# **United States Federal Government – Federal and State Policy Comparison**

Group 1

Ryan Briggs

John Cox

Kimberly Edmonds

Victoria Yuen

University of Maryland Global Campus

CYB 670: Capstone in Cybersecurity

Professor Yurek Hinz

October 13, 2021

## Federal and State Policy Comparison

There are five teams that are involved with this ELITE simulation. According to the Application model reference guide (UMGC.edu, 2013), there are five team, which are:

1. Federal Government
2. Avisitel – Telecommunications
3. DTL Power – Power
4. Mistral Bank – Financial Services
5. Hytema – Defense Contractor

All of these teams will need to work together to create a set of cybersecurity policies for this simulation. Group 1 will act as the Federal Government for this simulation. For this simulation, the Cyber Security Command (CSC) under the direction of the Department of Homeland

Security (DHS) that was created to unify the federal government’s cybersecurity responses. The stated goal of the CSC is to “prepare for, prevent, and respond to cyber emergencies” (UMGC.edu, 2013). The CSC has already spent $27.4 billion dollars of its allocated budget of $38.8 billion. Separate from this budget, the CSC has also given $15.6 billion dollars “in grants to state and local governments for cybersecurity and to improve their ability to identify and protect against cyber threats” (UMGC.edu, 2013). The primary responsibilities of the CSC are too:

1. Prescribe a uniform technical setup for federal agencies across the United States
2. Define operational cybersecurity policies for federal agencies across the United States
3. Control the areas of technical advisories
4. co-operation with the private sector
5. funding cybersecurity research

(UMGC.edu, 2013)

The CSC is a federal department and will focus on the federal government’s responses to cybersecurity events. However, some US states also have their own cybersecurity policies. In this report, we will first cover the federal government’s cybersecurity and then some of the state’s cybersecurity policies.

The federal government’s cyber network is massive. It contains “well over 100 agencies, millions of employees, and tens of millions of devices to manage” (Charlet, 2018). Due to the sheer size of the federal government, the budget is just a as big. The latest government-wide Information Technology (IT) spending for fiscal year 2021 was $90.9 billion dollars (itdashboard.gov, n.d.). The updated Federal Information Security Modernization Act of 2014 states that every federal agency is responsible for its own cybersecurity (Federal Information Security Modernization Act of 2014, 2014), but those agency’s policies are developed from the National Institute of Standards and Technology (NIST) developed standards and guidelines (Charlet, 2018). According to the paper written by Charlet, there are five major challenges for the federal government:

1. Difficult tradeoffs between centralized and decentralized

management.

1. Varying levels of engagement of agency top leadership on cyber risk

management.

1. Varying effectiveness of levers to direct, incentivize, and enforce

action by nonperforming federal agencies.

4) Resource constraints and a rigid government budgeting cycle.

5) Scattered congressional oversight.

(Charlet, 2018)

Most of these challenges are the same for the state governments with the minor difference being challenge number 5. Federal agencies will be subject to congressional oversight from multiple departments, where the state governments could have better control in this respect since they are not as large. However, one advantage the federal government has over the state governments is that “federal agencies have more mechanisms in place for sharing threat intelligence than do state and local organizations, which also lack the budgets to recruit and hire the needed experts” (Ziadeh, 2015).

On the other side of the federal government cybersecurity policies are the state government’s own cybersecurity policies. The state governments “face different flavors of cybersecurity threats” (Ziadeh, 2015). For example, the primary threat to the federal government is “negligent insider followed by the zero-day attacks”, whereas state governments primary threat “is the failure to patch known vulnerabilities” (fcw.com, n.d.). The failure to patch known vulnerabilities is also due to the lack of good budgets “to recruit and hire the needed experts” (Ziadeh, 2015). All states have some sort of cybersecurity plan, but states like “Vermont and Utah were virtually silent on the topic and only touched on the need for cybersecurity in a general fashion” (Dawson & Desouza, 2016). Then there are some states who have taken cybersecurity very seriously like, New Mexico and Colorado. For example, Colorado “has clear metrics and assigns specific responsibilities” and this includes tasks like “95 percent of its systems are monitored/evaluated in real time” and “more than 90 percent of its employees have taken security awareness training” (Dawson & Desouza, 2016). The federal government has a massive number of agencies, each with their own cybersecurity policies. This is very different from the state governments that might not have as many agencies, but each state, has their own threats, budgets, and cybersecurity priorities.

## References

Charlet, K. (2018). (publication). *Understanding Federal Cybersecurity*. Retrieved October 13, 2021, from <https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf>

Dawson, G., & Desouza, K. C. (2016, July 29). *How state governments are addressing cybersecurity*. Brookings. Retrieved October 13, 2021, from <https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/>

fcw.com. (n.d.). *State of Cybersecurity in Local, State & Federal Government*. FCW. Retrieved October 13, 2021, from <https://fcw.com/pages/hpsp/hpsp-10.aspx?m=1>

Federal Information Security Modernization Act of 2014 (2014). bill. Retrieved October 13, 2021, from <https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

itdashboard.gov. (n.d.). *Our information technology investments at work*. Welcome to IT Dashboard | IT Dashboard. Retrieved October 13, 2021, from <https://myit-2021.itdashboard.gov/>

UMGC.edu. (2013, April 24). Cybersecurity Capstone Simulation Student Manual. <https://leocontent.umgc.edu/content/dam/course-content/tgs/cyb/cyb-670/document/Student_Manual-withalttext.pdf?ou=610175>

Ziadeh, A. (2015, November 4). *States vs. Feds: Who does cybersecurity better?* GCN. Retrieved October 13, 2021, from <https://gcn.com/articles/2015/11/04/fed-vs-sl-cybersecurity.aspx/>