James Chad Ballay

**Week 9**

* Visit the US Government Accountability Office web site (gao.gov). Locate a recent report on information security in the US government. Review the report and briefly describe in your own words the information security issue addressed in the report.

# CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs (<https://www.gao.gov/products/GAO-19-144>)

Staffing shortfalls and mis-assignment of job roles is hampering HR efforts. This hurts primarily since it is a self-inflicted wound that’ll hamper having adequate coverage. (Plus if I ever go towards government work it might limit my own job prospects...) Most of the recommendations are for the various Departments to update any job roles that have a generic role assignment of 000 to the appropriate NICE code. (<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center>)

* Visit the Computer Security Resource Center (CSRC) section of the US Government National Institute of Standards and Technology web site (csrc.nist.gov). Locate a recent publication related to information security. Provide a one page synopsis of the publication in your own words. Include how this publication could be used by an organization's information security department.

### SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (<https://csrc.nist.gov/publications/detail/sp/800-122/final>)

**Summary**

Data collection goals are often created by the business side of operations with less input being provided by the security and data warehouse side of IT. This guide provides a framework of how to bridge the gap between the business objectives and the risk/compliance objectives.

* Organizations should identify all PII residing in their environment.
* Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
* Organizations should categorize their PII by the PII confidentiality impact level.
* Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.
* Organizations should develop an incident response plan to handle breaches involving PII

For each of those bullets it lays out in general terms the what/who/when/how to start attacking the problem. It doesn’t explicitly lay out the plan but it does provide some milepost to guide the plan. The appendix contains scenarios to even further highlight considerations to be used by the stakeholders.

### 