# Case Study #2: Can we ensure that Digital Government services are secure?

## Case Scenario:

You have been asked to participate in a panel discussion of security issues affecting digital government Websites. Each panel member has been asked to select a specific Website (from the list provided in Table 1) and then research (a) the information and services that it provides and (b) the security issues which could impact the delivery of digital government services. Your two to three page summary of your research will be provided to the panel audience in advance of the discussion.

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

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

## Research:

1. Read / Review the Week 3 readings.
2. Research three or more attacks which could compromise the security of a Digital Government Website which 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>
   4. *Cognitive Hacking and Digital Government: Digital Identity* <http://www.ists.dartmouth.edu/library/78.pdf>
   5. US-Cert Publications (See Technical Reports section) <https://www.us-cert.gov/security-publications#reports>
3. Review the Website for a digital government service (select one of the Websites listed in Table 1). What types of information or services are available via your selected Website? What population does this Website serve (who is the intended audience)?
4. As part of your Digital Government Website review, determine the types and sensitivity of information collected, displayed, processed, and stored by the Web applications which implement the Digital Government service.
   1. See <http://www.digitalgov.gov/resources/checklist-of-requirements-for-federal-digital-services/> for general security and privacy requirements.
   2. 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 and NIST SP 800-53, research the general types of security controls which are required for the IT systems hosting the Digital Government service that you reviewed.
6. Find three or more additional sources which 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. which impacted the security of digital government services.

## Write:

Write a two to three page summary of your research. At a minimum, your summary must include the following:

1. An introduction or overview of *digital government* which provides definitions and addresses the laws, regulations, and policies which require that federal agencies 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 your selected digital government Website. Answer the following questions:
   1. What types of information or services are available via your selected Website?
   2. What population does this Website serve (who is the intended audience)?
   3. What sensitivity level which should be assigned to the Website (use FIPS 199 criteria).
   4. What security issues were observed during your review?
3. A separate section which 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.
4. A separate section which 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 discussion.
5. A closing section in which you summarize your research and your recommendations.

Your white paper should use standard terms and definitions for cybersecurity. The following sources are recommended:

* ISACA Glossary <http://www.isaca.org/pages/glossary.aspx>
* *Guidelines on Security and Privacy in Public Cloud Computing* <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>

## Submit For Grading

Submit your case study in MS Word format (.docx or .doc file) using the Case Study #2 Assignment in your assignment folder. (Attach the file.)

## Formatting Instructions

Use standard APA formatting for the MS Word document that you submit to your assignment folder. Formatting requirements and examples are found under Course Resources > APA Resources.

## Additional Information

1. You are expected to 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.
2. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must comply with APA 6th edition Style requirements. Failure to credit your sources will result in penalties as provided for under the university’s Academic Integrity policy.