Project 1 Cybersecurity for Open Data

[Name of the Writer]

[Name of the Institution]

Project 1 Cybersecurity for Open Data

**Introduction**

Open data is the data that can be accessible to anyone and can be freely used anywhere for any purpose by anyone. It can be used by anyone for personal use or commercial use as there are no restrictions on who can use open data. Open data is available free of cost to the people and can be downloaded easily through the internet. Many federal agencies have designed open data to improve the safety and security of the people by providing them information on different events. Open data also has been a valuable tool for researchers and engineers. However, there are certain laws, regulations, and policies which federal agencies need to identify about the open data.

The privacy policy of Open data website includes that it does not collect personal information when someone visits the open data website. However, Data on the open data websites by the government should be offered free and without any restriction. It is important that data on open data websites is not plagiarised. There are certain regulations for the non-federal and federal data that non-federal data can be identified with the name of the publisher, but federal data should not include the name of the publisher. All the data and information must not contain any confidential data of federal agencies which is accessible to the public on websites. These are some laws, regulations, and policies which needs to be ensured by federal agencies when publishing data and information on open data government websites (Data.gov, 2019).

The role of the executive branch is to analyze and evaluate the data before making it available to the public. They will examine the security, privacy, confidentiality or other valid restrictions which are applicable to law, regulation or policy. The executive branch is responsible for forwarding data generated by the government while making sure the security of the data. They will launch new services via Data.Gov that will improve visualization and provide better context to help and understand the open data.

**Benefits of Open Data**

Open data is very important because it can contain usable and discoverable data which can have a huge impact on businesses. The open data helps in increasing transparency and accountability. It allows the public to stay connected and up to date with the operations of the government. Open data develops trust, credibility, and reputation among public and government. It helps the government to prove to the citizen that they are continually working to deliver their promises and making decisions which are best for the public interest.

Open data provides new opportunities to the public for commercial applications and help in enhancing the business. The information provided in open data can be significant for several sectors which include academic, public and industry. These sectors can utilize open data to improve brought innovation and improve economic growth. Open data stores and preserves data over time which means that current and historical data is easily available for the public use at an easily accessible location. There are several organizations which are using Open data provided by the government for their businesses. However, the general public is also using Open data for several purposes in their daily life. Different open data websites by the government are providing information for every sector.

For example, city data provided by the government includes detail information of all the cities in the United States. The detail information includes data about crime rates, weather patterns, cost of living, etc. This data is very useful for the general public to provide them information about the different cities (Data.gov, 2019). Similarly, hdscores is another example of open data provided by the government which help the general public in finding restaurants, schools, hospitals, stadiums, etc. (Data.gov, 2019). One of the most popular open data source provided by the government is LinkedIn which is helping both businesses and the general public. It allows companies to advertise their products and find employees easily. LinkedIn helps organizations to connect with colleagues and learn about potential opportunities. It is not only helping organizations but also to the general public in finding jobs easily according to their qualifications (Data.gov, 2019).

**Security issues**

There are certain security issues which can impact the availability and usefulness of open data. As the data is open to the public, there is a wide range of security threats regarding the confidentiality of data. There are threats to the federal government that how they can protect their confidential information away from the unauthorized people. Open data is accessible by anyone so it can be modified easily, so data integrity is also another major concern for the government currently. Another major security issue which currently federal government has addressed is how they can protect their websites confidential data from unauthorized persons.

Hackers try to access the confidential data of open data websites using different methods. SQL injection is one of the most commonly used methods hackers are using to destroy the database or hack the website. Hackers inject malicious code in the SQL statement via web page input to make changes in the web pages. Similarly, DDoS attacks have become very common and popular which are being addressed by federal agencies. They aim to deny users to access the website which can be very costly sometimes. DDoS attacks will have a huge impact on the availability of data.

Natural disasters are common and can have a huge impact on the availability of data. It is important to have a backup of the company data to make sure that data can easily be recovered in case of any natural disaster. Authentication issues are also very important which are being addressed by the federal government. Usually, users don't create strong passwords because they think they only know about the password. However, they don't have any idea that there are several techniques which hackers can use to easily identify weak passwords and get access to the confidential data of the user. These are some of the factors which are addressed by the federal government currently.

**Recommendations**

The most important thing to ensure data security is to apply authentication technology to digital government information. The government is using several techniques that can help them in user authentication. Cryptography is one of the most important security measures for the authentication of users. It helps in encrypting the confidential data of the users such as login information and passwords. Digital certificates are also another measure to ensure the integrity of content (Coggins & HOLTERHOFF, 2011).

There are several cybersecurity frameworks which are recommended as the best option to ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of Open Data. NIST SP 800-53 is one of the cybersecurity frameworks that represents security controls and associated assessment procedures for federal information systems and organizations. It was published by the National Institute of Standards and Technology who has created a lot of frameworks and standards which are being used by federal agencies (Ross, 2009).

The NIST SP 800-53 provides a description of controls that provide assistance in the development of secure federal information system. These controls are the technical and management safeguards utilize by the information systems to provide the integrity, availability, confidentiality, and security of FIS. NIST SP 800-53 works alongside NIST SP 800-37 which was built for the risk assessment of information systems for federal agencies. However, NIST SP 800-53 focuses on providing measures which can be used with the old risk assessment frameworks NIST SP 800-37. The controls provided by the SP 800-53 is further divided into three parts which include low impact, moderate impact, and high impact. The main function of this framework includes access control, configuration management, maintenance, media protection and risk assessment (Ross, 2009). NIST SP 800-53 is the best-recommended technique for federal agencies to ensure the security of their Open Data. This is one of the fundamental need for Open Data websites and helps in improving the security of organizations Information systems.

**Conclusion**

Open Data provided by the government is one of the essential needs of the general public and businesses these days. It is providing assistance to almost every sector and is becoming very important for everyone. However, there are some security threats which are major concerns for federal agencies because Open Data is accessible to everyone and any information which relates to federal agencies in that data can be a huge threat to these agencies. There are also security issues such as integrity, confidentiality, availability, and authenticity for Open Data websites which needs to be addressed. Many solutions are available which can help to ensure the security of Open Data websites. Different governance frameworks and mitigation techniques can be used to make sure the security of Open Data websites. However, the Executive branch is the one who is responsible for all these issues, and it is their responsibility to apply security measures to the Open Data websites. They also have to analyze the other problems related to the website and make sure the availability of information to the public.

**References**

Impact - Data.gov. (2019). Data.gov. Retrieved from <https://www.data.gov/impact/>

Privacy and Website Policies - Data.gov. (2019). Data.gov. Retrieved from <https://www.data.gov/privacy-policy#data_policy>

Coggins, T. L., & HOLTERHOFF, S. G. (2011). Authenticating Digital. Government Information Management in the 21st Century: International Perspectives, 133.

Ross, R. S. (2009). Recommended Security Controls for Federal Information Systems and Organizations [includes updates through 9/14/2009] (No. Special Publication (NIST SP)-800-53 Rev 3).