UNIVERSITY of VIRGINIA
FRANK BATTEN SCHOOL of LEADERSHIP and PUBLIC POLICY

CRITICAL ENERGY INFRASTRUCTURE CYBERSECURITY

PREPARED FOR

Booz | Allen | Hamilton

PREPARED BY

Rory Burke
Frank Batten School of Leadership and Public Policy
University of Virginia

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to thank my APP advisors this year, Professor Wyckoff and Professor Myung, for their guidance and advice throughout this process. Their constant encouragement and feedback were essential for the APP. I have learned from you both and appreciate the high levels of attention you give to your students.

Additionally, I would like to thank my wife and family for their love and support. My wife, Kristen, kept me grounded and supported me during the MPP program, and I'm grateful for her occasional and much-needed constructive criticism. Thank you to my parents- without your support, I would not be where I am today.

I would also like to thank my peers for both motivation and company. A special thanks to Dominique for the friendship, accountability bets, and great laughs over the past two years. I know you'll do great things wherever your career takes you! Thank you for challenging me and offering new perspectives.

Disclaimer: The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

Honor Code: On my honor as a student, I have neither given nor accepted unauthorized aid on this assignment or exam.

Rory O Burke

EXECUTIVE SUMMARY

Over the past several decades, globalization has allowed consumers, organizations, and companies to develop cyber infrastructure and implement strategies worldwide. The U.S. relies on secure infrastructure technology and communications to provide essential utility needs to citizens. These include clean water, stable electricity, secure internet and telecommunications, and natural gas/various fossil fuels. In recent years, foreign adversaries have committed mass-scale data breaches, infrastructure hacks, and cybercrime that harms U.S. citizens and companies. **Experts estimate that cyber-related crimes account for around $600B in annual losses from transferring wealth, trade secrets, and expertise** (Hallman, 2019). As technology advances in cybersecurity and computing, the public and private sectors must continue to invest in strengthening their resilience to cyberattacks.

Cyberterrorism continues to be an effective way for U.S. adversaries to target critical areas of our economy and wreak havoc on private industry and citizens. Moreover, cybercrime against energy infrastructure fosters doubt about America's ability to defend its national interests and domestic systems (Blair & Roth, 2022). Nation-states such as China, Iran, Russia, and North Korea are frequently at the top of state-sponsored or endorsed cyberattacks, as described in the background sections of this report.

This project analyzed the costs associated with a hypothetical 24-hr electric blackout for Fairfax County, Virginia to understand the scale and impacts of cyberattacks on critical infrastructure. Fairfax County is Virginia's largest county, with 1,139,720 people (U.S. Census Bureau QuickFacts, 2021). The total estimate for **Fairfax County direct costs of a 24-hr blackout is $67,875,181 (see Appendix A for cost breakdown).** This report was written for Booz Allen Hamilton to provide empirical research, policy options, and implementation recommendations to improve cybersecurity for the critical energy infrastructure. Below is a summary of the historical trends related to cybercrime, an overview of my three recommended policy options, and the implementation considerations of my recommendation.

Historical Trends

According to the **Federal Bureau of Investigation (FBI), data breaches, emails, and business scams increased by 126% from 2016 to 2018** (IC3, 2018). This statistic is likely much higher since not all data breaches and attacks are immediately reported to federal authorities. In May 2021, ransomware hacked the Colonial Pipeline, causing significant disruptions to U.S. East Coast gasoline and refined products distribution (Parfomak & Jaikaran, 2021). **The Colonial Pipeline is the largest fuel pipeline in the U.S., and the attack cost the company $4.4M in ransom payments via cryptocurrency to an organization with ties to Russia** (Mehrotra & Turton, 2021). The Colonial Pipeline ransomware attack also led to panic buying throughout the Southeastern U.S. states and supply shortages (Parfomak & Jaikaran, 2021).

Policy Options

- **Policy Option #1: Update to Executive Order 14028 To Improve the Nation's Cybersecurity Policy**

Policy Option #1 involves updates to Executive Order (EO) 14028 based on recommendations from cybersecurity analysts and national security experts. EO 14028 was released by the Biden Administration on May 12th, 2021, which was five days after the Colonial Pipeline attack ("Executive," 2021).

- **Policy Option #2: Invest in Research and Development Grants**

Policy Option #2 provides federal grant funding from the Department of Homeland Security (DHS) to Johns Hopkins University's (JHU) Hub for Imaging and Quantum Technologies research center ("Hub," 2022). Although this policy alternative mainly falls to private academic institutions to apply for grant funding, Booz Allen's contracts and acquisition associates can assist JHU with grant preparation.

- **Policy Option #3: Cybersecurity Online Training for an Individual Electric Company (recommended policy option)**

The final policy option is a Cybersecurity Awareness and Training (CAT) Program that shall be administered to all employees at Colonial Pipeline. The program will help employees recognize phishing email scams and malware downloads and prevent ransomware attacks. A study of roughly 20,000 employees found that cybersecurity awareness campaigns decreased the number of employees who opened a phishing campaign by 71.5% (Daenhsi et al., 2022).

Outcomes, Recommendation, and Implementation

Outcomes Matrix:

Alternative → / Criteria ↓	Policy Option #1	Policy Option #2	Policy Option #3
Cost	$18,595.6	$3,662,682.6	$42,292.7
Effectiveness	High	Medium	High
Risk	Moderate ⇨ Low	Mod. ⇨ Mod.	Moderate ⇨ Low
Political Feasibility	High	High	High
Administrative Feasibility	Moderate	High	High

This report concludes by recommending Policy Option #3 as the best-proposed solution to improve the cybersecurity of private energy companies. Implementation of Policy Option #3 requires coordination between Booz Allen Hamilton, Colonial Pipeline, and CISA officials (as needed). This program will be based on the calendar year and requires 90 days of preparation and engagement with key stakeholders before enactment.

The research used for this APP is both quantitative (literature review, defense analysis firms, and private industry analysis) and quantitative (expert opinions and industry projections).

OVERVIEW

INTRODUCTION AND PROBLEM STATEMENT

U.S. energy infrastructure's cybersecurity is a national security concern affecting all sectors, regions, and citizens. Cyberterrorism continues to be an effective way for U.S. adversaries to target critical areas of our economy and wreak havoc on private industry and citizens. Moreover, cybercrime against energy infrastructure fosters doubt about America's ability to defend its national interests and domestic systems (Blair & Roth, 2022). As described in the following sections, nation-states such as China, Iran, Russia, and North Korea are frequently at the top of state-sponsored or endorsed cyberattacks.

Problem Statement: U.S. energy infrastructure is vulnerable to cyberattacks from China, Russia, Iran, and North Korea. Power grid susceptibility allows adversaries to target critical infrastructure to cause U.S. instability and economic suffering to advance their military objectives.

This project analyzed the costs associated with a hypothetical 24-hr electric blackout for Fairfax County, Virginia, to understand the scale and impacts of cyberattacks on critical infrastructure. Fairfax County is Virginia's largest county, with 1,139,720 people (U.S. Census Bureau QuickFacts, 2021). The total estimate for **Fairfax County direct costs of a 24-hr blackout is $67,875,181 (see Appendix A, for cost breakdown).** This estimate does not include the effects of other critical infrastructure such as telecommunications, water, waste treatment, natural gas pipelines, or internet infrastructure.

This project will introduce the background of cyberattacks on critical infrastructure, discuss the cost to society of energy outages, and provide evidence-based policy options for my client to improve U.S. cybersecurity. In the first section of this report, I provide an overview of the critical energy infrastructure sector and the challenges faced by constant cyber threats. This section will also include the impacts of cyberattacks, historical trends, literature about best practices, and the costs to society of cyberattacks. In the second section, I shift from assessing the problem and causes of cyberattacks on the energy sector to providing criteria and policy alternatives to address this problem. The five criteria I used in this project are cost, effectiveness, risk, political feasibility, and administrative feasibility. I then introduce my three evidence-based policy options and evaluate their potential impacts and outcomes:

- **Policy Option #1: Update to Executive Order 14028 To Improve the Nation's Cybersecurity Policy**
- **Policy Option #2: Invest in Research and Development Grants**
- **Policy Option #3: Cybersecurity Online Training for an Individual Electric Company (recommended policy option)**

Lastly, a policy recommendation and implementation considerations are provided to ensure the policy option is sustainable for the coming decades.

CLIENT OVERVIEW

My client for the APP is Booz Allen Hamilton, a leading professional services company based out of McLean, VA. Booz Allen Hamilton has approximately 29,000 employees and serves many clients from Defense, Intelligence, Global and Commercial Spaces, and Civil Societies ("Company Factsheet," 2023). My specific client works under the Defense Sector of Booz Allen; however, the execution of this policy solution would require coordination with the Global and Energy sector of the company. Booz Allen is a management consulting firm committed to solving complex problems through innovation and data science/analytics. They have decades of experience assisting critical energy infrastructure companies in navigating technology changes and addressing digital system vulnerabilities.

Booz Allen would serve as a consultant for my APP with the private critical energy infrastructure sector. In the "fixer, doer, manager" policy implementation framework, Booz Allen would be hired as a "fixer". This role would have Booz Allen associates being the intermediary between the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), Colonial Pipeline energy company, and any stakeholders detailed in the policy alternatives section.

BACKGROUND

U.S. adversaries target the critical energy infrastructure and healthcare sectors to impact most of the population. In discussions with cybersecurity experts, cyber technology constantly evolves to face a growing and increased amount of cybercrime. For example, when cyber protection software identifies and blocks one specific ransomware or email phishing scheme, the hacking group changes tactics to avoid detection. Foreign adversaries use ransomware to hijack the computer system of a company or organization and require ransom payments to remove the ransomware infection. Scholars refer to these evolving challenges as a form of business extortion with a low likelihood of catching the perpetrators (Morse & Ramsey, 2016). One cyber security expert estimates that cybercrime costs to businesses and private citizens will reach $10.5 trillion annually by 2025 (Morgan, 2020). Cyberattacks linked to nation-state governments have increased in scale and effectiveness in recent years.

China uses cybercrime and corporate espionage to advance its economic and military objectives. In 2022, the Biden administration labeled China's Ministry of State Security as a key contributor to a 2021 Microsoft servers hack that affected at least 30,000 private and public entities (Nakashima, 2021). Military analysts point to China's massive technological advances due to the tenacious theft of U.S. defense secrets and technology (Blair & Roth, 2022).

This project focuses on the U.S. energy grid and its cyberattack susceptibility. U.S. adversaries are engaged in cyber espionage and data breaches to determine where critical U.S. infrastructure and systems may be vulnerable to potentially paralyze the United States in a crisis or military advance (Montgomery & Borghard, 2021).

The following historical trends in cybercrime and nation-state attribution to energy infrastructure attacks highlight the importance of immediate attention and solutions for this policy problem:

HISTORICAL TRENDS

1. **Colonial Pipeline Attack:** The Colonial Pipeline attack highlights cyberattack severity against domestic energy infrastructure. In May 2021, ransomware hacked the Colonial Pipeline, causing significant disruptions to U.S. East Coast gasoline and refined products distribution (Parfomak & Jaikaran, 2021). The Colonial Pipeline is the largest fuel pipeline in the U.S. and the attack cost the company $4.4M in ransom payments via cryptocurrency to an organization with ties to Russia (Mehrotra & Turton, 2021). Furthermore, the Colonial Pipeline ransomware attack led to panic buying throughout the Southeastern U.S. states and supply shortages (Parfomak & Jaikaran, 2021).

2. **The Office of Personnel Management (OPM) Hack:** The most significant hack of government officials' personal identifiable information (PII) was in April 2015. The OPM was hacked by a group of Chinese hackers, which led to the theft of 21.5 million federal employees' background information, family information, addresses, and social security numbers (Gootman, 2016). Some defense and intelligence individuals believe the Chinese government may build a database of U.S. government employees and their roles to gain access to other systems (Finklea et al., 2015).

3. **Nation-State Cyberattack Campaigns 2020-2021**: According to the Congressional Research Service, the U.S. has been increasingly targeted by other nation-states in the last two years, including Iran, China, North Korea, and Russia (Jaikaran, 2021). Attacks from these countries are designed to weaken U.S. domestic security and computing security by spying on government agencies, stealing sensitive information from private or public sector systems, and stealing intellectual property (Jaikaran). The 2021 Microsoft server hack, mentioned in the background section above, is one example of China's state entities attempting to disrupt U.S. domestic security (Nakashima, 2021).

A **data breach** is a "security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual" (Privacy Rights, 2019). Data has recently shown an increasing number of attacks on websites and personal security. The Privacy Rights Clearinghouse released a dataset with 9,015 data breaches in the U.S. from 2005 to 2019 (Africk & Levy, 2021). According to the Federal Bureau of Investigation (FBI), data breaches, emails, and business scams increased by 126% from 2016 to 2018, as shown in Figure 1 below (IC3, 2018). Financial data from these breaches can be traced to Asian banks in Hong Kong, China, Turkey, and Mexico (IC3, 2018). These trends have continued to increase in severity and scale while targeting U.S. energy infrastructure.

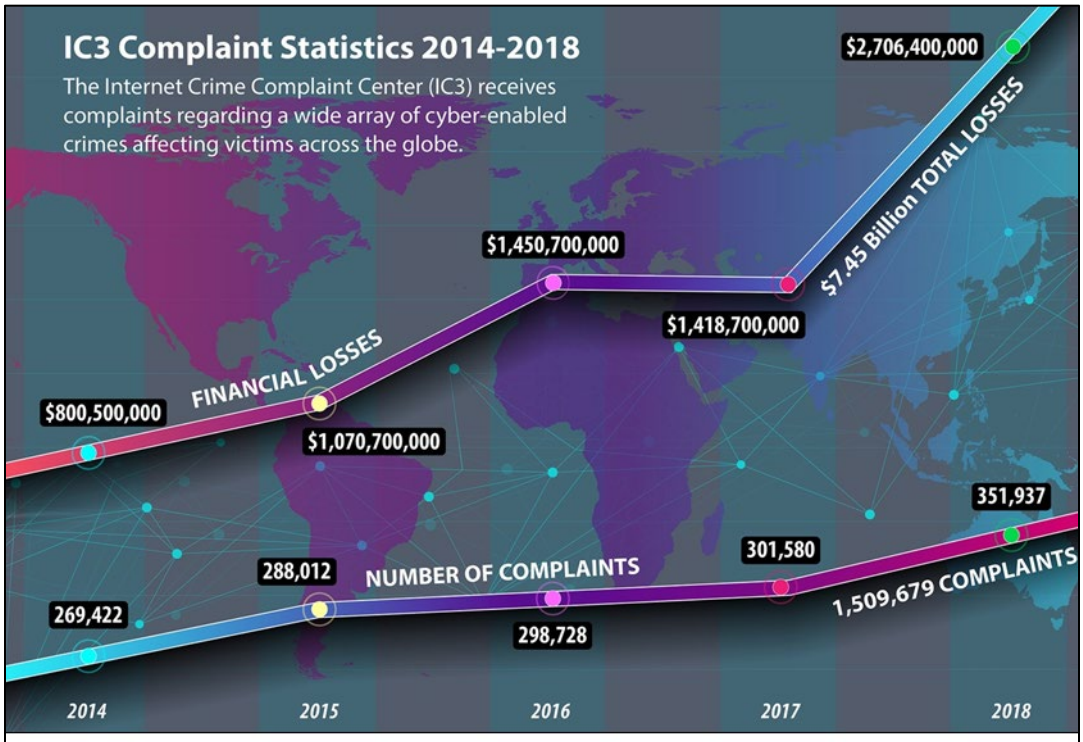

Figure 1: IC3 Complaint Statistics-Federal Bureau of Investigation (FBI)

The Department of Homeland Security identifies 16 critical infrastructures according to Homeland Security Presidential Directive 7 (see Figure 2, below), which are Federal, State, or Local essential government services or capabilities that would be susceptible to a significant loss in the event of terrorist activity (Homeland Security Presidential Directive 7, 2003). Damage to these critical infrastructures and resources could cause catastrophic health effects and mass casualties, impair essential missions, and damage the private sector's ability to maintain a

functioning economy. These 16 sectors include Energy, Food and Agriculture, Healthcare, and Nuclear Reactors (Critical Infrastructure Sectors, 2020). The Energy Sector comprises 6,413 power plants and is arguably the most important critical infrastructure that many of the other 15 sectors rely on to operate effectively (Ballou et al., 2016; Energy Sector, 2022).

The President's National Infrastructure Advisory Council (NIAC) within CISA, a nonpartisan council of executives representing public and private sector energy companies, expressed an urgent need in a December 2020 letter to President Biden for an *executive-driven* public-private partnership to set strategies and ensure accountability of all stakeholders to strengthen the nation's cyber defenses (Baich et al., 2020).

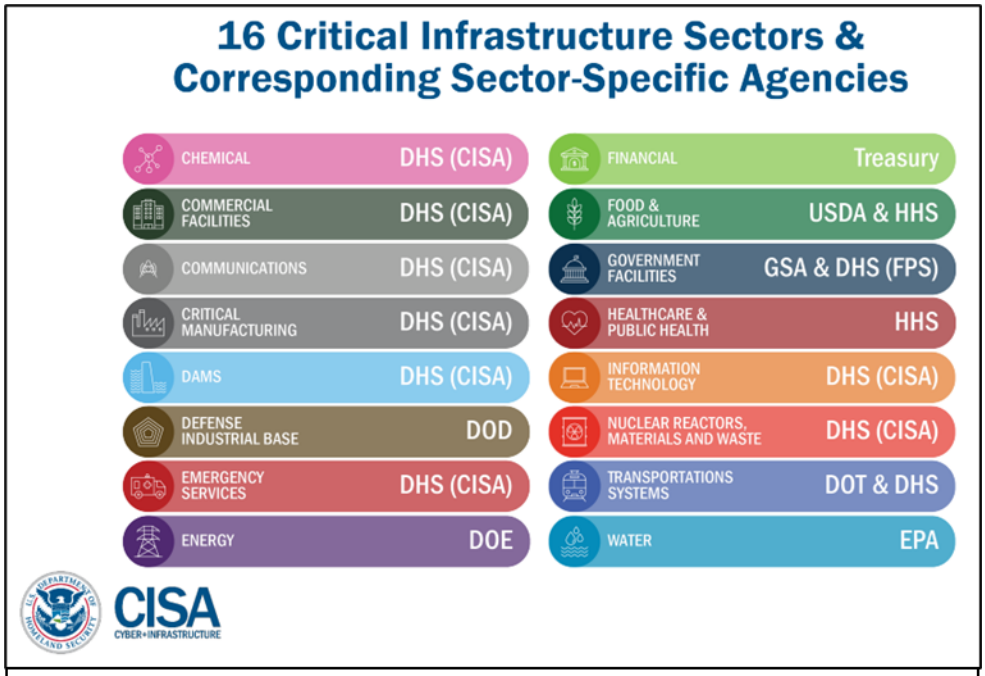

Figure 2: 16 Critical Infrastructure Sectors-CISA

IMPACTS

Cyber vulnerability and nation-state aggression towards the U.S. has already impacted our domestic energy capability. The Colonial Pipeline attack highlights cyberattacks' severity against domestic energy infrastructure. Panic buying by consumers in southeastern states caused outages and supply issues, showing policymakers and executive branch leadership how quickly a cyberattack could influence behavior and create fear around energy security (Grady, 2022).

The impacts of cyber hacking on energy infrastructure are immense for domestic and international energy sectors. Although this project focuses on the U.S. energy grid, it is vital to highlight the international implications of infrastructure vulnerabilities, primarily when they affect our NATO allies. Aggression toward NATO countries may obligate the U.S. to respond

with military or offensive cyber actions in support of Article 5 of the NATO agreement (Monov, 2019). The Center for Strategic and International Studies publishes an open-source, constantly updated list of significant global cyberattacks, many of which are against the U.S. government or private sector companies (Significant Cyber Incidents, 2022). Since the beginning of the war in Ukraine in early 2022, Russian cyber hackers have targeted Ukrainian and European allied energy infrastructure to advance their military objectives. In February 2022, several oil terminals in some of Europe's largest and most strategically important ports across Belgium and Germany fell victim to a ransomware cyberattack from a Russian-speaking hacking group (Significant Cyber Incidents, 2022). This port infrastructure attack temporarily halted the processing and movement of oil for the region. These vulnerabilities ensure that the U.S. and other oil exporting countries such as Norway and Qatar can support European energy needs. This impacts oil and gas prices for all Americans.

REGULATORY ENVIRONMENT AND FUNDING

The domestic regulatory environment for cybersecurity is multifaceted and requires coordination throughout the executive branch, government organizations, and private industry. The Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) leads the national effort to understand, manage, and reduce risk to U.S. cyber and physical infrastructure (CISA, n.d.). Figure 3 (right) shows a partial list of organizations related to U.S. cybersecurity. Funding for cybersecurity can come from various sources, including the NDAA or the President's Budget (IT Funding, 2022).

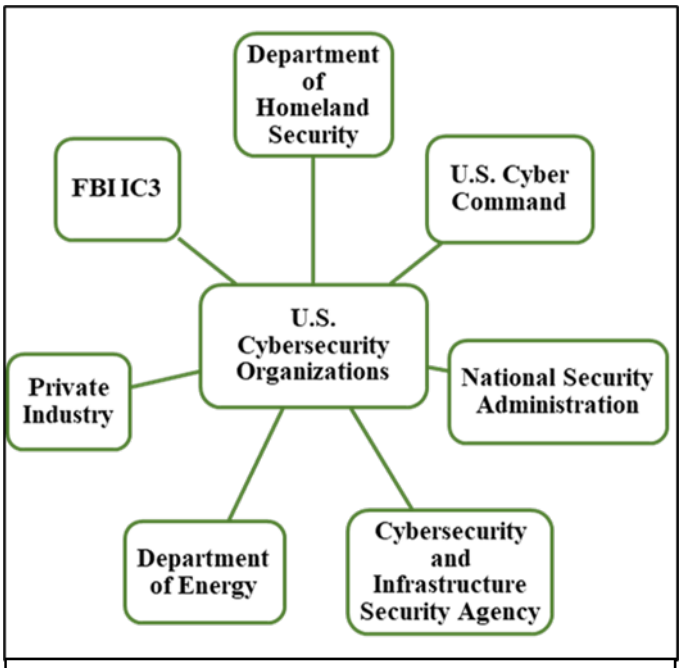

Figure 3: U.S. Cybersecurity Organizations

COSTS TO SOCIETY

Direct Costs

The costs associated with cyberattacks on domestic energy infrastructure cannot be fully quantified because of the second and third-order effects. For example, if China or Russia permanently disabled the computing capabilities of even 10% of the 6,413 U.S. power plants- the direct costs and externalities would be innumerable as it would impact every industry, citizen, and sector. Further, this would be considered an act of war, leading to a global retaliation for

American and allied forces. However, for this project, the costs associated with an electric blackout will be narrowed to 24 hours for Fairfax County, Virginia. Fairfax County is Virginia's largest county, with 1,139,720 people (U.S. Census Bureau QuickFacts, 2021). This report only focuses on the financial implications of the four electric power plants supplying energy to county residents and businesses. This estimate does not include the effects of other critical infrastructure such as telecommunications, water, waste treatment, natural gas pipelines, or internet infrastructure. The total estimate for **Fairfax County direct costs of a 24-hr blackout is $67,875,181 (see Appendix A, for cost breakdown).**

Externalities, Opportunity Costs, and Intangible Effects

During an electrical blackout period, public schools could not provide food for students. About 55,800 county students (31% of the student body) are provided free or reduced meals during an average school day (Free and Reduced-Price Meals FCPS, 2021). An estimate of $4.00 per day equates to $223,200 in food not being provided to students (School Meal Statistics, 2022). Most of the opportunity costs associated with an electric blackout are listed in the loss of business revenue or loss of wages under the direct cost section. However, this electrical blackout may also hinder a company's efficiency and prevent investing in future projects. For example, 10% of Fairfax County businesses may have lost future projects and are managing the backlog of not operating during the blackout. 10% of the county's daily business revenue is $617,771.

Psychological effects, emotional trauma, or climate-related impacts may also result from cyberattacks. Cyberterrorism may cause civil unrest or panic shopping at local grocery stores and gas stations and cause long-term mental health concerns for local communities. Households during winter months may experience frozen pipes or faulty equipment. In the summer months, vulnerable populations may be susceptible to heat exhaustion, heat stroke, or dehydration leading to higher hospitalization rates.

National Impacts

The data and costs above are estimated for a single U.S. county with approximately 1 million residents. Since the U.S. has approximately 333,186,506 people (U.S. Census Population Clock, 2022), the total county cost was used to calculate the total national cost of a 24-hour electric blackout. Therefore, the rough estimate of the **cost to society of a 24-hr blackout to the U.S. electric grid is at least $12,053,087,866** (see Appendix A).

Now that this policy topic has been introduced, provided historical trends, and detailed the cost to society of a national cyberattack, the next section of the project presents the five criteria used to evaluate my three policy options from the Executive Summary section: cost, effectiveness, risk, political feasibility, and administrative feasibility. These criteria will assess the range of policy alternatives for Booz Allen Hamilton to improve the cybersecurity resilience of private energy firms.

CRITERIA

COST

This criterion represents the total cost of the policy alternative for my client and the private energy company**.** This cost includes a given policy option's labor, material, or opportunity costs. I will use publicly available Bureau of Labor Statistics information for hourly occupation data. Grant proposal estimates are based on previously submitted and awarded federal cyber grants.

EFFECTIVENESS

Effectiveness is measured by the projected decrease in cybersecurity incidents in the year following implementing a given policy alternative. I used empirical research on the percent decrease in cyberattacks or ransomware takeovers from similar interventions to determine projected effectiveness. If implemented, Booz Allen Hamilton will receive input data from a company's Chief Technology Officer- or equivalent role- regarding the actual metrics of cyberattacks. Effectiveness is measured by the projected percent decrease in successful breaches that may halt or interrupt critical energy resources. Effectiveness is not measured by preventing any hacking group from targeting an electric utility service. Table 1 explains the three criteria to assess the effectiveness of a strategy.

Table 1 Effectiveness Rubric:

	Low	Medium	High
What is the expected change in successful cyberattacks in the first year after implementing a policy alternative?	0-10% decrease in successful cyberattacks for a single electric utility company	10-20% decrease in successful cyberattacks for a single electric utility company	>20% decrease in successful cyberattacks for a single electric utility company

RISK

This criterion is categorized by the expected economic losses of a cyberattack to critical energy infrastructure and the vulnerability of a system after implementation. The risk criterion is based on The Institute for Defense Analyses (IDA) cyber risk assessment of dams and navigation locks for the U.S. Army Corps of Engineers (USACE) (Seda-Sanabria et al., 2016). IDA conducted a mathematically rigorous and robust risk assessment of critical dam infrastructure to best prepare for a future cyber or physical attack. The IDA model has been modified to the economic loss of cyberattacks for critical energy infrastructure. Table 2.1 assesses each policy alternative and assigns a cyber risk rating for each energy company. The inputs to Table 2.1 are determined from Table's 2.2 and 2.3, respectively.

The cyber vulnerability rating (see Table 2.2 below) is defined as the probability of a cyberattack defeating current cyberattacks. The cyber package is a general category based on various aspects of a company's cyberattack mitigation strategy (e.g., Incident Response Plan, cyber infrastructure, annual training, etc.). This is a subjective categorical decision based on client judgment and expertise. See Appendix A for the mathematical risk equation, consequence rating, vulnerability rating, and supplemental information for this criterion.

Table 2.1 Risk Matrix:

Vulnerability Rating	Consequence Rating				
	Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Extremely High (Cyber Package 0)	Very Low	Low	High	Very High	Very High
High (Cyber Package 1)	Very Low	Low	Moderate	High	Very High
Moderate (Cyber Package 2)	Very Low	Low	Moderate	Moderate	High
Low (Cyber Package 3)	Very Low	Low	Low	Low	Moderate
Extremely Low (Cyber Package 4)	Very Low	Very Low	Very Low	Low	Low

Table 2.2 Cyber Vulnerability Rating-Cyber Package Description:

Cyber Defense Package	Description	Rating
Cyber Package 4	Robust cyber infrastructure, complete IT support for size of organization, annual training requirements, independent annual audit, Chief Technology Officer, complete Incident Response Plan	Extremely Low
Cyber Package 3	Substantial cyber infrastructure, full IT support for size of organization, annual training requirements, Chief Technology Officer, complete Incident Response Plan	Low
Cyber Package 2	Complete cyber infrastructure, full IT support for size of organization, Chief Technology	Moderate

	Officer, incomplete Incident Response Plan	
Cyber Package 1	Basic cyber infrastructure, limited IT support, Chief Technology Officer, incomplete Incident Response Plan	High
Cyber Package 0	Insignificant infrastructure, IT support, annual training, or Chief Technology Officer	Extremely High

The consequence rating is based on the economic losses of an electric utility company being hacked and unable to provide essential utilities to consumers (see Table 2.3 below). The economic loss is determined by the size of the electric utility company and the current number of customers.

Table 2.3 Consequence Rating:

Economic Loss Consequence				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
< $500K	**$500K < X ≤ $1.0M**	**$1.0M < X ≤ $5.0M**	**$5.0M< X ≤ $10.0M**	**> $10M**

POLITICAL FEASIBILITY

Political feasibility is the likelihood that key stakeholders will endorse and support each alternative, using assumptions based on the political or organizational climate. Political feasibility was measured on a low, moderate, and high scale. High feasibility options are bipartisan initiatives with limited political friction by congressional committees or electric company chief executives. Table 3 outlines the political feasibility rubric.

Table 3 Political Feasibility Rubric:

	Low	Medium	High
What is the expected political climate for the stakeholders involved with a policy alternative?	The climate is expected to be contentious and face bipartisan disagreements	The climate is expected to encounter moderate disagreement, however, can be settled through compromise.	The climate is expected to encounter limited political friction or barriers to implementation

What is the expected organizational climate for an electric utility company involved with a policy alternative?	The organizational culture is contentious and institutional resistance to change	The organization is willing but reluctant to make major changes to a policy alternative	The organization has a high willingness and ability to change

ADMINISTRATIVE FEASIBILITY

Administrative feasibility is determined based on the resources required to adopt and implement an alternative. Policy options with high feasibility currently have systems and management positions to enact a policy. This criterion considers the feasibility of Booz Allen Hamilton's ability to facilitate a given policy option. Additionally, administrative feasibility applies to whether executive branch agencies and electric utility companies can apply recommendations. Administrative feasibility will be measured on a low, moderate, and high scale, outlined below in Table 4.

Table 4 Administrative Feasibility Rubric:

	Low	Medium	High
What is the expected administrative process associated with a policy alternative?	Low if the process is burdensome and unable to be accomplished with current resources and constraints. Low feasibility involves nine or more key stakeholders in the policy alternative.	Medium implementation may encounter moderate challenges but can be accomplished within the established timeline. Medium feasibility has less than 5-8 key stakeholders involved in the policy alternative.	High if the process is projected to face minor administrative challenges. High feasibility has less than 4 key stakeholders involved in the policy alternative.
Is this policy alternative expected to be supported by company staff?	No	Yes, however, may need additional workforce supplementation	Yes

FINDINGS

Booz Allen Hamilton is interested in policy recommendations to improve the cybersecurity environment for critical energy infrastructure. As a defense consulting organization, they have divisions focused on cyber security, national security, and digital solutions. They would act as a consultant for this project when executing any of the policy alternatives.

Scope and Scale

Client: Booz Allen Hamilton hired as a consultant for Colonial Pipeline.

Prospective customer/firm requesting consulting services: Colonial Pipeline (see Background section) was chosen as a hypothetical customer for Booz Allen Hamilton's consulting services. This private energy company was chosen because the May 2019 cyberattack highlighted the severity and scope of a critical energy attack for millions of Americans (Parfomak & Jaikaran, 2021). Additionally, this case study provided costs associated with the ransomware attack, congressional hearings after the attack, and was mentioned in Executive Order 14028 ("Executive," 2021).

Cost to Society: Since Colonial Pipeline infrastructure spans the southeastern region of the U.S., including northern Virginia (see Figure 4 below), the cost to society section narrowed an electric blackout to 24 hours for Fairfax County, Virginia ("System map", 2023). Because Colonial Pipeline infrastructure provides utility services through northern Virginia, Fairfax County was chosen to provide adequate scope to estimate the business and economic costs of a 24-hr utility disruption.

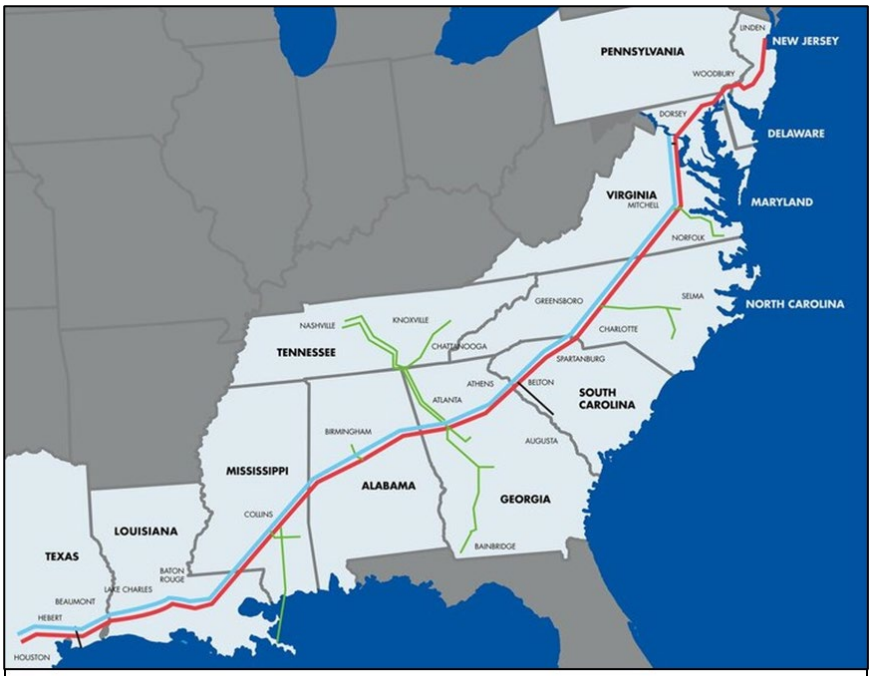

Figure 4: Colonial Pipeline Map

Figure 5 (right) framework describes how my client could approach an electric company's susceptibility to foreign nation attacks. Policy Option #1 is a "top-down" approach to propose changes to an Executive Order for strict federal requirements regarding cybersecurity. Policy Option #2 develops medium and long-term technological advancements to improve cybersecurity conditions for private industry. Lastly, Policy Option #3 is a "bottom-up" approach to improve the user capability and resilience to malware attacks from foreign countries that may degrade a company's cyber infrastructure.

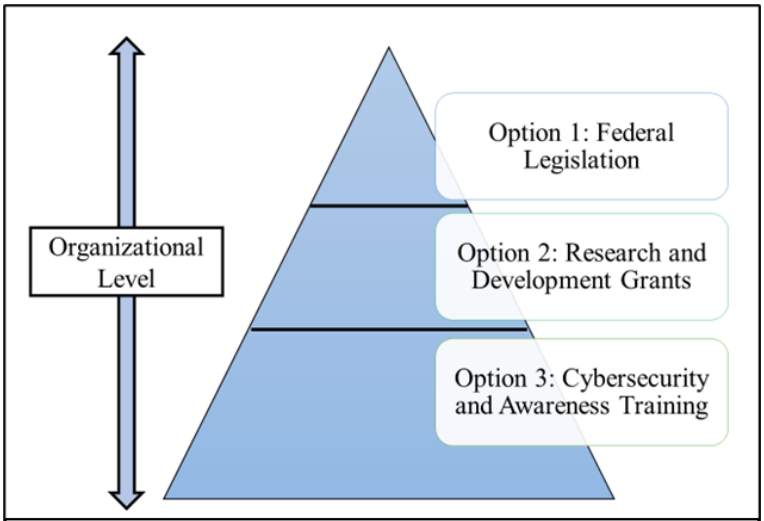

Figure 5: Policy Alternatives Organization Level Chart

POLICY OPTION #1: UPDATE TO EXECUTIVE ORDER 14028 TO IMPROVE THE NATION'S CYBERSECURITY POLICY

Policy Option #1 involves updates to Executive Order (EO) 14028 based on recommendations from cybersecurity analysts and national security experts. EO 14028 was released by the Biden Administration on May 12th, 2021, which was five days after the Colonial Pipeline attack ("Executive," 2021). This executive order was focused on government agencies' role and oversight in the coordination with the private sector and improving the supply chain for the cybersecurity software market. According to Harding and Ghoorhoo (2022), the executive order did not include the following critical requirements for private infrastructure companies that proactively approaches the cybersecurity issue in the U.S.:

1. Private industry must conduct contingency planning for inevitable ransomware attacks and be held accountable by CISA.
2. EO 14028 did not include any guidelines or requirements for employee awareness training or annual cyber hygiene.

I propose a policy option that includes the previously mentioned federal guidelines for cybersecurity and adds strict federal mandates for adherence to regulations. To accomplish this, Booz Allen Hamilton would serve in an advisor/policy advocate role with executive branch agencies.

The EO update should include language drafted by CISA and DOJ General Counsels to enforce company adherence to cybersecurity protocols. In short, the update will allow companies twelve months to comply with CISA contingency planning recommendations and develop an Incident Response Plan (IRP) to prepare for future cyberattacks or be fined by CISA and DHS. Companies must submit their IRPs to CISA based on the NIST Frameworks. If companies do not

comply after the federal fine, the DOJ may escalate to further restrictions based on legislative authority such as prosecution.

Policy Option #1 Evaluation:

Cost: **Total cost to update EO 14028 is minimal for my client, estimated at around $18,595** (see Appendix B for a detailed cost analysis breakdown). The main cost covers Booz Allen Hamilton associates coordinating with White House press points-of-contact, the Office of Management and Budget (OMB), the Senate and House Committee on Homeland Security, and think tanks (e.g., Center for Strategic & International Studies or the Heritage Foundation). Policy Option #1 has no cost to a private energy company. All costs and administrative coordination are between Booz Allen, OMB, congressional representatives/offices, and think tanks.

Effectiveness: **Policy Option #1, if implemented, would have high effectiveness in decreasing successful cyber-attacks**. A study of roughly 20,000 employees found that cybersecurity awareness campaigns decreased the number of employees who opened a phishing campaign by 71.5% (Daenhsi et al., 2022). Additionally, research indicates that an Incident Response Plan protects the critical aspects of a business's operations and can limit the time a system is degraded after an attack (Lewis, 2016). A 2020 study investigating nine significant global cyber-attacks on critical infrastructure or healthcare systems cited a cyber standard operating procedure (SOP) and capability training for staff members as key measures to prevent future attacks (Turell et al., 2020).

The impermanence of executive orders may reduce Policy Option #1's long-term effectiveness as legislative action. Scholars estimate that frequent executive orders enact temporary policy changes but create a pendulum effect with changes in administration (Wallach, 2020). The pendulum effect of constantly changing regulation can harm the industry, especially when language is intentionally broad and implementation can be nuanced. Therefore, the effectiveness of Policy Option #1 may be lower if a new president is elected in 2024. A change in presidential and executive branch agency leadership may remove or alter all previously signed executive orders under the Biden Administration.

Risk: Policy Option #1 assessed the change in risk rating from moderate to low risk for Colonial Pipeline. Prior to enacting Option #1, Colonial Pipeline was assigned the following vulnerability and consequence ratings (see Appendix A for rating details):

- Cyber Package 2: Complete cyber infrastructure, total IT support for the size of the organization, Chief Technology Officer, incomplete Incident Response Plan
- Level 3 economic loss consequence: $\$1.0M < X \leq \$5.0M$. This is based on the total ransom payments and cost of the 2019 Colonial Pipeline attack described in the background section.

After implementing Policy Option #1, Colonial Pipeline's cyber package 2 (moderate vulnerability) was upgraded to cyber package 3 (low vulnerability) based on the additional criteria of a required Incident Response Plan (IRP) and annual cyber training requirement per Table 2. There is no change to the economic loss consequence rating. Although the overall risk category improves for Policy Option #1, this alternative may not continue to improve the risk for subsequent fiscal years due to the impermanence of executive actions.

Political feasibility: An update to EO 14028 has high political feasibility. The executive order was previously drafted and released under the Biden Administration with input from the Democrat-controlled House and Senate Committees on Homeland Security. Although the House Committee on Homeland Security is Republican-controlled, Chairman Mark Green (R-TN) is a proponent of increased federal oversight and regulation related to cybersecurity. Chairman Green previously cosponsored a bill to strengthen CISA's ability to address cyber threats on Federal government systems ("Rep. Mark," 2020).

Administrative feasibility: **Option #1 ranks moderate for administrative feasibility**. This alternative involves seven key stakeholders in the implementation: Booz Allen, CISA leadership, CISA's President's National Infrastructure Advisory Council (NIAC), Office of Management and Budget (OMB), White House Chief of Staff, and potentially the House and Senate Committees on Homeland Security. Executive branch departments may be overwhelmed with more pertinent current events and less engaged in cybersecurity regulations. Likewise, the Office of Management and Budget (OMB) may be unable to draft and update the executive order before the 2024 Presidential Election.

POLICY OPTION #2: INVEST IN RESEARCH AND DEVELOPMENT GRANTS

Policy Option #2 expands federal grant funding for R&D. My client is particularly interested in next-generation cyber technology and infrastructure, including machine learning and quantum computing. Direct cybersecurity funding should focus on emerging technologies such as cloud architecture, artificial intelligence, and automation to improve an organization's ability to protect itself from cyber threats (Kramer & Butler, 2019). According to The Institute for Defense Analyses Science and Technology Policy Institute (IDA-STPI), a non-Federal critical energy company's ability to carry out R&D efforts to improve its cybersecurity is hindered by the priority to carry out its continuity of operations (Lev et al., 2016). In short, private energy companies focus on day-to-day utility responsibilities and do not prioritize R&D to improve their cybersecurity resilience. Option #2 will use federal funding to develop cyber technology at a single university- Johns Hopkins University (JHU).

Johns Hopkins University (JHU) is a leading research institution in quantum and cyber technology and recently partnered with the U.S. Department of Energy to develop next-generation devices (Schroeder, 2020). Policy Option #2 provides federal grant funding from the DHS to JHU's Hub for Imaging and Quantum Technologies research center ("Hub," 2022). Although this policy alternative mainly falls to private academic institutions to apply for grant funding, Booz Allen's contracts and acquisition associates can assist JHU with grant preparation.

Current research does not determine causal claims related to cyber grants. Gordon et al. (2015) find that private industry tends to underinvest in cyber technology, and their model shows that government incentives increase the amount and frequency of subsequent investments. Therefore, a federal grant might improve energy sector cybersecurity through university research. The DoD's research, development, testing, and evaluation (RDT&E) sector was analyzed as a comparison for the effectiveness of government investment in academia.

The U.S. is a global leader in science and technology, and the DoD accounts for approximately 41% of all federal R&D appropriations, with $65.7B in FY22 (Sargent, 2022). DoD RDT&E funding is divided into seven categories, each with a specific activity code, 6.1-6.8 (see Appendix C). Recent NDAAs have significantly increased the DoDs RDT&E budget, specifically for quantum computing and cybersecurity. The FY24 NDAA request released in March 2023 increased the RDT&E budget to $145B to address capability gaps and keep pace with our foreign adversaries, mainly Russia and China ("Department of Defense Releases," 2023). The FY24 budget document requests $13.5B for enduring cyberspace missions, hardening DoD networks, and increasing cybersecurity support for contractors ("Pentagon Boosts," 2023). Therefore, cybersecurity is a top national security priority, especially given the pace of changing cyber technology and innovation.

The renewable energy sector literature also supports Policy Option #2's effectiveness. Scholars evaluated the effectiveness of federal grant funding to improve investment in renewable energy and achieve clean energy goals under the American Recovered and Reinvestment Act (ARRA) of 2009 (Lim et al., 2020; Lim et al., 2021). A comprehensive Del Rio Gonzalez (2009) study found that policy support is critical for private industries to invest in technology to combat environmental issues. Lim et al. (2021) present a model that concluded that ARRA increased innovation, patent applications, and overall jobs in the subsequent years after the ARRA was implemented. The ARRA was studied using an Instrumental Variable (IV) research design and controlled for Gross State Product (GSP), state fixed effects, and the political party of the state governors. Lim et al. (2021) strongly argued about the 1–5-year effect of the policy intervention and concluded that ARRA funds successfully stimulated innovation in the renewable energy sector. Preliminary data showed adverse effects on patent applications and job creation; however, the data proved positive and statistically significant when expanding the time frame. Thus, federal grants for cyber technology awarded under Policy Option #2 should lead to more innovation within the industry and job creation.

Researchers in Poland used regression-discontinuity evidence to evaluate innovation policy in the science sectors of various countries (Bruhn & Mckenzie, 2019). Their findings suggest that federal grants in the science sector increase the probability of a specific project being completed by nearly 60 percentage points. Bruhn & Mckenzie (2019) also discovered that national funding leads to more science-industry collaboration and domestic patents. Based on the growth and innovation from government investment in the renewable energy sector, government grants will improve cyber technology and provide numerous hardware and software options for domestic energy companies to improve their IT systems. Additionally, expanding R&D efforts for cyber technology would likely increase employment statistics and provide local economic growth through funding, as seen in the environmental sector.

Policy Option #2 leverages previously passed legislation to enable research and development efforts. This policy option will seek grant funding previously passed by Congress in the 2022 Chips and Science Act ("Fact," 2022). This alternative is a long-term solution (5-10 + years) to ensure academia and private industry continue to advance technology and security capabilities for energy companies.

Policy Option #2 Evaluation:

Cost: Policy Option #2 includes two main areas: 1) federal grant money awarded to Johns Hopkins University for quantum computing and cyber technology, and 2) consulting expenses for Booz Allen Hamilton. The **total cost of Option #2 is $3,662,683** (see Appendix C for cost breakdown). Grant estimates are based on previous grant proposals submitted to the federal government. JHU was awarded $3.66 million in 2022 to assist with cyber technology development and fund education expenses for future industry experts ("Information," 2022). Appendix C details the DHS's cyber grant program and annual funding allocations.

Effectiveness: **Policy Option #2 ranks medium in the effectiveness criterion**. Government investment in private industry technology can increase innovation and has additional benefits such as increased jobs and market competition (Lim et al., 2021). The IDA Cost Analysis and Research Division (IDA-CARD) was used to determine best the effectiveness of government R&D funding for software or improved cyber technology. A 2016 IDA CARD report estimated that **research, development, and acquisition of new software could improve the overall capability of a system by 15 to 20% in the first year of a program** (Tate & Bailey, 2022). This data is based on whether the Defense Department received a prototype or Minimally Viable Capability Release (MVCR) from a private company within the first year of receiving federal funds and followed clear development and code requirements. Since Policy Option #2 allocates federal funds from the DHS, this study supports a medium effectiveness criterion for the R&D of cyber-related technology.

Risk: Policy Option #2 risk category for Colonial Pipeline is moderate. Prior to enacting Policy Option #2, Colonial Pipeline was assigned the following vulnerability and consequence ratings (see Appendix A for rating details):

- Cyber Package 2: Complete cyber infrastructure, full IT support for the size of organization, Chief Technology Officer, incomplete Incident Response Plan

- Level 3 economic loss consequence: $1.0M < X ≤ $5.0M. This is based on the total ransom payments and cost of the 2019 Colonial Pipeline attack described in the background section.

After implementing Policy Option #2, Colonial Pipeline does not change the Cyber Package based on upgrades or changes to the current cyber infrastructure system. There is also no change to the economic loss consequence rating. Therefore, Option #1 maintains a moderate risk rating.

Political feasibility: Policy Option #2 has high political feasibility due to the current allocation of grant funding to the Department of Homeland Security to support state, and local-level cyber R&D. Key stakeholders at Johns Hopkins University would also support cyber initiatives that would bring expertise and additional research opportunities to the university.

Administrative feasibility: Research and development grants to support emerging technology **scores moderate regarding administrative feasibility**. This criterion involves four key stakeholders involved in the implementation: 1) Booz Allen consultants, 2) JHU grant committees, 3) JHU's Hub for Imaging and Quantum Technologies Research Center, and 4)

Maryland's State Administrative Agencies (SAAs) for DHS grant requests. Although the university has a grant process for applying for federal grants, the administrative application process for cyber grants may get superseded by more pressing topics deemed by the university. Likewise, the DHS may prioritize other institutions or cyber initiatives.

POLICY OPTION #3: CYBERSECURITY ONLINE TRAINING FOR AN INDIVIDUAL ELECTRIC COMPANY

The final policy option is a Cybersecurity Awareness and Training (CAT) Program that shall be administered to all employees at Colonial Pipeline. Researchers suggest that CAT can allow organizations to identify the cyber-security weaknesses in their networks and systems (Kramer & Butler, 2019). The CAT Program is free since Colonial Pipeline will use the free Federal Virtual Training Environment (FedVTE) provided by CISA at no cost ("Public," 2023). Policy Option #3 recommends the "Cyberessentials" 1-hour course. The program will help employees recognize phishing email scams and malware downloads and prevent ransomware attacks. A 2020 international report surveyed over 3,500 employees and concluded that 69% of organizations were infected with ransomware, and roughly half agreed to pay the demanded ransom to access their systems (Proofpoint Annual Point, 2020).

Policy Option #3 Evaluation:

Cost: Based on a company with 900 employees, **Policy Option #3's cost is $30,221 to Colonial Pipeline and $12,072 to Booz Allen Hamilton for a total cost of $42,293**. All assumptions made for the cost analysis can be found in Appendix D. Most companies make professional development hours part of an employee's annual wage. These include online modules such as company benefits, sexual harassment prevention and reporting, and workplace ethics training. If the company included the "Cyberessentials" course in annual required training that was already being covered by employee wages, Policy Option #3's cost would drastically decrease to $6,479 for Colonial Pipeline.

Effectiveness: According to the National Institute of Standards and Technology Cybersecurity Division, email phishing awareness training decreases an employee's click rate on phishing attacks by about 15% (Dawkins & Jacobs, 2022). This data is based on 15 training exercises over 4.5 years and varies slightly by the specific email phishing campaign. Likewise, a study of roughly 20,000 employees found that cybersecurity awareness campaigns decreased the number of employees who opened a phishing campaign by 71.5% (Daenhsi et al., 2022).

Although current annual attempts or successful cyberattacks are unavailable from Colonial Pipeline, security firms have studied the exponential rise in ransomware attacks on businesses. According to estimates by Cybersecurity Ventures, businesses fell victim to ransomware attacks every 14 seconds in 2019 (Morgan, 2019). Moreover, the FBI reports ransomware hit U.S. critical infrastructure at least 649 times in 2021 ("Internet," 2021). Based on this research related to the effectiveness of cybersecurity awareness training and the prevalence of ransomware attacks on critical infrastructure, **Policy Option #3 has effectiveness criteria of high**.

Risk: Policy Option #3 assessed risk changed from moderate to low risk for Colonial Pipeline. Prior to enacting this policy option, Colonial Pipeline was assigned the following vulnerability and consequence ratings (see Appendix A for rating details):

- Cyber Package 2: Complete cyber infrastructure, total IT support for the size of organization, Chief Technology Officer, incomplete Incident Response Plan

- Level 3 economic loss consequence: $1.0M < X ≤ $5.0M. This is based on the total ransom payments and cost of the 2019 Colonial Pipeline attack described in the background section.

After implementing Policy Option #3, Colonial Pipeline's cyber package 2 (moderate vulnerability) was upgraded to cyber package 3 (low vulnerability) based on the additional annual cyber training requirement and tasking for the IT personnel. There is no change to the economic loss consequence rating.

Political feasibility: According to a congressional hearing after the May 2021 pipeline cyberattack, Colonial Pipeline leadership is committed to ensuring their critical infrastructure is protected against ransomware malware attacks and will "continue investing in cybersecurity and strengthening our systems" ("Hearing," 2021). There is no evidence that Colonial Pipeline leadership would be apprehensive about enacting training programs to prevent all employees from being susceptible to a ransomware attack. **Therefore, Policy Option #3's political feasibility is high.**

Administrative feasibility: **The administrative feasibility for Option #3 is high.** This criterion involves three key stakeholders involved in the implementation: 1) Booz Allen consultants, 2) Colonial Pipeline C-suite, 3) Colonial Pipeline's IT Department. At the time of the Colonial Pipeline attack, the company did not have a Chief Information Security Officer (CISO) and added an executive seven months after the pipeline attack (Jones, 2022). Moreover, Colonial added a Chief Information Officer in June 2022 to improve its ability to respond to threats and strengthen its infrastructure ("Colonial Pipeline Names," 2022).

OUTCOMES MATRIX

Table 5 Outcomes Matrix:

Alternative → / Criteria ↓	Policy Option #1	Policy Option #2	Policy Option #3
Cost	$18,595.6	$3,662,682.6	$42,292.7
Effectiveness	High	Medium	High
Risk	Moderate ⇨ Low	Mod. ⇨ Mod.	Moderate ⇨ Low
Political Feasibility	High	High	High
Administrative Feasibility	Moderate	High	High

RECOMMENDATION

I recommend Policy Option #3, the cybersecurity awareness training for my client. Although Policy Option #3 has the second highest cost, the total cost could be reduced from **$42,292.70 to $18,550.70** if the electric utility company included the cyber training in annual employee training. Additionally, Policy Option #3 has the most robust empirical research suggesting that it will reduce the amount of successful cyberattacks and ransomware attempts. A study of roughly 20,000 employees found that cybersecurity awareness campaigns decreased the number of employees who opened a phishing campaign by 71.5% (Daenhsi et al., 2022). Policy Option #3 was recommended over Policy Option #1 (Updating the Executive Order) due to the impermanence of executive actions for long-term sustainable policy.

Based on the cybersecurity literature, Policy Option #3 is likely to improve the current cyber situation of a private company in the shortest amount of time. Cybersecurity experts have noted that foreign adversaries relentlessly target critical industries (Marks & Schaffer, 2022). Therefore, the sooner a policy alternative can be implemented, the better. The risk profile was identical for Policy Option's #1 and #3; however, the political and administrative feasibility was higher for Policy Option #3.

Policy Option #2, the research and development grant, should not be discredited due to the high costs and extended period before implementation. John Hopkins University, or a similar academic institution, could develop next-generation cyber software or technology (e.g., quantum computing and internet protocols) that drastically improve the current private industry capability to thwart consistent cyberattacks. According to IDA-STPI, a non-Federal critical energy company's ability to carry out R&D efforts to improve its cybersecurity is hindered by the priority to carry out its continuity of operations (Lev et al., 2016). Thus, private energy companies focus on day-to-day utility responsibilities and do not prioritize R&D to improve their cybersecurity resilience. Policy Option #2 would direct federal funds to improve cybersecurity for the critical energy sector.

If Policy Option #3 is successfully executed at an individual company, this case-study method can be scaled to a larger regional group of energy companies. Policy Option #3 standardizes cybersecurity online training protocols based on federal cyber recommendations since CISA developed the training. There are also positive spillover effects for Policy Option #3. For example, employees who complete the annual required training will likely be more cognizant of personal data breach attempts outside of the workplace. This may prevent the stressful and time-consuming activity of dealing with a stolen personal identity, compromised email account, or stolen banking or financial information.

IMPLEMENTATION

Implementation Overview

Implementation of Policy Option #3 requires coordination between Booz Allen Hamilton, Colonial Pipeline, and CISA officials (as needed). This program will be based on the calendar year and requires 90 days of preparation and engagement with key stakeholders before enactment. This 90-day period allows Information Technology staff to provide detailed instructions and establish a fifteen-person focus group of employees to conduct the training. The annual cybersecurity training will be issued to employees on January 1st, with a completion date of October 31st. This allows for approximately 60 days to follow up with employees that still need to complete the training or provide waivers due to operational/job constraints or emergency leave situations. Cybersecurity training will also be required of all employees during the new hire process.

Comparable Program Implementation

Policy Option #3's implementation would mimic the Department of Defense (DoD) cyber requirements for DoD contractors and small businesses engaged in official business with defense agencies ("Defense," 2023). Starting in 2009, the DoD and Director of National Intelligence (DNI) required that private companies must adhere to two requirements aligned with NIST Security Frameworks: 1) provide adequate security and software to protect defense information on unclassified systems, and 2) rapidly report cyber incidents and cooperate with federal entities to protect systems and defense data ("Defense," 2023).

One way that the DoD was able to institute these requirements is to allow contractors or small businesses to outsource these requirements. Companies could hire outside security firms to assist with Incident Response Plans (IRP) and online cybersecurity training modules. In 2021, the Department of Justice (DoJ) followed suit by issuing a memorandum that would hold defense contractors and small businesses working with the DoD legally liable for not reporting cyber breaches and not adhering to NIST Cyber Frameworks ("Justice," 2021). Additionally, this memorandum established the Justice Department's new Civil Cyber-Fraud Initiative that would pursue civil penalties for companies that jeopardize citizen security and public trust.

Stakeholders and Next Steps

1) Booz Allen Hamilton: Booz Allen will coordinate with Colonial Pipeline and assist administratively with implementing Policy Option #3. Their first step will be to contact Colonial Pipeline's Chief Technology Officer (CTO) to provide information about the policy benefits and the empirical literature supporting this alternative.

2) Colonial Pipeline C-suite, Board of Directors, and Information Technology (IT) Personnel: Responsible for drafting company memorandums and policies that require annual cyber awareness training aligned to NIST Frameworks (see Appendix D). Overall, Colonial Pipeline leadership should support this policy option since the cost to the company is relatively low, and the effectiveness criterion is high. The CTO will need to address access to computers for all employees and manage the IT

professionals currently employed at the company. Colonial Pipeline leadership should also establish an internal focus group to complete the CISA training modules and provide user feedback. This allows IT personnel to develop a step-by-step employee guide to completing the training and provide company management with proof of completion.

3) Colonial Pipeline employees: Employees may be split on whether they support an annual cybersecurity awareness training. On the one hand, this added requirement increases workplace duties and may burden some sectors of the company, especially those who do not work on a computer daily. Conversely, employees may support this training opportunity as it allows them to develop critical skills to prevent cyber intrusions. Likewise, this training could be added to a CV or resume to benefit the employee, especially if they enroll in multiple CISA training courses or certifications.

4) CISA/DHS office representatives and administrative leadership: CISA personnel should fully support this policy option as it aligns with federal recommendations for improving the energy infrastructure. If the CISA training website becomes inundated with users or has technical issues, this may present a problem for CISA's IT Department.

5) The President's National Infrastructure Advisory Council (NIAC): NIAC includes leaders from the private sector and state/local government who advise the White House on how to reduce physical and cyber risks within the critical infrastructure sector ("Council," 2023). NIAC's role is to include findings and recommendations in an annual or biannual report to the executive branch to strengthen energy companies' resilience to cyberattacks.

Potential Implementation Challenges

One major implementation challenge for private companies is simply the refusal to implement the training without a federal requirement or potential civil charges. As seen in the mentioned example of the DoD requiring private companies to adhere to a basic set of cybersecurity frameworks, the Justice Department had to establish a legal precedent to hold companies accountable. Due to the cost to society of cyberattacks, especially when dealing with national security priorities. To encourage adherence to CISA guidelines and adopt cyber awareness and training practices, CISA could conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to all CEOs of identified critical energy infrastructure. This TS/SCI briefing recommendation was originally established with a 2019 NIAC letter to President Biden discussing different tactics and strategies to make cyber intelligence actionable (Lau et al., 2019). This one-day briefing intends to build a case for company C-suite executives to counter severe cyber threats and engage in proactive cybersecurity training and awareness.

Another approach my client may use to encourage private companies to adhere to federal recommendations is to focus on the benefits to the company and their employees of lowered susceptibility to cyberattacks (Daenhsi et al., 2022). For example, an annual workplace training focused on ransomware, phishing attacks, and password security will likely improve employees'

resiliency to a personal data breach. Across all U.S. businesses, the average cost of a data breach was $9.44 million in 2022 (“Cost,” 2022). Therefore, there are additional benefits and positive externalities of improved cyber skills in the workplace.

Policy Sustainability Through Legislative Support

While Policy Option #3 is the best first step to address cybersecurity vulnerabilities, legislative action is also recommended to maintain positive outcomes. Policy Option #3 and legislative action could be combined to provide a tiered implementation model. Chairman Mark Green (R-TN, House Committee on Homeland Security) is a proponent of increased federal oversight and regulation related to cybersecurity (“Rep. Mark,” 2020). Chairman Green previously cosponsored a bill to strengthen CISA’s ability to address cyber threats on federal government systems (“Rep. Mark,” 2020). Congressman Green would be an ideal candidate to sponsor a bill to require critical energy infrastructure companies to require all employees to complete annual cyber training to address the constantly changing threat of a cyber breach. Additionally, federal legislation is more permanent than the current government requirements enacted under EO 14028, which could be removed with a change of president in 2024 (“Executive,” 2021).

State legislatures are another avenue to propose a bill or policy rider to require energy companies to implement an annual cyber training requirement. According to the National Conference of State Legislatures, 40 states introduced or considered over 250 cyber bills in 2022 ("Cybersecurity Legislation," 2022). Most bills are related to government employee cyber training; however, California proposed or enacted 16 bills to improve businesses’ alignment to NIST Frameworks, increase legal jurisdiction, and protect schools and hospitals from cyberattacks (“Cybersecurity Legislation,” 2022). Federal or state legislature requiring cyber training for the critical energy infrastructure sector would strengthen the company’s independent ability to recognize, block, and report cyber threats.

Raise Public Awareness Through Education

Although it is outside the scope of Policy Option #3, CISA could engage in a public awareness campaign related to cyber awareness. Addressing common ransomware attacks and best practices could improve the nation's resilience to foreign cyberattacks. Stanford scholars suggest that public awareness campaigns must provide actionable steps for citizens to get involved or provide clear steps for a path forward (Christiano & Neimand, 2017). A CISA awareness campaign could provide data related to the economic cost of data breaches and the difficulty for consumers to deal with a stolen identity or seized email and social media accounts.

CONCLUSION

I recommend Policy Option #3, the cybersecurity awareness training for my client. Policy Option #3 has the most robust empirical research suggesting that it will reduce the amount of successful cyberattacks and ransomware attempts. A study of roughly 20,000 employees found that cybersecurity awareness campaigns decreased the number of employees who opened a phishing campaign by 71.5% (Daenhsi et al., 2022). Policy Option #3 was recommended over Policy Option #1 (Updating the Executive Order) due to the impermanence of executive actions for long-term sustainable policy.

The cost to society of cyberattacks is immense, especially when dealing with national security priorities. One major implementation challenge of Policy Option #3 for private companies is simply the refusal to implement the training without a federal requirement or potential civil charges. To encourage adherence to CISA guidelines and adopt cyber awareness and training practices, CISA could conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to all CEOs of identified critical energy infrastructure. This TS/SCI briefing recommendation was originally established with a 2019 NIAC letter to President Biden discussing different tactics and strategies to make cyber intelligence actionable (Lau et al., 2019). This one-day briefing intends to build a case for company C-suite executives to counter severe cyber threats and engage in proactive cybersecurity training and awareness.

One area of future research opportunity is a longitudinal study of the detailed impacts of cybersecurity awareness training for the critical energy sector. Companies that institute annual cybersecurity training could elect to track the improvements in their cybersecurity. These trends could be tracked over a five-to-ten-year time frame to compare with the empirical cyber research and determine if results exceed expectations.

Cyberattacks are a pervasive problem in today's globalized and digital society. The 2021 Colonial Pipeline ransomware attack was a reminder of how foreign actors strive to disrupt American life by interfering with critical oil and gas distribution systems. Although the attack increased government regulations related to energy cybersecurity, cyber professionals estimate that sophisticated attacks will only increase and continue to target the healthcare sector and energy pipelines (Marks & Schaffer, 2022). Cybersecurity research is robust regarding the susceptibility of employees and citizens to cyberattacks. Policy Option #3 will best posture energy companies to improve their employee's ability to thwart and defend against cyberattacks.

GLOSSARY

Definitions

Data breach: security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual

Acronyms

CISA: Cybersecurity and Infrastructure Security Agency

DHS: Department of Homeland Security

NATO: North Atlantic Treaty Organization

OMB: United States Office of Management and Budget

NDAA: National Defense Authorization Act

IDA: Institute for Defense Analyses

IDA-STPI: The Institute for Defense Analyses-Science and Technology Policy Institute

TS/SCI: Top Secret/Sensitive Compartmented Information

REFERENCES

Africk, E., & Levy, Y. (2021). An examination of historic data breach incidents: What cybersecurity big data visualization and analytics can tell us? *Online Journal of Applied Knowledge Management*, 9(1), 31–45.

Ahmed, E. M. (2021). Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth. *Journal of the Knowledge Economy*, 12(1), 412–430.

Alqahtani, M. (2022). Cybersecurity Awareness Based on Software and Email Security with Statistical Analysis. *Computational Intelligence and Neuroscience.*

Baich, R., Ledgett, R., Fehrman, W., Morley, K., Sage, O., Wallace, M., Lau, C., Scott, B. (2020). NIAC Actionable Cyber Intelligence: An Executive-Led Collaborative Model. *The Cybersecurity & Infrastructure Security Agency (CISA).* Retrieved 2 April 2023 from https://www.cisa.gov/sites/default/files/2023-01/NIAC%20Actionable%20Cyber%20Intelligence_FINAL_508_0.pdf

Ballou, T., Allen, J., & Francis, K. (2016). U.S. Energy Sector Cybersecurity: Hands-off Approach or Effective Partnership? *Journal of Information Warfare*, 15(1), 44–59. https://www.jstor.org/stable/26487480

Blair, D. C., & Roth, W. "Bud." (2022). Cyber Crime and Geostrategic Clash Over the Internet: Deputizing the Private Sector to Assist. *The Cyber Defense Review*, 7(2), 15–34. https://www.jstor.org/stable/48669290

Bruhn, M., & McKenzie, D. (2019). Can Grants to Consortia Spur Innovation and Science-Industry Collaboration? Regression-Discontinuity Evidence from Poland. *World Bank Economic Review*, 33(3), 690–716. https://doi.org/https://academic.oup.com/wber/issue

Business Email Compromise The 12 Billion Dollar Scam. (2018). *Internet Crime Complaint Center (IC3)*. Retrieved September 18, 2022, from https://www.ic3.gov/Media/Y2018/PSA180712

Careers, Meet Our People. (2022). Colonial Pipeline. Accessed 26 February 2023. https://www.colpipe.com/careers/meet-our-people-1

Cassotta, S., & Sidortsov, R. (2019). Sustainable Cybersecurity? Rethinking Approaches to Protecting Energy Infrastructure in the European High North. *Energy Research and Social Science*, 51, 129–133.

Colonial Pipeline Names Darrell Riekena Senior Vice President, Chief Information Officer. Colonial Pipeline Company. Retrieved 1 March 2023 from https://www.prnewswire.com/news-releases/colonial-pipeline-names-darrell-riekena-senior-vice-president-chief-information-officer-301567532.html#:~:text=Colonial%20Pipeline%20Names%20Darrell%20Riekena%20Senior%20Vice%20President%2C%20Chief%20Information%20Officer

Company Factsheet: About Booz Allen- Overview. Booz Allen Hamilton. Retrieved 1 April 2023 from

https://www.boozallen.com/content/dam/boozallen_site/esg/pdf/slick_sheet/booz-allen-hamilton-fact-sheet.pdf

Council: The President's National Infrastructure Advisory Council (NIAC) (2023). *The Cybersecurity & Infrastructure Security Agency (CISA).* Retrieved 2 April 2023 from https://www.cisa.gov/resources-tools/groups/presidents-national-infrastructure-advisory-council-niac

Christiano, A., Neimand, A., (2017). *Stanford Social Innovation Review*. Retrieved 16 March 2023 from https://ssir.org/articles/entry/stop_raising_awareness_already

Cost of a Data Breach (2022). *IBM*. Retrieved 15 March 2023 from https://www.ibm.com/reports/data-breach

Critical Infrastructure Sectors (2020). *Department of Homeland Security*. https://www.cisa.gov/critical-infrastructure-sectors

Cybersecurity Legislation 2022. *National Conference of State Legislatures*. Retrieved 16 March 2023 from https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2022

Daengsi T, Pornpongtechavanich P, Wuttidittachotti P. Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Educ Inf Technol (Dordr)*. 2022;27(4):4729-4752. doi: 10.1007/s10639-021-10806-7. Epub 2021 Nov 15. PMID: 34803469; PMCID: PMC8591595.

De Bruijne, M & Van Eeten, M 2007, 'Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment', *Journal of Contingencies and Crisis Management*, vol. 15, no. 1, pp. 18-29.

Defense Cybersecurity Requirements for Small Businesses (2023). *Defense Advanced Research Projects Agency (DARPA)*. Retrieved 15 March 2023 from https://www.darpa.mil/work-with-us/for-small-businesses/cybersecurity

Del Rio Gonzalez, P. (2008). The empirical analysis of the determinants for environmental technological change: A research agenda. *Ecological Economics*, 68(3), 861-878. https://doi.org/10.1016/j.ecolecon.2008.07.004

Department of Defense Releases the President's Fiscal Year 2024 Defense Budget (13 March 2023). *U.S. Department of Defense*. Retrieved 2 April 2023 from https://www.defense.gov/News/Releases/Release/Article/3326875/department-of-defense-releases-the-presidents-fiscal-year-2024-defense-budget/#:~:text=On%20March%209%2C%202023%2C%20the,billion%20more%20than%20FY%202022

Dimeff, L., Harned, M., Woodcock, E., Skutch, J., Koerner, K., Linehan, M. (2015). Investigating Bang for Your Training Buck: A Randomized Controlled Trial Comparing Three Methods of Training Clinicians in Two Core Strategies of Dialectical Behavior Therapy. *Behavioral Therapy*, Volume 46, Issue 3, Pages 283-295. ISSN 0005-7894. https://doi.org/10.1016/j.beth.2015.01.001

Doubleday, J. (2018). DOD's cyber posture review driving new investments in security. *Inside the Pentagon*, 34(45), 13–14. https://www.jstor.org/stable/90026023

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, 9, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Eling, M., & Schnell, W. (2016). What Do We Know about Cyber Risk and Cyber Risk Insurance? *Journal of Risk Finance*, 17(5), 474–491.

Executive Order on Improving the Nation's Cybersecurity (May 2021). The White House. Retrieved 1 March 2023 from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China. (2022). The White House. Retrieved 2 March 2023 from https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V., & Theohary, C. A. (2015). Cyber Intrusion into U.S. Office of Personnel Management: In Brief. *Congressional Research Service*. Retrieved September 18, 2022, from https://sgp.fas.org/crs/natsec/R44111.pdf.

Free and Reduced-Price Meals FCPS (2021). *Fairfax County Public Schools*. https://www.fcps.edu/frm

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber Security on the Farm: An Assessment of Cyber Security Practices in the United States Agriculture Industry. *International Food and Agribusiness Management Review*, 21(3), 317–334. https://doi.org/http://ifama.org/page-18348

Gill, J. (13 March 2023). *Breaking Defense*. Retrieved 2 April 2023 from https://breakingdefense.com/2023/03/pentagon-boosts-spending-on-rd-jadc2-rapid-experimentation-and-cybersecurity-in-fy24-request/#:~:text=%E2%80%9CThe%20FY24%20budget%20request%20affirms,said%20in%20a%20briefing%20today

Goh, J., Kang, H., Xing Koh, Z., Way Lim, J., Wei Ng, C., Sher, G., & Yao, C. (2020). Cyber Risk Surveillance: A Case Study of Singapore. 31.

Gootman, S. (2016). OPM Hack: The Most Dangerous Threat to the Federal Government Today. *Journal of Applied Security Research*, 11(4), 517–525. https://doi.org/10.1080/19361610.2016.1211876

Gordon, L., Loeb, M., Lucyshyn, W., Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity,* 1(1), 3-17. https://doi.org/10.1093/cybsec/tyv011

Goss, D. D. (2017). Operationalizing Cybersecurity — Framing Efforts to Secure U.S. Information Systems. *The Cyber Defense Review*, *2*(2), 91–110. http://www.jstor.org/stable/26267345

Grady, J. (2021). Lawmakers Grill Pentagon Officials on How to Prevent Another Colonial Pipeline-Style Attack. *USNI News*. https://news.usni.org/2021/05/18/lawmakers-grill-pentagon-homeland-security-officials-on-how-to-prevent-another-colonial-pipeline-style-attack

Hall, Andrew O. "The Cyber Defense Review: Investing in Cybersecurity Solutions." *The Cyber Defense Review*, vol. 2, no. 2, 2017, pp. 9–12. JSTOR, http://www.jstor.org/stable/26267339. Accessed 6 Nov. 2022.

Hallman, W. (2019). Cybersecurity: Front and Center for Industry. *National Defense*, 104(788), 4–4. https://www.jstor.org/stable/27022623

Harding, E., Ghoorhoo, H. (September 2022). Hard Choices in a Ransomware Attack. *Center for Strategic & International Studies*. Retrieved 1 March 2023 from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220928_Harding_HardChoices_RansomwareAttack.pdf?VersionId=XzYG9_BSC1yZhE.sAbvYXThCqSBQNmb4

Healthcare Facilities and Power Outages (2019). *Federal Emergency Management Agency.* https://www.fema.gov/sites/default/files/2020-07/healthcare-facilities-and-power-outages.pdf

Hearing Before The United States Senate Committee On Homeland Security & Governmental Affairs — Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company (June 8, 2021). Colonial Press Release. Retrieved March 1, 2023 from https://www.colpipe.com/news/press-releases/hearing-before-the-united-states-senate-committee-on-homeland-security-governmental-affairs-testimony-of-joseph-blount-president-and-chief-executive-officer-colonial-pipeline-company

Herring, MJ, and KD Willett. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." *Journal of Information Warfare 13*, no. 2 (2014): 46–55. https://www.jstor.org/stable/26487121

Homeland Security Presidential Directive 7 (2003). *Department of Homeland Security*. https://www.cisa.gov/homeland-security-presidential-directive-7

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber Risk Management in SMEs: Insights from Industry Surveys. *Journal of Risk Finance*, 22(3–4), 240–260.

H.R.4346 - Chips and Science Act (2021). Congress.gov. https://www.congress.gov/bill/117th-congress/house-bill/4346

Hub for Imaging and Quantum Technologies. *Johns Hopkins University*. Retrieved 2 March 2023 from https://research.jhu.edu/bloomberg-distinguished-professorships/clusters/hub-for-imaging-and-quantum-technologies/

Internet Crime Report (2021). Federal Bureau of Investigation. Retrieved March 1, 2023 from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Jaikaran, C (2021) Cybersecurity: Selected Cyberattacks, 2012-2021. *Congressional Research Service*. Retrieved September 18, 2022, from https://crsreports.congress.gov/product/pdf/R/R46974/2

Johnston, S. (2019). Nonrefundable Tax Credits versus Grants: The Impact of Subsidy Form on the Effectiveness of Subsidies for Renewable Energy. *Journal of the Association of Environmental and Resource Economists*, 6(3), 433–460. https://doi.org/http://www.journals.uchicago.edu/loi/jaere

Jones, D. (2022). Colonial Pipeline Names Cybersecurity Veteran As First CISO. Retrieved 1 March 2023 from https://www.cybersecuritydive.com/news/colonial-pipeline-ciso-adam-tice/619272/#:~:text=Colonial%20Pipeline%20tapped%20veteran%20cybersecurity,information%20and%20data%20security%20program

Justice News: Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (2021). The Department of Justice. Retrieved 15 March 2023 from https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

Kramer, F. D., & Butler, R. J. (2019). A Roadmap To Better Cybersecurity. In Cybersecurity: Changing The Model (pp. 5–20). *Atlantic Council*. http://www.jstor.org/stable/resrep20932.5

Lach, S., Neeman, Z., & Schankerman, M. (2021). Government Financing of R&D: A Mechanism Design Approach. *American Economic Journal: Microeconomics*, 13(3), 238–272. https://doi.org/http://www.aeaweb.org/aej-micro/

Lev, S., Ressler, A., Jonas, S. (2016). Implementing a Roadmap for Critical Infrastructure Security and Resilience. *The Institute for Defense Analyses (IDA) Science and Technology Policy Institute Research (STPI)*. Retrieved 2 April 2023 from https://www.ida.org/-/media/feature/publications/r/rn/rn-hs-roadmap/rn-hs-roadmap.ashx

Lewis, L. (2016). Cyber Center: Practical Strategies for Developing a Cyber-Incident Plan. *Business Law Today*, 1–4. https://www.jstor.org/stable/businesslawtoday.2016.08.11

Lim, T., Guzman, T., & Bowen, W. M. (2020). Rhetoric and Reality: Jobs and the Energy Provisions of the American Recovery and Reinvestment Act. *Energy Policy*, 137.

Lim, T., Tang, T., & Bowen, W. M. (2021). The Impact of Intergovernmental Grants on Innovation in Clean Energy and Energy Conservation: Evidence from the American Recovery and Reinvestment Act. *Energy Policy*, 148.

Marks, J., Schaffer, A. (2022). One year ago, Colonial Pipeline changed the cyber landscape forever. The Washington Post. Retrieved 16 March 2023 from https://www.washingtonpost.com/politics/2022/05/06/one-year-ago-colonial-pipeline-changed-cyber-landscape-forever/

Mehrotra K., & Turton, W. (2021) Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg. Retrieved September 18, 2022, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Monov, L. (2019). NATO Under Pressure. *Journal of Strategic Security*, 12(1), 1–14. https://www.jstor.org/stable/26623075

Montgomery, M., & Borghard, E. (2021). Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence. *JFQ: Joint Force Quarterly*, 102, 79–89.

Morgan, S., (2019). 2019 Official Annual Cybercrime Report. Cybersecurity Ventures. Retrieved 1 March 2023 from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. Retrieved 1 April 2023 from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Morse, E. A., & Ramsey, I. (2016). Navigating the Perils of Ransomware. *The Business Lawyer*, *72*(1), 287–294. https://www.jstor.org/stable/26419124

Nakashima, E. (2021). Biden Administration Moving To Address A Global Compromise By Chinese And Other Hackers Of Microsoft Email Servers. *The Washington Post*. Retrieved 1 April 2023 from https://www.washingtonpost.com/national-security/china-hack-microsoft-email-biden-response/2021/03/06/7fe6652c-7e1a-11eb-85cd-9b7fa90c8873_story.html

NIST Cybersecurity Framework (2023). https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework

Occupational Outlook Handbook (2022). *U.S. Bureau of Labor Statistics.* Retrieved February 26, 2023 from https://www.bls.gov/ooh/a-z-index.htm#M

Parfomak, P. W., & Jaikaran, C. (2021). Colonial Pipeline: The DarkSide Strikes. *Congressional Research Service*. Retrieved September 18, 2022, from https://crsreports.congress.gov/product/pdf/IN/IN11667

Paul, J. A., & Zhang, M. (2021). Decision Support Model for Cybersecurity Risk Planning: A Two-Stage Stochastic Programming Framework Featuring Firms, Government, and Attacker. *European Journal of Operational Research*, 291(1), 349–364.

Pósa, T., Grossklags, J. (2022). Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students. *Journal of Cybersecurity and Privacy*. 2022, 2, 490–515. ttps://doi.org/10.3390/jcp2030025

Proofpoint 2020 State of the Phish Annual Report. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

Public Courses. (2022). Federal Virtual Training Environment (FedVTE). Accessed 26 February 2023 from https://fedvte.usalearning.gov/public_fedvte.php

Rep. Mark Green Introduces the Protecting Federal Networks Act (2020). Retrieved on 2 March 2023 from https://markgreen.house.gov/2020/8/rep-mark-green-introduces-the-protecting-federal-networks-act

Sargent, J. (2022). Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure. *Congressional Research Service.* R44711. Retrieved 2 April 2023 from https://sgp.fas.org/crs/natsec/R44711.pdf

Scholten, D., Criekemans, D., & Van de Graaf, T. (2019). AN ENERGY TRANSITION AMIDST GREAT POWER RIVALRY. *Journal of International Affairs*, *73*(1), 195–204. https://www.jstor.org/stable/26872789

School Meal Statistics (2022). *School Nutrition Association*. https://schoolnutrition.org/about-school-meals/school-meal-statistics/

Schroeder, J. (2020). Two From Hopkins Join National Effort To Advance Quantum Computing. Retrieved 2 March 2023 from https://hub.jhu.edu/2020/09/09/tyrel-mcqueen-surjeet-rajendran-quantum-computing/

Security Awareness Training as a Key Element in Changing the Security Culture (March 2022). *Osterman Research*. https://ostermanresearch.com/wp-content/uploads/2022/03/ORWP_0352-Osterman-Research-Security-Awareness-Training-as-a-Key-Element-in-Changing-the-Security-Culture-March-2022.pdf

Seda-Sanabria Y., Morgeson, J., Dechant, J. (July 2016). An Integrated Approach for Physical and Cyber

Security Risk Assessment: The U.S. Army Corps of Engineers Common Risk Model for Dams. *The Institute for Defense Analyses*. IDA Paper NS P-8092.

Significant Cyber Incidents (2022). *Center for Strategic and International Studies*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

State and Local Cybersecurity Grant Program (2022). *Department of Homeland Security-Federal Emergency Management Agency*. Retrieved 2 March 2023 from https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program#:~:text=In%20fiscal%20year%20(FY)%202022,state%2C%20local%20and%20territorial%20governments

System Map (2023). Colonial Pipeline. Retrieved 23 April 2023 from https://www.colpipe.com/about-us/our-company/system-map

Tate, D., Bailey, J. (April 2022). When Is it Feasible (or Desirable) to Use the Software Acquisition Pathway? *The Institute for Defense Analyses, Cost Analysis and Research Division.* IDA Paper D-33047.

Turell, J., Su, F., & Boulanin, V. (2020). Lessons from past cyber incidents and country studies. In Cyber-incident Management: Identifying and Dealing with the Risk of Escalation (pp. 32–42). Stockholm International Peace Research Institute. http://www.jstor.org/stable/resrep26199.11

U.S. Census Bureau QuickFacts: Fairfax County, Virginia (2021). https://www.census.gov/quickfacts/fact/table/fairfaxcountyvirginia/PST045221

U.S. Census Population Clock (2022). *United States Census Bureau*. https://www.census.gov/popclock/

APPENDIX A

Costs to Society-Direct Costs	
50% of Fairfax County Business Revenue Using 5.3% Sales Tax Data	$6,177,717
Fairfax County Businesses- 50 % of average daily sales tax receipts	$327,419
Fairfax County Population (According to 2021 Census)	1,139,720 people
*Of those 1,139,720 people, assume 60% of working age	683,832 people
Labor participation Age 16+ Currently Working: 70.3%	480,734 people
Fairfax County Daily Average Income based on $127,866 annual income	$492
Fairfax County Total Daily Average Income for Labor Force	[480,734*492] =$236,521,128
Loss of wages-20% of daily household income for hourly employees	$47,304,226
Total daily loss of electricity revenue for Fairfax County residents	$3,989,020
National average for daily energy consumption cost-approx. 29 kWh	$3.5
Estimated Daily Power Plant Operations and Maintenance (O&M) Cost	$10,000,000
Approximate number of restaurants in Fairfax County	137 restaurants
Number of restaurants without backup power-70% of all restaurants	$96
Spoiled restaurant food supply $800/establishment	$76,800
Total Estimate for County Direct Costs of 24-hr Blackout	**$67,875,181**

Risk Criterion: The risk criterion is based on The Institute for Defense Analyses (IDA) cyber risk assessment of dams and navigation locks for the U.S. Army Corps of Engineers (USACE). In 2016, IDA conducted a mathematically rigorous and robust risk assessment of critical dam infrastructure to best prepare for a future cyber or physical attack (Seda-Sanabria et al., 2016). The IDA model has been modified to the economic loss of cyberattacks for critical energy infrastructure.

Vulnerability Rating	Consequence Rating				
	Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Extremely High (Cyber Package 0)	Very Low	Low	High	Very High	Very High
High (Cyber Package 1)	Very Low	Low	Moderate	High	Very High
Moderate (Cyber Package 2)	Very Low	Low	Moderate	Moderate	High
Low (Cyber Package 3)	Very Low	Low	Low	Low	Moderate
Extremely Low (Cyber Package 4)	Very Low	Very Low	Very Low	Low	Low

Risk is a function of three variables: threat (T), vulnerability (V), and consequences (C). Threat (T) is defined as a nation-state or hacking group attempting to interfere with or disable a private energy company's networks or IT systems. Vulnerability (V) and consequences (C) are defined below:

$$R=f(T,V,C)$$

The cyber vulnerability rating (left column of the above table) is defined as the probability of a cyberattack defeating current cyberattacks. The cyber package is a general category based on various aspects of a company's cyberattack mitigation strategy (e.g., Incident Response Plan, cyber infrastructure, annual training, etc.). This is a subjective categorical decision based on client judgment and expertise. The following table has criteria for the vulnerability assignment of an individual energy company:

Cyber Defense Package	Description	Rating
Cyber Package 4	Robust cyber infrastructure, complete IT support for size of organization, annual training requirements, independent annual audit, Chief Technology Officer, complete Incident Response Plan	Extremely Low
Cyber Package 3	Substantial cyber infrastructure, full IT support for size of organization, annual training requirements, Chief Technology Officer, complete Incident Response Plan	Low
Cyber Package 2	Complete cyber infrastructure, full IT support for size of organization, Chief Technology Officer, incomplete Incident Response Plan	Moderate
Cyber Package 1	Basic cyber infrastructure, limited IT support, Chief Technology Officer, incomplete Incident Response Plan	High
Cyber Package 0	Insignificant infrastructure, IT support, annual training, or Chief Technology Officer	Extremely High

The consequence rating is based on the economic losses of an electric utility company being hacked and unable to provide essential utilities to consumers. The economic loss is determined by the size of the electric utility company and the current number of customers.

Economic Loss Consequence				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
< $500K	**$500K < X ≤ $1.0M**	**$1.0M < X ≤ $5.0M**	**$5.0M< X ≤ $10.0M**	**> $10M**

APPENDIX B

Expense	Number of hours for Policy Option #1	Number of employees	Cost
Business consultant wages- $134.13/hr	30hr	4	$134.13 * 120 = **$16,095.6**
Material expenses	N/A	4	**$2,500**
Total cost for Booz Allen Hamilton	30	4	$16,095.6+$2,500= **$18,595.6**

***Cost calculation note: labor costs for Policy Option #1 only includes the cost to my client. The annual salary of Johns Hopkins University grant writing officials and Cybersecurity professors is not included in the total cost. Consultant wages are based on Bureau of Labor Statistics estimates and client conversations. Consultant wage for all calculations is $89.42/hr plus a 50% fringe rate for a total of $134.13/hr.

APPENDIX C

DoD RDT&E Budget Activity Codes and Description	
Code	**Description**
6.1	Basic Research
6.2	Applied Research
6.3	Advanced Technology Development
6.4	Advanced Component Development and Prototypes
6.5	System Development and Demonstration
6.6	RDT&E Management Support
6.7	Operational System Development
6.8	Software and Digital Technology Pilot Programs
Source: Department of Defense, *Financial Management Regulation* (DoD 7000.I 4-R), Volume 2B, November 2017.	

Expense	Number of hours for Policy Option #2	Number of employees	Cost
Federal grant funding for cybersecurity technology	N/A	N/A	**$3,660,000**
Business consultant wages- $134.13/hr**	10hr	2	$134.13*10*2 = **$2,682.6**
Total cost of the policy option	N/A	N/A	$3,660,000+$2,682.6= **$3,662,682.6**

**Cost calculation note: labor costs for Policy Option #2 only includes the cost to my client. The annual salary of Johns Hopkins University grant writing officials and Cybersecurity professors is not included in the total cost. Consultant wages are based on Bureau of Labor Statistics estimates and client conversations. Consultant wage for all calculations is $89.42/hr plus a 50% fringe rate for a total of $134.13/hr. The annual salary of Johns Hopkins University grant writing officials and Cybersecurity professors are not included in the total cost.

The Department of Homeland Security has allocated $185 million in FY22 for the State and Local Cybersecurity Grant Program (“State,” 2022).

APPENDIX D

Five assumptions related to a Cybersecurity Awareness and Training (CAT) program:

1) Below is the complete list of 15 free courses offered by CISA that companies could offer to employees as professional development or heightened cyber awareness:
2) Companies will utilize their current Information Technology (IT) department for training support and troubleshooting. Companies will also rely on current computer and software infrastructure to conduct the training. However, $5,000 is added to the cost calculations to cover unforeseen material expenses (e.g., additional computer monitors or redundant computer base stations).
3) The training will be conducted while the employee is at work, including the opportunity cost of the employee's wage.
4) Company size will be based on the Colonial Pipeline company, which is 900 people ("Careers," 2022).
5) The average hourly salary is $26.38. This is the average of three separate professions based on the Bureau of Labor Statistics: 1) Utility Construction Laborer- $18.04 per hour, 2) Customer Service Representative-$17.75, and 3) Administrative/Management Analyst- $44.71 per hour ("Occupational," 2022).
6) Consultant wages are based on Bureau of Labor Statistics estimates and client conversations. Consultant wage for all calculations is $89.42/hr plus a 50% fringe rate for a total of $134.13/hr.

Complete list of free courses offered by the Federal Virtual Training Environment (FedVTE) provided by the Cybersecurity & Infrastructure Security Agency ("Public," 2023):

Course Title	Max Completion Time
101 Coding for the Public	varies
101 Critical Infrastructure Protection for the Public	varies
101 Reverse Engineering for the Public	varies
Cloud Computing Security	2.5 hours
Cloud Security - What Leaders Need to Know	1 hour
Cryptocurrency for Law Enforcement for the Public	varies
Cyber Supply Chain Risk Management for the Public	varies
Cyberessentials	**1 hour**

Don't Wake Up to a Ransomware Attack	1 hour
Foundations of Cybersecurity for Managers	2 hours
Fundamentals of Cyber Risk Management	varies
Introduction to Cyber Intelligence	2 hours
Securing Internet-Accessible Systems	1 hour
Understanding DNS Attack	1 hour
Understanding Web and Email Server Security	1 hour

One additional explicit cost associated with Policy Option #3 is the cost of labor for the Information Technology (IT) professions to assist employees with the training. For this analysis, let us assume an IT professional makes $49.33 an hour, according to the U.S. Bureau of Labor Statistics. For example, a company with three full-time IT staff members allocated 10 hours per year per staff member to assist with troubleshooting and technology problems. This would total about **$1,480** in gross salary. Below is the total cost of the program:

Expense	Number of hours per year	Number of employees	Cost
Software expenses	N/A	N/A	$0
Employee wages- $26.38	1hr	900	$26.38 * 900= **$23,742**
IT employee wages- $49.33	10hr	3	$49.33 * 10 * 3= **$1,479.9**
Business consultant wages- $134.13/hr	30hr	3	$134.13 * 90 = **$12,071.7**
Material expenses	N/A	900	**$5,000**
Total cost per company	930	900	$23,742+1,479.9+ 5,000= **$30,221.9**
Total cost per company without charging for 1hr of employee's opportunity cost	930	900	$1,479.9+$5,000= **$6,479.9**