Description 2. Research three or more attacks that could compromise the security of a Digital Government Website that uses Web Applications, a Web Server, and a Database Server. Here are some sources to get you started: a. Web Applications Architectures and Security (in the Week 3 content module). b. Cyber Vandalism -- https://www.digitalgov.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit/ c. Cybersecurity: Actions needed to address challenges facing federal systems (GAO 15-573T) http://www.gao.gov/assets/670/669810.pdf 3. Review three or more websites that deliver digital government services (select from those listed in Table 1). What types of information or services are available via these websites? What population do these websites serve (who is in the intended audience for each website)? 4. As part of your Digital Government websites review, determine the types and sensitivity of information collected, displayed, processed, and stored by the Web applications that implement the Digital Government services. a. See http://www.digitalgov.gov/resources/checklist-of-requirements-for-federal-digital-services/ for general security and privacy requirements. b. See FIPS 199 for additional guidance on determining the sensitivity level of a Federal IT system. (See the section on public websites.) 5. Using FIPS 200, the NIST Cybersecurity Framework, and NIST SP 800-53, research the general types of security controls required by IT systems hosting the Digital Government service that you reviewed. a. FIPS 200 https://doi.org/10.6028/NIST.FIPS.200 b. NIST Cybersecurity Framework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf c. NIST SP 800-53 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf 6. Find three or more additional sources that provide information about best practice recommendations for ensuring the security of the Web Applications used to deliver Digital Government information and services. These additional sources can include analyst reports and/or news stories about recent attacks/threats, data breaches, cybercrime, cyber terrorism, etc. that impacted the security of digital government services. Write a five- to seven-page summary of your research.

At a minimum, your summary must include the following: 1. An introduction or overview of digital government that provides definitions and addresses the laws, regulations, and policies that require federal agencies to provide information and services via the Web. This introduction should be suitable for an executive audience. 2. An overview of the information and services provided by the digital government Websites that you reviewed. Answer the following questions: a. What types of information or services are available via your selected Websites? b. What populations do the websites serve (who is the intended audience)? c. What sensitivity level are applicable to each Website (use FIPS 199 criteria). d. What security issues did you observe during your review? 3. A separate section that addresses the architectures and security issues inherent in the use of Web applications when used to deliver the services provided by your selected digital government Website. Include 5 or more examples of security issues and address how these issues contribute to increased risk. 4. A separate section that includes recommendations for best practices for ensuring Web application security during the design, implementation, and operation of digital government websites. Include five or more best practice recommendations in your recommendations. (Hint: at least one of your recommendations should address use of the NIST Cybersecurity Framework. Another recommendation should address use of NIST SP 800-53 controls for ensuring security and privacy.) 5. A closing section in which you summarize your research and your recommendations