, Public service and personal data.

Infrastructural data has minor concern of privacy and the security. Temperature, weather and transport data comes in this category. Governmental activities data is called public service data. Schools and hospitals statistics and information belongs to this category. Budget and facilities of a specific area is also called public service data. Personally identifiable information (PII) is called Personal data and a person can legally protect its information. Full name, sexual orientation, email address, social security no, medical records, and others are examples of personal data. Personal data cannot release publicly. It is everyone’s right to protect his privacy.

The US government has three branches called legislative, executive and judiciary. Legislative branch made the laws and executive branch execute or force the laws. The executive branch force federal agencies to check the sensitive information before release to the public. This helps to protect privacy and governmental secrets and national security. No one should release and put in danger the national security information. Information collection organization and releasing agency are responsible for integrity, confidentiality, and privacy of the data. Best way is to put the information online on website for public. Federal government’s Data.gov website hugely encourages the transparency between the government and public.

# Value (benefits) of Open Data

There are many valuable benefits of open data for government and public. Open data helps to share the crucial information with the public. Anyone can use open data for research, business or any positive purpose. It builds transparency and trust between government and public. It brings the both parties close by make tight trust relationship between them. Every US president keeps open data his priority to get the people’s confidence. The administration improves and facilitates the flow of data between agencies and public by considering integrity and data confidentiality.

Open data helps the organization to understand their deficiencies and improve them. It also assists the organization to understand the public interest and life patterns, so they could make better business policies and strategies.

Open data could be reused without any limitation. It does not matter how many peoples use the information. Organizations have many departments and each department have many data analyst to use the data. So there is no data usage restriction or limitation.

Nonprofit organizations use open data for educational purpose to make their schooling system easier. U.S Department of Education provides Education Data Initiative open data to analyze education standards. So many organizations use that open data to implement standards.

Health care sector takes advantage form open data to manage medical bills and appointments. Some organizations use that information to get health services and professionals.

Securities and Exchange Commission (SEC) provides financial data and investment analysis information to the public. Financial institutions and investors get this information to promote their business and find relative investment companies. 401K plan information is also open data example.

Open data provides very useful information about real estate and housing. Peoples can easily get information about specific area’s neighborhood, schools rating and crimes report and job opportunities by using zip code of the area. Zillow website is an example for this. Zillow uses a Census Bureau open data to create products and economic analyses reports for the public. Peoples get befit from these reports before buying a home.

# Security issues

No doubt, open data provides several benefits to government and people but there are some security concerns as well. Publishing too much information on the governmental website upraised different queries about its confidentiality, integrity, and availability. People think their Personally Identifiable Information (PII) could be expos to public. Transparency of open data some time develops security issues.

The advancement in technology generated some issues in data protection and safety. Although technology makes life easier but protection and security is a big challenge. Hackers and cyber-criminals are big threats for data. This is reason; many organizations had data breaches in recent years. Internet related products have more safety and privacy concerns.

Above and beyond the security concern, some people said open data is stay locked by one particular body, and it made only to be available for different parties. Sometimes open data is hard to use due to its nature of the restriction. Public sector is not familiar with those technical tools can be used to remove the restrictions on data.

Government always tries to convince the public that open data is secure. Open data follows a serious processing cycle and has a serious procedure and criteria. Data having national security risk and individuals privacy is not allowed to expose.

Federal agencies and companies take ownership, responsibility and accountability of the information they released to public. Agencies follow an efficient and dynamic process executed by certified officials. These executives and officials are expert of data minimization, security, limitation, integrity, confidentiality, authenticity, availability, auditing, and non-repudiation.

Agencies identify the purpose of data need to ensure few things before openly sharing information. Once its purpose is determined, it is necessary to put the permissions and access level. Protection of data from unauthorized access is very important along with confidentiality disclosure. For security of PII, it should be deleted from the system when it no longer required.

 Federal agencies should compliance the open data with the confidentiality controls Federal Information Processing Standard (FIPS) controls published by the National Institute of Standards and Technology (NIST). Agencies should consult Controlled Unclassified Information (CUI) controls to reduce the risks and integrity of open data. Authenticity have key role in open data use because many peoples may be doubtful about open data published by an untrusted source or tampered data. NIST established standards for the open data to ensure that federal agencies are generating proper standard to classify their information systems and information that use the FIPS 199 publication.

# Best Practice Recommendations

Confidentiality, Integrity, and Availability (CIA) must be considered in dealing of open data because these are very important security procedures for any federal agency. CIA always integrates authenticity and non-repudiation. All InfoSec systems require continuity to protect CIA of open data.

Public Key Infrastructure (PKI) ensures the authenticity and non-repudiation. All the federal agencies should use PKI for confidentiality, integrity, and availability (CIA) of open data. Well-trusted authority shares private cryptographic key pair PKI that provides warranty that data is private and secure.

The individuals’ privacy needs more attention than other data. Agencies should pay more attention to personal data before release to public. If any information puts the national security in danger then it should not be published. All the institutions should strictly follow the National Institute of Standards Technology (NIST) and the Federal Information Processing Standard (FIPS) for data publication. NIST and FIPS provide risk free guidance for data publication.

All the government agencies should obey with the Privacy Act 1974 and the E-Government 2002, CIPSEA, and FISMA. These standards and acts limit the amount of information to be collected or created. They identify and limit the number of data sharing. These acts ensure the information is secured from unauthorized access, unauthorized modification. They also ensure that only responsible government officials need to work closely with different agency's Senior Agency Official for Privacy (SAOP) before the agency resale any information. Chief information Security Officers (CISO) is also responsible person in all agencies. He should pay close attention, study and survey the risks of releasing important and sensitive information. All these best practices are important in the governmental as well as private sector for open data because open data is beneficial and risky for government and public.

**Summary and Conclusion**

 Open data is valuable in wide areas for government and public. Different groups of people and organizations could get benefits from open data including government. It is valuable in transparency and democratic control, self-empowerment, innovation and to improve the efficiency of government services. There are many examples how open data is saving millions of dollars of government because it supports transparency. Open data saved Canadian $3.2 billion in charity tax fraud. Danish folketsting.dk track activity in parliament and the law making processes, so you can see what exactly is happening, and which parliamentarians are involved. It means open data is beneficial for all governments of the world but on the other hand all governments should work on Confidentiality, Integrity, and Availability (CIA) of data. They should follow the best practices and obey different security acts and protocols for its privacy and security.

**References**

[1] OECD (Oct 2017). Open Government Data [Online]. Available:

<http://www.oecd.org/gov/digital-government/open-government-data.htm>

[2] Open Data Handbook (June 2017). What is Open Data? [Online]. Available:

<http://opendatahandbook.org/guide/en/what-is-open-data/>

[3] The Agility Effect (2017). Open Data and Cyber Security [Online]. Available:

<https://www.theagilityeffect.com/article/open-data-cyber-security-impossible-equation/>

[4] Rocky DeStefano (July 2017). Fighting Cyber Threats with an Open Data Model [Online]. Available:

 <https://www.infosecurity-magazine.com/opinions/fighting-cyber-threats-open-data/>

[5] The White House (May 2013). Open Government Initiative [Online]. Available:

<https://obamawhitehouse.archives.gov/open>

[6] Kathleen Hickey (Feb 2014). Open data gurus share best practices [Online]. Available:

<https://gcn.com/articles/2014/02/07/open-data-best-practices.aspx>