# Paper #1: Can we ensure that Open Data is useful AND secure?

## Scenario:

A federal agency has asked your cybersecurity consulting firm to provide it with a white paper that discusses the issues of usefulness and security in regards to Open Data. The white paper is intended for a group of executives at the agency who are opposed to the planned conversion of its current controlled distribution for several highly valuable and frequently requested datasets (DVDs purchased through the Government Printing Office) to *OPEN Data* distribution via the government’s Data.Gov portal (website). Currently, these data sets are purchased by businesses and academic institutions and are used for a variety of purposes.

A customer satisfaction survey revealed that purchasers are willing to change over to the new *Open Data* distribution method for data sets. But, the agency head has received phone calls from several large and politically well-connected customers who expressed concerns about potential issues with the *integrity* and *authenticity* of downloaded data. The agency’s executives were also surveyed and they provided the following security-related items in a list of concerns for the planned conversion to an *Open Data* delivery method:

1. Confidentiality / Privacy (ensuring proper redaction)
2. Data integrity
3. Data authenticity
4. Availability (reliability) of the Open Data service (website)
5. Non-repudiation of data sets

## Research:

1. Read / Review the weekly readings.
2. Research the federal government’s *OPEN Data* mandate. Here are some sources that you may find useful:
   1. *Open Data Policy-Managing Information as an Asset* - OMB Memorandum M-13-13 (PDF file is in the week 2 readings). This Memorandum includes significant discussion of security issues and policy solutions including references to FIPS 199 and NIST SP-800-53)
   2. U.S. Open Data Action Plan (see file us\_open\_data\_action\_plan.pdf in week 2 readings).
   3. <https://www.data.gov>
   4. <https://www.data.gov/privacy-policy#data_policy>
   5. *Guidance for Providing and Using Administrative Data for Statistical Purposes* - OMB Memorandum M-14-06 (PDF file is in the week 2 readings). This Memorandum includes discussion of privacy and security issues arising from the use of information collected for statistical purposes (e.g. the Census, employment, economic data, etc.).
3. Research how government information, e.g. *OPEN Data*, is used by businesses and the general public. Here are some sources to get you started:
   1. *7 Ways Companies Are Using the Government's Open Data* <http://mashable.com/2013/05/30/7-ways-government-open-data/>
   2. *Government open data proves a treasure trove for savvy businesses* <http://www.computerworld.com/article/2488683/business-intelligence-government-open-data-proves-a-treasure-trove-for-savvy-businesses.html>
   3. *Open data: Unlocking innovation and performance with liquid information* <http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information>
4. Research the issues that can arise when businesses depend upon the *confidentiality, integrity, availability, authenticity,* and *non-repudiation* of government provided *Open Data.* Suggested sources include:
   1. *Authenticating Digital Government Information* <http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1954&context=law-faculty-publications>
   2. *Legal and Institutional Challenges for Opening Data Across Public Sectors* <http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=97430297&site=eds-live&scope=site>
   3. *Risk Analysis to Overcome Barriers to Open Data* <http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=poh&AN=93550378&site=eds-live&scope=site>
   4. *Reconciling Contradictions of Open Data Regarding Transparency, Privacy, Security and Trust* <http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=97430299&site=eds-live&scope=site>
5. Find five or more best practice recommendations for ensuring the security (confidentiality, integrity, availability, authenticity, non-repudiation) of information provided by the federal government through its OPEN Data initiative. N.B. For the purposes of this assignment, you may treat “licensing” concerns as an “availability” issue.

## Write:

Write a five (5) to eight (8) page summary of your research. You should focus upon clarity and conciseness more than length when determining what content to include in your paper. At a minimum, your summary must include the following:

1. An introduction or overview of *OPEN Data* which provides definitions and addresses the laws, regulations, and policies which require federal agencies to identify and publish datasets and information collections. Discuss the role of the executive branch’s *Open Data / Open Government* policies in making data available via Data.Gov. This introduction should be suitable for an executive audience.
2. A separate section in which you discuss the value (benefits) of *Open Data*. This section should provide several specific examples of how government provided *Open Data* is being used by businesses and the general public.
3. A separate section in which you address security issues (confidentiality, integrity, availability, authenticity, and non-repudiation ) which can impact the usefulness of *Open Data* and how these issues are currently being addressed by the federal policies and plans for *Open Data*. Again, you should provide examples of issues and mitigations or solutions.
4. A section in which you address *best practice* recommendations for ensuring the confidentiality, integrity, availability, authenticity, and non-repudiation of *Open Data*.
5. A separate section in which you summarize your research and recommendations.

## Submit For Grading

Submit your white paper in MS Word format (.docx or .doc file) using the OPEN Data Assignment in your assignment folder. (Attach the file.)

## Additional Information

1. Your white paper should use standard terms and definitions for cybersecurity concepts. 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>

1. 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.
2. Use APA 6th edition style (formatting) for the organization and appearance of the MS Word document that you submit to your assignment folder. This includes margins, section headings, and consistent use of fonts (Times New Roman 12 in black), paragraph styles (first line indent by ½ inch), and line spacing (double). Formatting requirements and examples are found under Course Resources > APA Resources. Your file should contain both a title page and a separate References page. Use page breaks to ensure that the title page and references page are separate from the body of the paper.
3. 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.