Project 2

[Name of the Writer]

[Name of the Institution]

Project 2

The digital government which is also known as e-government refers to the governance which is affected due to the use of information technologies. Their role is to provide services and information to the people. There are different websites which were built by the digital government to assist people. Some of the digital government websites include Benefits.gov, Data.gov, Healthcare.gov, research.gov, foodsafety.gov, etc. It is important for the digital government to build a governance structure that enforces policies and provide standards which meet the requirements of the public. The digital government provides services or information to the viewers which include assistance on different tools, health issues, food safety, research on different topics and data, tools & resources to conduct research.

The concept of digital government that is closely connected to change in institutional and organizational is due to 3 fields which include political science, organization theory and connection of technology and structure of the organization. The most critical topics which are part of e-government include both social and technical challenges. These websites are basically used to serve the public which includes not only individuals but also organizations, firms and interest groups. These websites have a huge impact on the country like the United States. Digital government websites provide the public the opportunity to use different digital technologies which enable civic engagement and public deliberation (Fountain, 2004).

The agencies need to analyze their websites and categorize their websites to different impact levels. There are three impact levels which include low-impact, moderate-impact, or high-impact. These impacts are to fulfill the objectives of security for confidentially, integrity and availability of data. Since the impact levels are different for different websites security, so it is important first to analyze the sensitivity level of each website before assigning them to impact values for confidentiality, integrity and availability of data. The security issues which are common on these websites include access control, data and information integrity, etc. These security issues are a huge concern for the agencies, and it is difficult to built new websites for technical change, so they are finding security measures which are important for the security of their confidential data and privacy (Minimum Security Requirements for Federal Information and Information Systems, 2006).

There are different challenges which agencies are facing due to the involvement of cyber attacks. Some times attacks can be unintentional, and some times hackers do these attacks to create a bad impact on the reputation of the agency and get their confidential data for inappropriate use. The digital government faces a lot of challenges while delivering services via web applications. The most common security issues are for them is the integrity of their confidential data. Data of these agencies are very sensitive and only be accessible to the authorized persons, but some people try to access their data which may include criminals, hackers, terrorists, etc. There are also some unintentional threats which are involved in these web applications include hardware failure, software failure, or not proper training of users of these applications. These issues pose some crucial problems for the agencies because they adversely affect secret information, networks, operations, disruption in the work, and causes damage to national security (Wilshusen & Powner, 2009).

There are different frameworks which need to be implemented for the security of web application during the design, implementation, and operation of digital government websites. The most important thing when designing a web application is to analyze who will have access to the website and which measures are required to ensure that only authorized people can access sensitive data. NIST cybersecurity is the framework which is best to reduce the risk of cyber attacks and increase the security of web applications. There are many types of NIST frameworks which can be used to secure the web applications from cybersecurity threats. NIST framework must ensure to provide a cost-effective approach to control the web applications and take appropriate measures to secure the data of federal agency (Force & Initiative, 2013).

NIST framework uses business drivers to guide cybersecurity activities and focuses on managing risk which organizations are facing. The framework consists of three parts which include the framework core, framework profiles, and implementation tiers. The elements in the framework core provide a full guideline for developing organizational profiles at the individual level. NIST SP 800-53 is one of the NIST frameworks which is used to control the security of the web applications. To implement the NIST framework first organizations must identify the impact level with the help of FIPS 200 and then apply appropriate security controls using NIST SP 800-53. This framework is considered best for the organization because it helps in meeting the business requirements of the organization and allow organizations to take security measures relevant to security control baseline (Force & Initiative, 2013).

It is very important to ensure the security of web applications for the federal agencies because federal agencies website usually contains content which is very sensitive and should be accessible to only authorized people. There are different frameworks like NIST which include ISO IEC frameworks, COBIT, ASD, etc. These frameworks are necessary for the organizations to implement when creating a web application because they help organizations to reduce threats of cyber attacks. Different cybersecurity frameworks provide different functionality for meeting the requirements of the organization security. It is important first to analyze which frameworks are necessary for organization security and how they can help the organization to meet its business requirements during the designing and implementation of the web application. Web applications have a lot of security issues which needs to be resolved by taking appropriate measures, and the best way to analyze these issues is to implement cybersecurity frameworks which ensure the security of the web applications.

**References**

Minimum Security Requirements for Federal Information and Information Systems (2006). Nvlpubs.nist.gov. Retrieved from <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

Fountain, J. E. (2004). Digital government and public health. Preventing chronic disease, 1(4).

Wilshusen, G. C., & Powner, D. A. (2009). Cybersecurity: Continued efforts are needed to protect information systems from evolving threats (No. GAO-10-230T). GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC.

Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800(53), 8-13.