# Project 6: Public-Private Partnerships for Election Systems Cybersecurity

**Before you begin:** Please remember that our purpose here is to study cybersecurity. This assignment should be approached from a non-partisan perspective and, to the maximum extent possible, resources used and cited should be from non-partisan, independent sources.

## Background

The 2020 elections were like no others in recent times due in large part to the global pandemic and increasing societal impacts as rates of infection from the COVID-19 virus increased rapidly across the United States. Individual states, who are responsible for running state and federal elections, had to pivot from primarily in-person voting to a mix of face-to-face, absentee, and mail-in ballots. The vote counting processes had to change as well since absentee and mail-in ballots usually required additional steps to verify the validity of individual ballots. Central to many ballot challenges were the technologies used to verify signatures and record votes from physical ballots. If you’re not familiar with some of the issues that arose during the post-election vote tallying, this analysis from the Constitution Center is a place to start <https://constitutioncenter.org/blog/faq-what-happens-next-in-the-presidential-election-process>

In addition to concerns raised by state governments, think tank after think tank has studied the problems of election security for years now. For example, the National Academy of Sciences published a report in 2018 that detailed many cybersecurity concerns which arose during the 2016 election (See <https://www.nap.edu/read/25120/chapter/7> ). A more recent analysis by the Brennan Center was published in September 2020 detailed additional election processes that “need improvement.” (See <https://www.brennancenter.org/our-work/research-reports/our-election-system-resilient-still-has-room-improvement> ).

Clearly, there are differences of opinion as to what the problems were with the 2016 and 2020 elections. But, there seems to be growing agreement among the state governors and the Secretaries of State who are responsible for running elections at the state level – something needs to be done to improve election security in the future. Public-private partnerships are a tool that state governments and the federal government have used with success in other areas to encourage the participation of businesses and others in developing solutions for public-policy problems.

## Your Task

**For this research project,** you will help identify best practices and strategies for encouraging business participation in public-private partnerships designed to improve cybersecurity for the US Elections System. Your deliverable will be a research report that provides an overview of existing public-private partnerships (focus on Election Security), the types of cybersecurity improvements such partnerships address, the potential benefits to industry partners, and the potential risks and/or costs in resources. Your report should also address the types of *due diligence* activities a company should engage in before committing to participation in information sharing and other public-private partnership activities.

## Research:

1. Read / Review the Weekly readings.
2. Research the concepts and structures for public-private partnerships as a means of furthering public policy goals. Your starting resources are:
	1. *What are Public Private Partnerships* (World Bank)
	<https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships>
	2. *The Policy Cycle*<https://www.policynl.ca/policydevelopment/policycycle.html>
3. Research existing or proposed public-private partnerships in cybersecurity and critical infrastructure protection for Elections Systems Security. Here are some sources to get you started:
	1. <https://gcn.com/articles/2020/02/20/government-industry-partners-election-security.aspx>
	2. <https://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf>
	3. <https://fedtechmagazine.com/article/2020/04/role-dhs-can-play-election-security>
4. Research the DHS-led public-private partnership for Critical Infrastructure Cybersecurity improvements in the area of Election Systems Security. You should also review the requirements and provisions of the NIST Cybersecurity Framework for Critical Infrastructure Protection. Research why DHS is encouraging the adoption of the NIST framework.
	1. <https://www.dhs.gov/topic/election-security>
	2. <https://us-cert.cisa.gov/ncas/tips/ST19-002>
	3. <https://us-cert.cisa.gov/resources/cybersecurity-framework>
5. Find additional sources that provide information about public-private partnerships for cybersecurity, i.e. Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations. Here are two overview/directory web pages to help you get started.
	1. <https://www.dhs.gov/isao>
	2. <https://www.cisecurity.org/ei-isac/>

## Write:

Write a five- to seven-page research report that includes a summary of your research. At a minimum, your report must include the following:

1. An introduction or overview for public-private partnershipsthat provides definitions and addresses the laws, regulations, and policies that permit this type of cooperation between federal, state, and local governments and private companies. This introduction should be suitable for an executive audience.
2. A separate section that provides an overview of public-private partnerships for Elections Systems cybersecurity that addresses the types of activities contributed by a company (e.g. information sharing, development of threat intelligence, development of risk profiles, etc.). You should provide three or more specific examples.
3. An analysis of whether participation in a public-private partnership in the area of Elections Security is likely to have benefits for businesses (with specific examples of those benefits). After you address the benefits, address the problem of costs and/or risks which a company could expect to face (with at least three or more specific examples). (One risk to consider is how a partnership exposes information about company operations to the federal government.)
4. A set of recommendations or best practices for companies to engage in before committing to participation in a public-private partnership for cybersecurity. (Address the requirement for *due diligence* in decision-making.)
5. A separate closing section in which you summarize your research and recommendation(s).

## Submit for Grading

Submit your work in MS Word format (.docx or .doc file) using the Project 6 Assignment in your assignment folder. (Attach the file.)

## Additional Information

1. Consult the grading rubric for specific content and formatting requirements for this assignment.
2. Your 5- to 7-page research report should be professional in appearance with consistent use of fonts, font sizes, margins, etc. You should use headings and page breaks to organize your paper.
3. Your paper should use standard terms and definitions for cybersecurity.
4. The CSIA program recommends that you follow standard APA formatting since this will give you a document that meets the “professional appearance” requirements. APA formatting guidelines and examples are found under Course Resources. An APA template file (MS Word format) has also been provided for your use CSIA\_Paper\_Template(TOC+TOF,2021).docx.
5. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be on a separate page at the end of your file. These pages do not count towards the assignment’s page count.
6. You should write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
7. You must credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.).