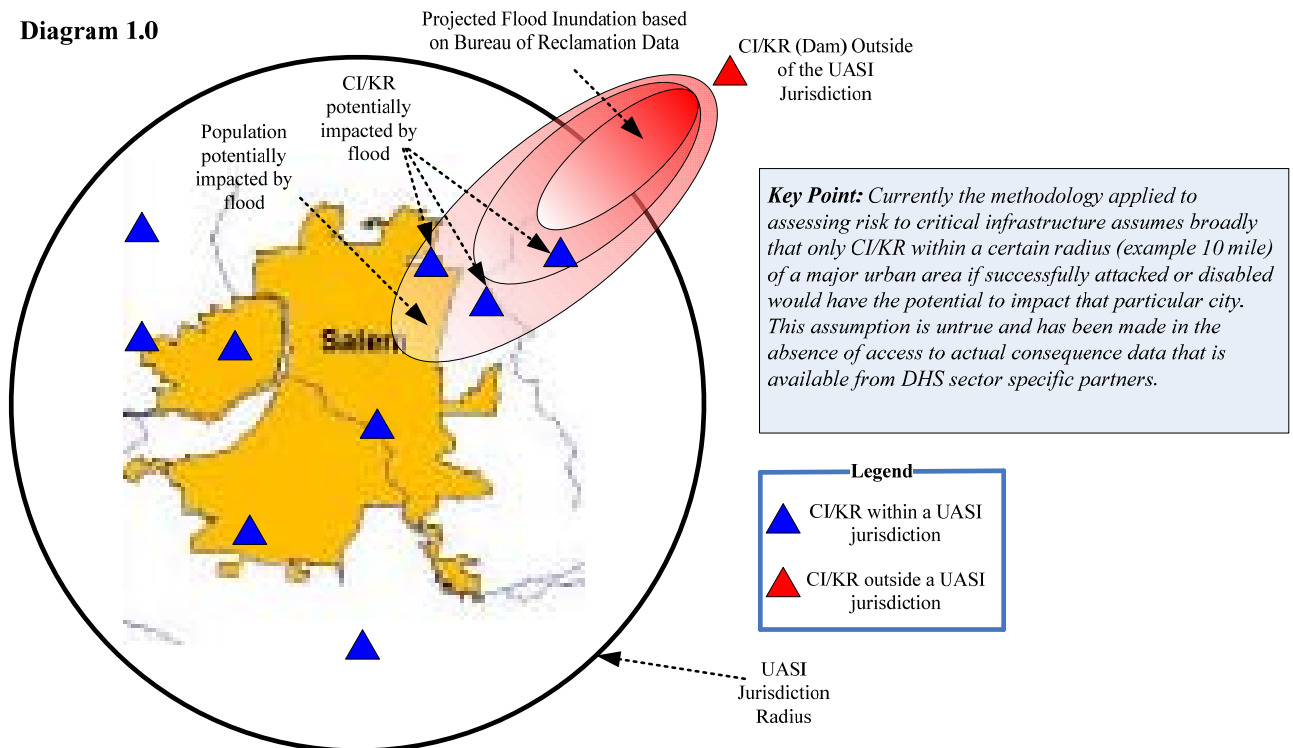


# ArdentMC

***Business Need – Access to disparate data sources, facilitating the CI/ KR risk analysis process and effectively applying grant funding to mitigate risk:***

Prior to 2005, DHS was using a rather simplistic methodology to analyze risk to CI/KR for the purpose of applying grant funding to mitigating risk. This methodology focused on applying grant funding based on population densities within a set of the major urban areas. In 2006, DHS moved towards a grant funding methodology based on sector, state and local risk within a UASI jurisdiction. Although the revised methodology is a level of maturation beyond the prior year process, it should be noted that CI/KR inclusion in the risk analysis and eligibility for funding is often limited to assets that fall within a defined Urban Area Security Initiative (UASI) jurisdiction. As a result it is likely that not all CI/KR that either support or could impact those UASI jurisdictions were identified as inputs into the risk analysis or even eligible to apply for grant funding. Below is an example of CI/KR outside of a UASI jurisdiction (in this case a dam that has been destroyed) impacting an urban area.

**Diagram 1.0**

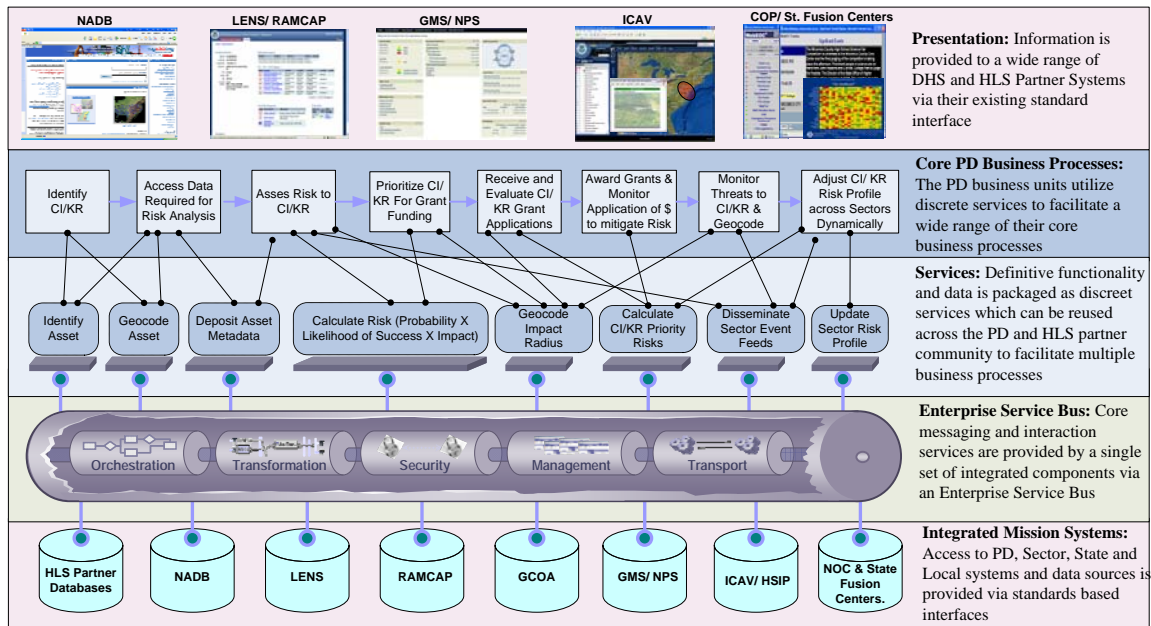


In order to conduct a comprehensive risk analysis on CI/KR and the urban areas that could be impacted by loss of those assets, DHS will need to have access to more extensive data from a variety of heterogeneous sources. In the example above, access to the Bureau of Reclamation (BoR) flood inundation data for this particular dam would

have helped DHS to understand the true impact of this dam being destroyed and would have resulted in the expansion of the UASI jurisdiction to include this particular asset in the list of CI/KR eligible for grant funding. Furthermore, threat analysis and mitigation data available for this CI/KR would allow DHS to not only understand the current protective measures being taken but also the additional measures (and funding) required to bring the overall risk profile for this asset to an acceptable level. Applying this logic (access to specific threat, protection and impact data from definitive sources) across the range of assets in a UASI jurisdiction would help DHS, Grants and the urban area develop not only a comprehensive view of their overall risk profile, but also a prioritized list of infrastructure and assets that are the *most critical* as well as specific recommendations to Grants on the most effective application of grant funding to protect those CI/KR.

**Solution & Scenario:**

The business need of timely and cost effective access to disparate data sources drives the technical solution. As outlined in the diagram below, disparate data sources internal and external to DHS are integrated via an Enterprise Service Bus (ESB). Core messaging and interaction services are facilitated via the ESB, and multi use functionality and data are packaged as discreet services which can be used to facilitate a wide range of core business processes - asset identification and data acquisition, risk analysis, grants management, maintaining CI/KR situational, operational and strategic awareness etc.



In this scenario, assets internal and external to a UASI jurisdiction are identified and geo-coded. Asset attribute data (protective measures, economic impact, loss of life and production output consequence etc.) from definitive sector, state and local sources is

made available via the ESB. This data is ingested either via a push or pull mechanism to the National Asset Database (NADB) regardless of system or format. Risk analysts then use the asset data from the NADB to feed their risk analysis tools (RAMCAP, GCOA etc.). These tools are used to determine:

- Criticality of an asset or set of interdependent assets
- Vulnerability of an asset
- Impact to a given UASI area or other CI/KR if successful

Criticality X Vulnerability X Impact = the Risk Score for individual CI/KR which is then aggregated to provide a number of different risk profile views (risk by sector, priority risk by UASI area etc.). This information is then passed on to Grant analysts who determine with a greater level of fidelity the amount of grant funding that needs to be applied holistically in order to bring the National risk profile to an acceptable level. Lastly, CI/KR situational, operational and strategic awareness is enhanced as information on protective measures taken, threats mitigated and emerging threats are geospatially plotted and linked to CI/KR, sectors and UASI areas – thereby providing a dynamic view into the national risk profile rather than the current static view.

***Summary:***

A defined and consistent set of core business processes supported by the appropriate data, systems and ESB technology will:

- Provide DHS with relevant data in order to assess more accurately probability, impact and consequence.
- Provides a repeatable and cost effective means to integrate with heterogeneous state, local and sector systems and data
- Provides for the fusion of data across assets and sectors – enhancing the existing HSIP data sets
- Provides for a logical and defensible National Common Risk Assessment (NCRA) methodology
- Increase the efficiency with which grant funding is applied
- Increase the security posture of our Nations most critical assets and infrastructure