# 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.

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. These items are graded under Professionalism and constitute 20% of the assignment grade.
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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | **Excellent** | **Outstanding** | **Acceptable** | **Needs Improvement** | **Needs Significant Improvement** | **Missing or Unacceptable** |
| Introduction or Overview for the Case Study | 20 points  Provided an excellent introduction or overview of digital government which provided definitions and addressed the laws, regulations, and policies which require that federal agencies provide information and services via the Web. The overview appropriately used information from 3 or more authoritative sources. | 18 points  Provided an outstanding introduction or overview of digital government which provided definitions and addressed the laws, regulations, and policies which require that federal agencies provide information and services via the Web. The overview appropriately used information from 2 or more authoritative sources. | 16 points  Provided an acceptable overview of digital government discussed the laws and policies which require that federal agencies provide information and services via the Web. The overview appropriately used information from 1 or more authoritative sources. | 14 points  Provided an overview of digital government but, the section lacked important details about the case. Information from authoritative sources was cited and used in the overview. | 10 points  Attempted to provide an introduction to the case study but this section lacked detail and/or was not well supported by information drawn from authoritative sources. | 0 points  The introduction and/or overview sections of the paper were off topic. |
| Review of a Digital Government Website | 20 points  Provided an excellent overview of the information and services provided by the selected digital government Website. Provided full, complete, and concise answers to the following questions:  a. What types of information or services are available via the selected Website? b. What population does this Website serve (who is the intended audience)? c. What sensitivity level which should be assigned to the Website (use FIPS 199 criteria)? d. What security issues were observed during the review?  Appropriately used information from 3 or more authoritative sources. | 18 points  Provided an outstanding overview of the information and services provided by the selected digital government Website. Provided answers for the following questions:  a. What types of information or services are available via the selected Website? b. What population does this Website serve (who is the intended audience)? c. What sensitivity level which should be assigned to the Website (use FIPS 199 criteria)? d. What security issues were observed during the review?  Appropriately used information from 2 or more authoritative sources. | 16 points  Provided an acceptable overview of the information and services provided by the selected digital government Website. Answered the following questions:  a. What types of information or services are available via the selected Website? b. What population does this Website serve (who is the intended audience)? c. What security issues were observed during the review?  Appropriately used information from  1 or more authoritative sources. | 14 points  Provided a review of a digital government website, but the discussion lacked important details.Appropriately used information from authoritative sources. | 9 points  Provided a discussion of the information and services provided by digital government websites. The discussionlacked detail and/or was not well supported by information drawn from authoritative sources. | 0 points  This section was missing, off topic, or failed to provide information about a digital government website. |
| Web Application Architectures and Security Issues | 15 points  Provided an excellent discussion of Web application architectures and common / frequent security issues inherent in the use of Web applications in the context of digital government Websites. Discussion included 5 or more examples of security issues.Appropriately used information from 3 or more authoritative sources. | 14 points  Provided an outstanding discussion of Web application architectures and common / frequent security issues inherent in the use of Web applications in the context of digital government Websites. Discussion included 3 or more examples of security issues.Appropriately used information from 2 or more authoritative sources. | 13 points  Provided an acceptable description of Web application architectures. Discussed common / frequent security issues inherent in the use of Web applications in the context of digital government Websites. Discussion included at least one example of a relevant security issue.Appropriately used information from 1 or more authoritative sources. | 11 points  Discussed web application architecture and security issues.Appropriately used information from authoritative sources. | 4 points  Mentioned web application architectures and security issues. Discussion was substantially lacking in content and/or organization OR was not well supported by information drawn from authoritative sources. | 0 points  Section was missing or off topic. |
| Best Practices and Recommendations for Ensuring Security of Digital Government Websites | 15 points  Provided an excellentdiscussion of best practices for ensuring Web application security during the design, implementation, and operation of digital government websites. Included 5 or more best practices (with recommendations) which could be implemented to improve the security of digital government websites. Appropriately used information from 3 or more authoritative sources. | 14 points  Provided an outstandingdiscussion of best practices for ensuring Web application security during the design, implementation, and operation of digital government websites. Included 3 or more best practices (with recommendations) which could be implemented to improve the security of digital government websites. Appropriately used information from 2 or more authoritative sources. | 13 points  Provided an acceptable discussion of best practices for ensuring Web application security for digital government website. Included at least one best practice example for improving the security of digital government websites. Appropriately used information from 1 or more authoritative sources. | 11 points  Discussion provided some information about best practices and included recommendations for improving security for digital government websites. Mentioned information obtained from authoritative sources. | 4 points  Included recommendations for improving security in the context of digital government websites but the discussion lacked detail and/or was not supported by information from authoritative sources. | 0 points  This section was missing, off topic, or failed to address best practices and/or recommendations. |
| Addressed security issues using standard cybersecurity terminology | 5 points  Demonstrated excellence in the integration of standard cybersecurity terminology into the case study. | 4 points  Provided an outstanding integration of standard cybersecurity terminology into the case study. | 3 points  Integrated standard cybersecurity terminology into the into the case study | 2 points  Used standard cybersecurity terminology but this usage was not well integrated with the discussion. | 1 point  Misused standard cybersecurity terminology. | 0 points  Did not integrate standard cybersecurity terminology into the discussion. |
| APA Formatting for Citations and Reference List | 5 points  Work contains a reference list containing entries for all cited resources. Reference list entries and in-text citations are correctly formatted using the appropriate APA style for each type of resource. | 4 points  Work contains a reference list containing entries for all cited resources. One or two minor errors in APA format for in-text citations and/or reference list entries. | 3 points  Work contains a reference list containing entries for all cited resources. No more than 3 minor errors in APA format for in-text citations and/or reference list entries. | 2 points  Work has no more than three paragraphs with omissions of citations crediting sources for facts and information. Work contains a reference list containing entries for cited resources. Work contains no more than 5 minor errors in APA format for in-text citations and/or reference list entries. | 1 point  Work attempts to credit sources but demonstrates a fundamental failure to understand and apply the APA formatting standard as defined in the *Publication Manual of the American Psychological Association* (6th ed.). | 0 points  Reference list is missing. Work demonstrates an overall failure to incorporate and/or credit authoritative sources for information used in the paper. |
| Professionalism Part I: Organization & Appearance | 5 points  Submitted work shows outstanding organization and the use of color, fonts, titles, headings and sub-headings, etc. is appropriate to the assignment type. | 4 points  Submitted work has minor style or formatting flaws but still presents a professional appearance. Submitted work is well organized and appropriately uses color, fonts, and section headings (per the assignment’s directions). | 3 points  Organization and/or appearance of submitted work could be improved through better use of fonts, color, titles, headings, etc. OR Submitted work has multiple style or formatting errors. Professional appearance could be improved. | 2 points  Submitted work has multiple style or formatting errors. Organization and professional appearance need substantial improvement. | 1 point  Submitted work meets minimum requirements but has major style and formatting errors. Work is disorganized and needs to be rewritten for readability and professional appearance. | 0 points  Submitted work is poorly organized and formatted. Writing and presentation are lacking in professional style and appearance. Work does not reflect college level writing skills. |
| Professionalism Part II: Execution | 15 points  No formatting, grammar, spelling, or punctuation errors. | 14 points  Work contains minor errors in formatting, grammar, spelling or punctuation which do not significantly impact professional appearance. | 13 points  Errors in formatting, spelling, grammar, or punctuation which detract from professional appearance of the submitted work. | 11 points  Submitted work has numerous errors in formatting, spelling, grammar, or punctuation. Work is unprofessional in appearance. | 4 points  Submitted work is difficult to read / understand and has significant errors in formatting, spelling, grammar, punctuation, or word usage. | 0 points  Submitted work is poorly executed OR does not reflect college level work. |
| **Overall Score** | **Excellent 90 or more** | **Outstanding 80 or more** | **Acceptable 70 or more** | **Needs Improvement 56 or more** | **Needs Significant Improvement 36 or more** | **Missing or Unacceptable 0 or more** |