Within U.S. federal government agencies, hosting linked data requires compliance with the Federal Information Security Management Act (FISMA). FISMA delegates responsibilities for security standards and guidelines to the National Institute of Standards and Technology (NIST). To comply with U.S. federal government standards, federal agencies must first determine the security category of their information system in accordance with Federal Information Processing Standard (FIPS) 199, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication (SP) 800-53. Finally, a responsible official in the agency must accept the risk associated with the information system, and grant an authorization to operate (ATO) in accordance with NIST SP 800-37.

Ultimately, the linked data will be managed within the physical and conceptual boundaries of a federal information system. This information system may be internally managed by the agency, or it may be a cloud-based system authorized by the General Services Administration (GSA) through the new Federal Risk and Authorization Management Program (FedRAMP). Whether an existing information system is used or new system is developed for the linked data hosting project, the type of activities associated with the linked data must be accounted for in the risk categorization and security controls, and the system must receive an ATO from a responsible federal official.

While security plan specifics will vary widely based on a range of factors like hosting environment and software configuration, the process for developing and getting a security plan approved can be streamlined if the following guidelines and best practices are considered:

Notify your security official of your intent to publish open government data.

* Provide an overview of the Linked Data project
* Describe how you plan to host the data (e.g., cloud, agency data center), implementation timelines
* Consider including your hosting service/software vendor in discussion(s)

Solicit assistance from the security official:

* Identify guidance that should be used (e.g. for U.S. federal agencies this typically would entail compliance with security control recommendations from NIST Special Publication 800-53)
* Request clarification on regarding specific content/areas that the plan should address
* Request a system security plan template to ensure the plan is organized to facilitate the review process (if a vendor is contributing information on controls related to their service/software, the vendor needs to adhere to the template in their response)

Security plans are typically comprised of a set of security controls, describing physical, procedural, technical and other processes and controls in a system which are in place to protect information access, availability and integrity, and for avoiding, counteracting and minimizing security risks. These are typically comprised of several layers, such as physical facility security, network and communications, to considerations of operating system, software, integration and many other elements. As such, there will typically be some common security controls which are inherited, and which may not be specific or unique to the linked data implementation, such as controls inherited from the hosting environment, whether cloud hosting provider, agency data center, et cetera. Additionally, some security controls will be inherited from the software vendors.

As such, opportunities may exist to streamline the development of a security plan, or conversely, to identify potential project security vulnerabilities and risks, through early engagement with hosting providers, software vendors and others who may be responsible for those common, inherited controls. If the inherited controls meet the recommendations, they can then be assembled following the requisite templates, and the system security plan can be completed through addition of any applicable controls specific or unique to the linked data application's configuration, implementation, processes or other elements described in the security control and security plan guidance.