Case Study Assignment

This assignment is based on 1 of your readings from this module:

Cybersecurity and Infrastructure Security Administration (2018). Cybersecurity Governance. Click here (link opens in a new browser window)Links to an external site. to access this web page.

Compare the governance approaches of two states based on the case studies introduced in this module. In what ways were they similar? In what ways did they differ? Write up your responses in a short paper of 500 words or less.

Grading

Your paper submission should be approximately 1-2 pages in length (not to exceed a maximum of 500 words) with double line spacing. Your submission should adhere to the APA reference standard for all sources used to support your writing.

You will receive a grade of 0-100% which will reflect the quality of your submission. Please refer to the course syllabus for more detailed information about how your grade will be calculated.

Module 4: Case Study Assignment

Kyler Kent

School of Continuing Studies, Georgetown University

MPCR-620-101: Cybersecurity Governance Framework

Prof. Matthew Shabat

September 25, 2022

Module 4: Case Study Assignment

Governance in the United States is a complicated subject that requires comprehensive investigation and review. During this week, I analyzed the governance patterns of Washington and Virginia from the Department of Homeland Security's perspective. I discovered many similarities and a few differences between each state, representing governance in a federal republic government model.

While discovering commonalities, I found that both states have an emphasis on "leadership" with limitations and a multidisciplinary approach to governance (U.S. Department of Homeland Security, 2017a, p. 2; U.S. Department of Homeland Security, 2017b, p. 2). I found a difference in Washington's organizational chart as nearly all cybersecurity and governance functions report to the "Washington Technology Solutions" entity (U.S. Department of Homeland Security, 2017b, p. 7). This reporting structure requires the CIO and their "Center for Shared Solutions" to report up as well (p. 7). Virginia's organizational structure appears to revolve around centralization under the Secretary of Technology and the state Chief Information Officer (CIO) (U.S. Department of Homeland Security, 2017a, p. 7). No organizational chart was provided to directly compare and contrast Virginia's structure with other states (p. 7).

Regarding budgeting governance in Virginia and Washington, both states have their CIO oversee budgeting operations (U.S. Department of Homeland Security, 2017a, pp. 9-10; U.S. Department of Homeland Security, 2017b, p. 9). Washington directly involves risk management in their budgeting process by comparing budget proposals to a "corresponding risk profile" (U.S. Department of Homeland Security, 2017b, pp. 9-10). Virginia appears to have their CIO as the final arbiter in the budget process (U.S. Department of Homeland Security, 2017a, p. 10). Virginia also "has a single vendor contract in place with Northrop Grumman to provide" the vast majority of IT resources for the state (p. 10). Washington does not appear to have such partnerships or private contracts.

Furthermore, there are some similarities and differences regarding risk identification and mitigation. Washington appears to centralize most of the activities in this genre under their CISO (U.S. Department of Homeland Security, 2017b, p. 11). Virginia appears to combine both the CISO and the CIO for this purpose to identify and manage risk (U.S. Department of Homeland Security, 2017a, p. 11). Washington seems to delegate risk assessments to each respective department "for every project" (U.S. Department of Homeland Security, 2017b, p. 11). Virginia appears to have no such stipulations and focuses on a C-suite form of control over risk management (U.S. Department of Homeland Security, 2017a, p. 11). Next, Washington emphasizes "cross-organizational" risk management with "the Military Department," which Virginia does not appear to have (U.S. Department of Homeland Security, 2017b, p. 11). Washington's Military Department even appears to work with private businesses and companies regarding "critical infrastructure" (U.S. Department of Homeland Security, 2017b, p. 11).

In summary, each state represents a convergent and divergent approach to governance regarding objectives, organizational structure, budgeting, and risk management. I found several takeaways from each state to include in my course project and augment my overall governance strategy.

References

U.S. Department of Homeland Security. (2017a, December). Cybersecurity Governance in the Commonwealth of Virginia. In CISA.gov. CISA. Retrieved September 22, 2022, from https://www.cisa.gov/sites/default/files/publications/Virginia_Cyber_Governance_Case_Study_2.pdf

U.S. Department of Homeland Security. (2017b, December). Cybersecurity Governance in the State of Washington. In CISA.gov. CISA. Retrieved September 22, 2022, from https://www.cisa.gov/sites/default/files/publications/Washington_Cyber_Governance_Case_Study_508.pdf