# CS332 Midterm

## The State and Local Government Cybersecurity Act of 2021

1. What does the new “The State and Local Government Cybersecurity Act of 2021” law do?

* The State and Local Government Cybersecurity Act (S. 2520) passed in Congress which is now law since 2021, enforces Cybersecurity collaboration between the federal and local government entities (state, local, tribal, territorial). More specifically the Department of Homeland Security (DHS) will provide training, put in act new policies to the local entities, provide hands on technical assistance, and mandate information sharing ‘about Cybersecurity related risks/incidents’ between federal and local entities.

1. Describe how it impacts the Cybersecurity community and penetration testing.

* The cost estimate for implementing S. 2520 for the next 5 year period is $500,000. This might seem strange but in fact the DHS has been already conducting these coordination activities mentioned. This law is simply codifying what the DHS has already been responsible for, thus giving them the recognized authority to do so now. Because of this fact, the next 5 year period after S. 2520 comes into effect there will be actually no new operating requirements required. Looking onward I suspect that this law can have many different outcomes on Cybersecurity and penetration testing. I think that S. 2520 is laying the foundation for further legislation; specifically to increase the efforts to minimize the impact from cybercriminals domestic and abroad. Our government has been overdue on increasing the security of their systems especially due to recent tensions.
* In S. 2520 section F, there is heavy emphasis on promoting the security of elections. This will be done through collaboration between chief officials from all government entities to enforce policies and procedures related to the security of election systems. I think that in the long term this law is setting the foundation of locking down election systems and treating election systems as critical systems themselves, using the same security designs and procedures that would give them reliability and fault tolerance the likes of the power grid system and computers that send objects out of our orbit. This is a problem that has caused divide and heart- ache between the American people.
* One direction I see this impacting Cybersecurity and penetration testing in the future is the plethora of openings that need to be filled for Cybersecurity experts working for the DHS and local government entities. Due to the scope of all those jobs that need to be filled and the incompetency of the government to gather these individuals to work for the local government and the DHS, they will create new standardized education to fill these jobs. Further study on good solutions for this problem can be beneficial, a new Cybersecurity certification offered by the federal government or making Cybersecurity courses ubiquitous at every education institution at the community college and upper class high school level can prove to be beneficial; Funneling these students into roles that help the government at the local levels.
* No matter the outcome of this bill I can say that S. 2520 will negatively effect black-hat hackers by tightening up the security on low hanging fruit targets they would otherwise hack or not get caught hacking. Penetration testers will now have to be careful when running intrusive enumeration scanning techniques on IP address space ranges that might contain hosts to government entities. This is a trend that I see to continue for the noticeable future.

### Sources

* [Senate Bill](https://www.congress.gov/bill/117th-congress/senate-bill/2520/text)
* [Cost Estimate](https://www.cbo.gov/publication/57504)