# Project #2: Securing Digital Government Services

For this paper, you will research potential and existing security issues affecting digital government websites. Government websites enable customers to enroll in programs and services, check the status of benefits, and receive information about the federal government’s activities. Your audience for this research report is the Chief Information Officer for a small federal agency who asked for assistance in developing a risk assessment and risk mitigation strategy for the agency’s digital government websites.

**Note: this research report is separate from the report you previously prepared about OPEN data and may not reuse information from that report.** This paper must address other types of government services. See Table 1 for the list of websites to use in your research.

For this report, you should begin by reviewing three or more specific digital government websites (from the list provided in Table 1) to determine:

1. the types of information provided by the websites
2. the types of services provided by the websites
3. security issues which could impact the delivery of digital government services by the websites

After you have reviewed these websites, review the *Federal Cybersecurity Risk Determination Report and Action Plan* <https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf> to identify additional sources of risk that the agency must be aware of and should address in its planning. You should also review Executive Order 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>

**Table 1. List of Digital Government Websites**

|  |  |  |  |
| --- | --- | --- | --- |
| Base URLs | | | |
| BENEFITS.GOV | CANCER.GOV | CONSUMERFINANCE.GOV | DATA.GOV |
| DIGITALGOV.GOV | DISASTERASSISTANCE.GOV | FOODSAFETY.GOV | GRANTS.GOV |
| HEALTHCARE.GOV | HEALTHFINDER.GOV | MEDICARE.GOV | READY.GOV |
| RECREATION.GOV | REGULATIONS.GOV | RESEARCH.GOV | SAFERCAR.GOV |
| SERVE.GOV | STOPFAKES.GOV | USA.GOV | VOLUNTEER.GOV |

## Research:

1. Read / Review the Weekly readings
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:
   1. Web Applications Architectures and Security (in the Week 3 content module).
   2. Cyber Vandalism -- <https://www.digitalgov.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit/>
   3. *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.
   1. See <http://www.digitalgov.gov/resources/checklist-of-requirements-for-federal-digital-services/> for general security and privacy requirements.
   2. See [FIPS 199](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf) 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.
   1. FIPS 200 <https://doi.org/10.6028/NIST.FIPS.200>
   2. NIST Cybersecurity Framework <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
   3. 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:

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:
   1. What types of information or services are available via your selected Websites?
   2. What populations do the websites serve (who is the intended audience)?
   3. What sensitivity level are applicable to each Website (use FIPS 199 criteria).
   4. 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.

## Submit for Grading

Submit your work in MS Word format (.docx or .doc file) using the Project 2 Assignment in your assignment folder. (Attach the file.)

## Additional Information

1. Consult the grading rubric for specific content and formatting requirements for this assignment.
2. Your 5- to 7-page paper should be professional in appearance with consistent use of fonts, font sizes, margins, etc. You should use headings and page breaks to organize your paper.
3. Your paper should use standard terms and definitions for cybersecurity. See Course Content > Course Resources > Cybersecurity Concepts Review for recommended resources.
4. The CSIA program recommends you follow standard APA formatting since this will give you a document that meets the “professional appearance” requirements. You can find APA formatting guidelines and examples under Content > Course Resources > APA Resources. You can use the provided APA template file (MS Word format) CSIA\_Basic\_Paper\_Template(APA\_6ed,DEC2018).docx.
5. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be a separate page at the end of your file. These pages do not count towards the assignment’s page count.
6. You should write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct, and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
7. You must credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.).