Scientia Moralitas International Journal of Multidisciplinary Research
ISSN 2472-5331 (Print) | ISSN 2472-5358 (Online) | Vol. 10, No. 1, 2025
DOI: 10.5281/zenodo.16415237

How Forced Regulation Affects Minority Underserved Communities in Cybersecurity

Allison Fullwood
Capitol Technology University, United States
https://orcid.org/0009-0000-6484-6396

Eugene J. Lewis
Capitol Technology University, United States
https://orcid.org/0000-0002-2956-0760

ABSTRACT: The forced regulation debate has been an ongoing discussion among media, academics, and practitioners surrounding several elements of the plan. The underlying challenge would constitute extreme problems and issues for minorities in underserved communities seeking to attain a collegiate education, especially in the cybersecurity market, where minority representation is still one of the lowest among other collegiate majors and disciplines. Forced regulation specifically details the complete removal of the Department of Education. If implemented, many minorities in underserved communities will potentially not have an opportunity to attend college. Many first and second-generation college graduates cannot afford to pay for college out of pocket. Therefore, the use of Financial Aid to assist is a primary source of an academic resource to attend college. Moreover, the extensive effects on Historically Black Colleges and Universities (HBCUs) would constitute a loss of dollars on Student Aid (FAFSA) to support their institution's administrative needs. This paper will focus on how minority Science, Technology, Engineering, and Mathematics (STEM) and cybersecurity programs will severely be affected in minority underserved communities.

KEYWORDS: cybersecurity, diversity, Historically Black Colleges and Universities (HBCUs), forced regulation, Science, Technology, Engineering, and Mathematics (STEM), underserved communities

Introduction

Forced regulation represents a comprehensive presidential transition initiative to fundamentally restructure federal governance through four primary pillars: policy guidance, personnel development, administrative training, and implementation strategy (The Heritage Foundation, 2023). This initiative, spearheaded by the Heritage Foundation in collaboration with over 100 conservative organizations, builds upon the historical precedent of the 1981 "Mandate for Leadership" that guided the Reagan administration's policy framework (Rosen & Quinn, 2024).

The initiative's organizational structure reflects a strategic approach to government reform, operating under the leadership of former federal officials with extensive experience in personnel management and executive operations (The Heritage Foundation, 2023). The cornerstone of forced regulation is its comprehensive policy guide, which presents detailed recommendations for restructuring federal agencies and implementing significant policy changes across the executive branch (Grim, 2020).

Forced regulation provides specific guidance for entities ranging from the President's Executive Office to specialized agencies like the Export-Import Bank. Several policy areas are seen in forced regulation policy structure, such as education reform policies, social welfare programs, and immigration policies. The educational proposals call for expanding school choices and radical shifts in the approaches to the federal funding of academic institutions. For social welfare, the initiative suggests putting work incentives for some assistance programs in place and reorganizing several federal aid instruments (Esterline, 2024). This initiative is accompanied by major proposed reforms in federal personnel management, structures for civil servants, and organizational practices across agencies. These proposals include changes in the classification of civil service jobs, changes to the performance appraisal systems, and changes to federal funding distribution (The Heritage Foundation, 2023). The plan also touches on promotion policies in the military and organizational and departmental controls, proposing radical shifts in current bureaucratic practice.

Forced regulation has outlined some proposed social and healthcare changes, including reproductive health and family planning. The proposal that is being made entails radical changes to the current FDA policies and guidelines, particularly regarding medication and its distribution outlets (The Heritage Foundation, 2023). These recommendations entail policy changes that would impact the structures of the delivery of health care as well as the access to health care. The initiative's healthcare proposals go beyond the scope of the policy tweaks to include structural reforms within the Department of Health and Human Services. One of them is restructuring the current task forces and introducing new supervisory bodies related to family healthcare projects (Grim, 2020). The plan focuses on traditional family values and suggests how these views could be incorporated into the federal health care policy systems. Forced regulation implies radical restructuring of the federal agencies and major transformations of the existing institutions. The initiative changes the scope and organization of the National Oceanic and Atmospheric Administration (NOAA), including organizational changes to the agency (The Heritage Foundation, 2023). Similar recommendations can be made to dismantle and divide the Department of Homeland Security into other federal departments.

The plan for agency reorganization is the formation of a new cabinet-level immigration and border agency to deal with the functions that are presently

divided between different departments (Esterline, 2024). According to Alvarez (2022), this new entity would join immigration operations from the Departments of Homeland Security, Justice, and Health and Human Services, employing more than 100,000 staff. The diversity and administrative reforms initiative concerns the institutional policies on DEI programs in the federal sector. These proposals comprise major changes to current DEI positions and initiatives, particularly to sources of funding and plans of execution (The Heritage Foundation, 2023). The recommendations include the federal employment policies in agencies, proposing changes in the criteria for assessing and rewarding employees. Forced regulation places significant emphasis on border security and immigration enforcement mechanisms. The initiative proposes expanding military involvement in border operations, including deploying active-duty personnel and National Guard units for enforcement operations (Esterline, 2024). These recommendations include modifications to existing enforcement protocols and expanding physical border infrastructure. The proposal advocates revising current Immigration and Customs Enforcement (ICE) policies, particularly regarding enforcement locations and operational guidelines (Alvarez, 2022). Specific recommendations address emergency response protocols during increased migration, suggesting expanded authority for the Secretary of Homeland Security to implement expedited procedures. The administrative restructuring and civil service reform initiative outlines comprehensive changes to federal workforce management through the "Schedule F" classification system. This proposal would modify the status of numerous civil service positions, potentially affecting employment terms and conditions for federal employees (Grim, 2020). The plan includes recommendations for restructuring performance evaluation systems and modifying federal fund allocation procedures. Forced regulation proposes significant changes to traditional administrative boundaries, particularly regarding executive oversight of federal departments. The policy implementation and oversight initiative suggest modifying existing relationships between executive offices and federal agencies, potentially expanding direct presidential authority over various operational aspects (The Heritage Foundation, 2023). These changes would affect funding allocation processes and departmental decision-making procedures.

The initiative presents extensive recommendations for restructuring educational administration and funding mechanisms. Key proposals include eliminating the Department of Education and implementing alternative funding models for educational institutions (Prokop, 2023). These recommendations extend to federal nutrition programs and student loan policies, suggesting substantial modifications to existing support systems. Forced regulation addresses environmental and energy policies, proposing significant changes to current regulatory frameworks. The initiative recommends modifications to clean energy policies and environmental regulations, suggesting alternative approaches to

resource management and energy production (Millhiser, 2024). These proposals include recommendations for restructuring federal environmental oversight and modifying existing regulatory mechanisms. Forced regulation proposes comprehensive reforms to healthcare delivery systems and social programs. The initiative recommends significant modifications to Medicaid structure and administration, including changes to funding mechanisms and eligibility criteria (Quinn, 2022). These proposals extend to policies regarding medical billing practices and healthcare access protocols. The initiative outlines policy recommendations aligned with religious and traditional family perspectives. Proposals include modifications to contraceptive coverage requirements and restrictions on certain types of medical research funding (Hubbard et al., 2024). Millhiser (2024) denotes that the framework addresses issues of reproductive healthcare access and interstate healthcare regulations. Forced regulation addresses economic policy areas where conservative perspectives diverge, particularly trade policies and antitrust regulation.

The initiative acknowledges ongoing debates within conservative policy circles about the role of institutions like the Export-Import Bank (The Heritage Foundation, 2023). Notable omissions include detailed proposals regarding Social Security and Medicare reform. The initiative provides a detailed implementation framework for the first 180 days of a new administration. This includes specific timelines for policy implementation, agency restructuring, and personnel changes (Rosen & Quinn, 2024). Grim (2020) states that the strategy emphasizes the rapid deployment of key policy initiatives while maintaining operational continuity in essential government functions.

The Department of Education supports Historically Black Colleges and Universities (HBCUs) through targeted funding sources and specialized initiatives. According to Escobar et al. (2023), the Department's contribution to HBCUs in fiscal year 2023 represents a considerable boost in assistance, enhancing these institutions' ability to serve their communities. Elliott and Kellison (2021) found that HBCUs rely significantly on federal aid for their operational budgets. HBCUs get specified money under the Higher Education Act's Title III, Part B program, which Escobar et al. (2023) highlight as critical for academic achievement and faculty expansion. Streit (2023) underlines this dependency, indicating that Department of Education financing is a major source of support for HBCU institutional assistance programs. Taylor (2020) notes that these financing streams significantly impact institutional stability and program sustainability at HBCUs. The Department of Studies distributes federal financial aid to HBCU students to help them further their studies. Crosby (2023) found that a large proportion of HBCU students receive Pell Grants, which is higher compared to other college students. Moore (2021) emphasized the socioeconomic challenges faced by HBCU students, most of whom come from low-income families. According to Taylor (2020), the HBCU Capital Financing Program

under the Department has issued over $3 billion in low-cost loans essential to creating and maintaining campuses. Mallory (2021) observed that funding from the Department of Education is directly proportional to the improved retention of students at HBCUs. Pinchot et al. (2020) demonstrate that the FAS affects graduation rates and student success outcomes at HBCUs.

The COVID-19 pandemic highlighted the Department of Education's role in HBCU stability and operation. Davis (2024) found that federal intervention played a crucial role in preventing many HBCUs from closing during the pandemic. Pinchot et al. (2020) said the Department's strategic 2021 objective included paying off significant institutional debt through the HBCU Capital Financing initiative. This program significantly improved financial metrics for participating institutions. Johnson and Thompson (2021) evaluate these emergency response methods and emphasize the Department's role in HBCU strength. Taylor (2020) discovered that this federal financing enabled many HBCUs to maintain academic programs and student services during the pandemic, thus ensuring the education of marginalized groups. The White House Initiative on HBCUs started in 1980 and oversees all Direct Grant funds through the Department of Education's hierarchy.

In the recent study by Williams (2022), the effort has paid off as it secured significant federal financing across many agencies for the 2021 to 2023 period. According to Crosby (2023), there has been a significant rise in program involvement, with HBCU engagement with government programs increasing due to better resource-leveraging strategies. Ellis et al. (2020) established that when HBCUs partnered with federal agencies through the department-coordinated partnership, the possibility of research funding greatly improved, enhancing institutional research capability. Taylor (2020) clarifies that the initiative is not limited to financial contributions, as he notes an increase in institutional performance due to enhanced government engagement. Domingo et al. (2022) report that the integrated strategy led to a significant increase in federal grant successes from HBCUs and a notable improvement in institutional resource development and program viability. The Department's management facilitates Title IV programs, which Mallory (2021) believes are essential for maintaining stable enrollment rates to guarantee HBCUs' involvement in federal student aid programs. Danner (2020) states that HBCU students received substantial federal grants and loans during the 2022-2023 academic year.

Taylor (2020) assesses the impact of the Department's technical assistance projects in strengthening the institutional capacity to sustain the accreditation standards and regulatory requirements. Streit (2023) shows considerable success in regulatory compliance, with a significant reduction in breaches following Department-provided support measures. Taylor (2020) supports these findings, demonstrating the Department's critical role in promoting HBCU sustainability and expansion. Johnson and Thompson (2021) found that institutions with

complete Department support have a significantly higher student completion rate and graduate employment success compared to those with little federal engagement.

HBCUs contribute to cybersecurity, filling critical industry gaps and talent shortages. According to Johnson and Thompson (2021), HBCUs provide a substantial portion of African American graduates with cybersecurity degrees despite accounting for a small percentage of higher education institutions in the United States. Roy et al. (2022) found that HBCU cybersecurity programs have a high job placement rate within six months after graduation. Pitman et al. (2022) show that HBCU graduates in cybersecurity professions earn more than the national average for entry-level occupations. Thomas (2024) recognizes many HBCUs Centers of Academic Excellence in Cyber Defense Education, including Morgan State University, Norfolk State University, and North Carolina A&T State University. Ellis et al. (2020) found that these recognized colleges graduate a notable number of cybersecurity experts annually.

Additional research by Williams (2022) shows that HBCU cybersecurity graduates had a greater retention rate in the field than graduates from other colleges. Industry partnerships improve HBCU cybersecurity education through strategic efforts and resource investments. Goldstein (2020) documents significant business engagement, saying that big technology corporations have invested substantial amounts in HBCU cybersecurity education programs since 2021. Domingo et al. (2022) discuss the impact of IBM's HBCU Cybersecurity Leadership Centers, which began in 2022 and have formed relationships with 20 HBCUs to provide specific curricula and professional development opportunities. Johnson and Thompson (2021) report significant progress, documenting an increase in HBCU students entering cybersecurity careers over recent years. Pinchot et al. (2020) show that corporate mentorship programs at HBCUs are practical, leading to a higher internship-to-job conversion rate in cybersecurity positions. Turner et al. (2022) highlight the infrastructural improvements that arise from these collaborations, including the construction of specialist cybersecurity laboratories at HBCUs to support practical training programs. Strategic funding allocations and specific program development initiatives from the federal government help to boost HBCU cybersecurity research capabilities.

According to Diverse (2023), the Department of Defense has allocated significant amounts to HBCU cybersecurity research institutes since 2021. Thomas (2024) highlights the actual impact of these efforts, citing a notable increase in peer-reviewed cybersecurity publications by HBCU teachers and students. Johnson and Thompson (2021) use Howard University's Center for Applied Data Science and Analytics as an example of federal financing for advanced cybersecurity research initiatives. Turner et al. (2022) report intellectual property development, citing numerous cybersecurity-related patents gained by HBCU research institutes in recent years. Burrell and McAndrew (2023)

underline the economic implications of these research activities, pointing out that federally sponsored HBCU programs have contributed to the creation of several cybersecurity firms. Diverse (2023) adds that these firms have created numerous high-paying technology jobs in traditionally underprivileged neighborhoods.

HBCUs create supportive learning environments that effectively meet the needs of underrepresented students seeking cybersecurity education.

Diverse (2023) found that HBCU cybersecurity programs outperformed comparable programs at other schools, with higher retention rates. According to McGee et al. (2021), the success of the shift in enrolment could be attributed to culturally responsive teaching pedagogy and support frameworks for minority students in STEM disciplines. Taylor (2020) provided an analysis of the performance of HBCU mentorship activity, showing higher graduation rates for cybersecurity majors compared to the national average. Pinchot et al. (2020) provide substantial proof of the long-term career outcomes, pointing out that HBCU cybersecurity programs secure a significant portion of graduates in management-level jobs within five years. According to Johnson and Thompson (2021), these enabling conditions lead to a notable improvement in students' research engagement. HBCU cybersecurity programs have a far-reaching impact beyond graduation, given established alumni networks and substantial industrial implications.

According to Johnson and Thompson (2021), a significant portion of HBCU cybersecurity alumni maintain strong relationships with their alma mater, establishing long-term paths for future recruiting and mentorship. Elliott and Kellison (2021) highlight the effectiveness of these networks by reporting a higher job placement rate for recent graduates compared to non-networked colleges. Johnson and Thompson (2021) highlight leadership successes, pointing out that HBCU cybersecurity alumni hold executive roles at a significant portion of Fortune 500 technology organizations. Lewis and Burrell (2023) found that HBCUs have produced some of the most influential and successful graduates in all fields of study. Escobar et al. (2023) give proof of this influence, citing a rise in minority participation in senior cybersecurity roles. Pinchot et al. (2020) discovered that alumni networks spur more career growth in the first decade after graduation.

Problem Statement

According to research by Pinnock et al. (2023), the United States population has over 35% of people belonging to the minority communities represented in its population. For most, especially guided by the due process clause in the United States Constitution, the high presence of such communities in the population prompts the need for their rights and freedoms to be upheld or protected based on guidance from major statutes and legislations within governance (Strauss, 2022).

The United States, however, has illustrated a negative track record when it comes to ensuring that the basic rights of underserved minority communities are protected. In a 2023 UN article, major leaders discussed how minorities from indigenous communities are still being discriminated against and experience issues related to their degradation in the form of commodification (United Nations, 2023). Some of the tenets of forced regulation, a major agenda of Trump and his accolades, further the notion of showing little to zero attention towards underserved minority communities.

As scholars such as Valant et al. (2024) argue, forced regulation, particularly its proposal to overhaul the federal education policy that significantly benefits children from minority and underserved communities, represents a major misstep. As mentioned, not only does the project propose to completely do away with the Department of Education, but it also seeks to deny loan access to students at "schools that provide in-state tuition to illegal aliens". It is important to recall that among those who require these loans are majorly children and people from underserved communities. Bell (2023) paints a clearer picture by arguing how individuals from the Asian, Indian, Latino, or Hispanic, as well as those from the Black communities, still have issues accessing quality college education due to affordability issues. Statistics from the National Science Foundation (2023) illustrate that only 15% of people in STEM came from underserved communities like Hispanic communities, while those from the Black, Asian and American Indians, and Alaska natives made up 10%, 9%, and 1% respectively. These low numbers can be tied back to the lack of affordability of STEM courses that range from a little over $10,000 to $60,000 annually (Okechukwu, 2024). All these show that with the implementation of forced regulation, which proposes the denial of loan access to minorities, even lower numbers will be witnessed in STEM.

Another important issue that is likely to present itself due to forced regulation is an attack on cybersecurity, especially for those from underserved minority groups in the United States. Renaud and Coles–Kemp's (2022) study shows that the lack of basic resources is a huge hindrance for people from underserved communities to have the capability to protect themselves from issues related to cybersecurity. The proposition to remove the statutes of the CISA Act related to the Department of Homeland Security poses even more cyber threats to the United States' cyber and physical security (Tisler & Norden, 2024). If the threat is significant for the total United States population, how much will it be for those who lack the knowledge or basic resources to cushion themselves from any cybersecurity-related issues?

The problem statements for this research consists of the following:

1) How likely is it that the abolishment of the Department of Education would hinder career advancement for minorities in cybersecurity?
2) How significant is the potential impact of the proposed forced regulation policies on workforce diversity in the cybersecurity sector?

Nature and significance of the study

The significance of this study includes its analysis of the policies in forced regulation and the consequences for underrepresented minority groups in cybersecurity. This study is significant, especially considering the current changing cyber risks and the increased demand for a diverse, well-trained workforce in this field. According to Shrestha (2023), the need for more professionals in the field of cybersecurity is increasing, especially in the United States, which is one of the field's major markets. The need is also increased by the rapid digital changes due to the digitalization and innovation of novel technologies (Admass et al., 2024). For the United States, one major issue related to cybersecurity is the prevalence of ransomware, a factor that the Office of the National Cyber Director (2024) poses huge risks to national security. Namukasa et al. (2023) postulate that while the independent attributes of digital are growing, there is a need to have a large number of individuals who bring a variety of opinions and methods of tackling problems. However, the presence of diverse individuals in the cybersecurity industry is not as diverse as it should be, especially regarding minorities (Hamburg, 2023). This research will examine how the proposed elimination of the Department of Education and associated policies from forced regulation will change existing inequalities and create new barriers to diversification in the cybersecurity profession. This study offers valuable information on the potential effects of these topics in today's society, touching on diversity, education, and national security (Justice & Sample, 2022). In addition, this study attempts to educate politicians, educators, and business executives concerning the possible implications of such profound changes for the cybersecurity workforce and the nation's general cyber resilience and security posture.

This research highlights the significant implications of forced regulation for the cybersecurity workforce and identifies the benefits and obstacles for minority populations in the cybersecurity field while analyzing the relationship between education policy, workforce, and national security. According to Blažič (2022), there is a great significance in having a diverse and gendered cybersecurity team due to the expanding need and complexity of technology. Other research conducted in the past years showed that diverse teams can be more effective and solve multifaceted problems (Namukasa et al., 2023). This array of ideas and knowledge may lead to designing significantly more effective protection systems and coming up with new approaches to deal with novel threats in the realm of cybersecurity. Furthermore, this study focuses on identifying the impacts that implementing the policy changes in the future will have on national cybersecurity response readiness. The investigation into how forced regulation may affect the flow of skilled people from underrepresented groups into the workforce is intended to contribute to the current conversation on workforce development, education, and national security in the digital era (Blažič, 2022).

Resorting to forced regulation and the actual abolishment of the Department of Education would be evidence that there has been a shift in the federal education policy that might not benefit minority students aspiring to work in the field of cybersecurity (McGee, 2020). As stated by Pierszalowski et al. (2021), this proposal involves students in marginalized groups who mainly rely on government funding to enroll in post-secondary education. The loss of these individuals might present difficulties that would hinder well-developed, gifted minority applicants interested in cybersecurity from realizing their optimal objectives (Cain, 2022). Furthermore, reductions in federal funding for schools concentrating on disadvantaged students might also reduce early education in STEM so that fewer minority children would dream of cybersecurity careers (Armeen & Das, 2023). This study also goes beyond the brief impact on the students and the communities in which they live. As noted earlier by Pierszalowski et al. (2021), the cybersecurity sector is currently experiencing a staffing shortage, with the demand for cybersecurity professionals growing significantly faster than the actual number of employees.

According to the (ISC)² Cybersecurity Workforce Study (2023), the global shortfall in the cybersecurity workforce is 3.4 million, with a severe shortage in the United States. This gap threatens national security and restricts economic development and advancement in digital-related projects (Cain, 2022). This study expands the existing literature on the impact of workforce development and national security by investigating how proposals in forced regulation might influence the acquisition of minority talent in the cyber-security sector (Pierszalowski et al., 2021). Furthermore, it draws attention to the unintended consequences of relevant policies that can potentially worsen workforce deficits and limit employment diversity in essential fields. This research also identifies the relationship between education policy, the cybersecurity workforce, and national security. Examining these relationships in the study aims to provide individuals with critical insights that aid in tackling the challenges still affecting the cybersecurity industry.

This research focuses on the role of HBCUs in preparing minority students for cyber employment. Traditionally, HBCUs have been at the forefront of the fight to increase diversity in STEM. Nevertheless, these colleges often rely on federal funds and student aid programs to fulfill their educational goals (Armeen & Das, 2023). Achievement of forced regulation may lead to financial problems for HBCUs, which can limit their capacity to provide proper education and training in cybersecurity (Justice & Sample, 2022). For this reason, this study will assess the repercussions of a decline in government funding to HBCUs and their role in enhancing a diverse workforce of cybersecurity personnel. These institutions must continue to be supported to build talent from underrepresented groups. This study also emphasizes the need for continued funding and support of HBCUs to address the cybersecurity skills shortage effectively. The analysis aims

to provide valuable information concerning the nature of the interaction between federal education policies and institutional support for worker diversity in the cybersecurity field. According to McGee (2020), these insights may influence future governmental decisions and initiatives to support HBCUs and their mission to educate young minority individuals about the cybersecurity profession.

The research also considers other areas of cybersecurity within forced regulation, focusing on how it impacts underprivileged groups. Renaud and Coles-Kemp (2022) state that individuals in these environments constantly reinvent where they get the necessities to protect themselves from cybersecurity threats. It is essential to consider that the proposed restructuring of cybersecurity agencies and regulations under forced regulation might expose this and other vulnerable populations to these cyber threats (Atkins & Lawson, 2021). The research focuses on federal cybersecurity policy and educational funding shifts and their impact on the cyber defense of minority populations. By highlighting these possible weaknesses, the study contributes to a better understanding of the connection between workforce development, education policy, and national cybersecurity readiness (Koukakis, 2024). Also, this analysis intends to discover possible cybersecurity deficiencies due to the suggested legislative changes.

The research intends to provide insights that can lead to more inclusive and prosperous cybersecurity solutions addressing the particular issues marginalized areas face. This research stresses the need to incorporate diverse opinions and requirements when formulating national cybersecurity strategies and educational plans. This study is important because it explores the possible future economic impacts of forced regulation's proposals directed at minority groups in cybersecurity. The technology industry sees the cybersecurity sector not just as one of the fastest-growing but also as a leading sector in terms of salary (Crumpler & Lewis, 2022). The United States Bureau of Labor Statistics (2023) reports that information security analysts earned a median annual salary of $102,600 in 2022, and job growth is projected at 35% from 2021 to 2031, which is much higher than the average for all professions (National Center for Science and Engineering Statistics, 2023). This study provides information about the potential operational impacts of forced regulation by examining how this initiative may impact the opportunity for minorities to enter careers in cybersecurity. The study will evaluate the economic effects of reduced diversity in the cybersecurity workforce and will aim to highlight the more significant socioeconomic effects of the concepts in forced regulation by examining the relationship between educational possibilities, career choices, and sustained economic success. The findings contribute to generating better and more fairer policies conducive to diversity.

The study also examines what certain proposals from forced regulation mean for competitiveness internationally. Cybersecurity is vital for the nation's security and to gain a competitive edge in this world of integration (Koukakis, 2024). Nations that can produce and maintain a talented and robust cybersecurity

workforce are ready to protect their cyber assets and, therefore, can adequately cope with the challenges of the global digital economy (Atkins & Lawson, 2021). This research explores the impact of the diversity drop in United States cybersecurity personnel due to policies from forced regulation based on the status of the country's standing in the global cybersecurity scene. This analysis contributes to a deeper appreciation of the general approaches to forced regulation by revealing the relationship between domestic educational policy and global market competition. In addition, the work seeks to establish how changes in the United States cybersecurity environment could affect its international cooperation. Through these analyses of the global implications, the research reveals the potential consequences of shifts to home policy in the global cybersecurity field. This study demonstrates that a diverse and competent cybersecurity workforce is needed to uphold the competitiveness of countries within the growing realm of digitalization. Lastly, this study offers research support to policymaking and advocacy work. This investigation seeks to provide individuals with the information needed to make an informed decision by providing a detailed impact analysis of the implication of forced regulation on the efficacy of minorities in cybersecurity.

The findings of this study offer a grouped understanding of a broad array of policy strategies and diversification at the national security level in the context of cybersecurity (Triplett, 2022). Furthermore, this research could enrich public discourse on the connection between education policy, skills development, and national security by highlighting what the recommended policies may bring (Koukakis, 2024). Also, it will provide insights to advocacy organizations that seek to increase equity in the STEM fields. The findings of this study benefit projects to maintain and increase the representation of underrepresented groups in cybersecurity education and jobs by exploring the repercussions of forced regulation. Ultimately, the research intends to help create more effective policies that improve diversity and national cybersecurity preparedness.

Finding the gap in the research

Although a wealth of research exists on STEM diversity and the cybersecurity workforce shortage, there is an important missing focus on the potential consequences of substantial education policy reforms, including those from forced regulation, for minority representation in cybersecurity (Crumpler & Lewis, 2022). Botha-Badenhorst and Veerasamy (2023) have discussed the challenges preventing underrepresented groups from entering and remaining in the field. These studies need to be adjusted to analyze how the proposed extensive revamping of federal education policy might impact these challenges. In addition, although Lyon (2020) explored the role of federal financial aid in promoting

diversity in higher education, there has been no exploration of how discontinuing these programs might affect the flow of minority talent into cybersecurity.

More research needs to be done on the connection between education policy, the development of the cybersecurity workforce, and national security issues, particularly in disadvantaged populations. Namukasa et al. (2023) and Hamburg (2023) present an extensive analysis of the general benefits of diversity in cybersecurity teams. However, there has been a minimal investigation on alterations in governing body policy and minority educational opportunities and the readiness of a state in cyberspace security. Furthermore, the particular position of historically black colleges and universities (HBCUs) as minority students preparing for cybersecurity careers is acknowledged (Lyon, 2020). However, there is more that needs to be understood about changes in federal funding and the effect that might have on the output of these institutions in the diverse field of cybersecurity.

Another rather extensive area of further study applies to the social and economic impacts of the reduced minority involvement in cybersecurity caused by amendments to the legal regulations. Triplett (2022) looked at the broad gains of diversity in the technology industry. Despite growing concerns, there has been limited research into cybersecurity issues and how changes in educational opportunities might affect wealth disparity and access to economic advancement in disadvantaged regions. However, more details are needed about how potential reductions in worker diversity might affect global competitiveness, especially in sensitive areas like cybersecurity (Botha-Badenhorst & Veerasamy, 2023). This study aims to analyze the potential effects of forced regulation on minority access to cybersecurity professions. By doing so, it seeks to address existing gaps in literature and enhance our understanding of the relationship between diversity, education policies, and national security.

Theoretical framework explained

The project employs three theoretical frameworks—Resource-Based View (RBV), Competitive Advantage, and Power and Influence theories—to analyze the potential impact of forced regulation on cybersecurity education for minorities, particularly in HBCUs. These frameworks help assess how institutional resources, strategic positioning, and power dynamics shape the educational outcomes for minority students in cybersecurity programs. These theories are effective tools for understanding the implications of policy changes, including those proposed by forced regulation, on educational institutions. By examining how these theories apply to the current state of HBCUs and their cybersecurity programs, we can gain insights into the expected consequences of forced regulation's funding and resource shifts.

RBV theory suggests that organizations derive sustainable value from their resources and capabilities. These resources, which may include financial assets, human capital, and institutional knowledge, contribute directly to an organization's competitive advantage and performance (Burrell & McAndrew, 2023). In the context of HBCUs, Johnson and Thompson (2021) highlight that federal funding, academic expertise, industry relationships, and cultural capital are essential resources that support cybersecurity education. The application of RBV theory to HBCUs suggests that any policy change that disrupts these resources—such as the proposed funding cuts under forced regulation—could significantly hinder their educational capabilities. For example, Turner et al. (2022) argue that federal support directly impacts program quality and student success, ensuring HBCU viability in the cybersecurity field. Furthermore, Thomas (2024) found that HBCUs' cultural resources, including faculty-student relationships and institutional support, enhance the success of minority students in cybersecurity programs. In applying RBV to the effects of forced regulation, Ramirez et al. (2021) report that government funding is a critical resource for HBCU STEM programs, including cybersecurity education. As Kononets et al. (2020) note, the potential abolition of the Department of Education under forced regulation poses a significant threat to these resource-based advantages. HBCUs have strategically allocated federal funds to enhance cybersecurity training, research, and support services, as shown by Domingo et al. (2022), who found that federal subsidies have led to higher graduation rates for minority students in STEM fields. The loss of these resources could undermine HBCUs' ability to maintain specialized cybersecurity labs and research centers, diminishing their overall educational impact (Justice & Sample, 2022). Thus, the RBV theory demonstrates that forced regulation's proposed cuts could disrupt the resource configurations essential for sustaining HBCUs' cybersecurity programs.

Competitive Advantage theory explores how organizations achieve superior performance by developing unique capabilities that distinguish them from competitors (Elliott & Kellison, 2021). HBCUs have built a competitive edge in cybersecurity education by leveraging their distinctive institutional strengths, including their reputation for fostering minority success, their specialized programs, and their industry partnerships (Johnson & Thompson, 2021). Davis (2024) identifies four key components of competitive advantage in higher education: institutional reputation, program differentiation, student success rates, and industry linkages. For HBCUs, these components are particularly crucial because they allow these institutions to compete effectively with better-funded universities. However, the continued success of HBCUs depends on maintaining a steady flow of federal funding, which supports their unique position in cybersecurity education. Applying Competitive Advantage theory to forced regulation, it becomes evident that potential funding reductions could threaten HBCUs' strategic positioning. Taylor (2020) observes that specific federal funds

have been vital for HBCUs' cybersecurity programs, enabling them to develop distinctive programs and attract top talent. Pettersson (2021) highlights that these advantages have led HBCUs to graduate a disproportionately high percentage of African American cybersecurity professionals. If forced regulation leads to the loss of these funding streams, as Johnson and Thompson (2021) suggest, HBCUs will likely face challenges in maintaining their competitive position. As Lewis and Burrell (2023) argue, a disruption in funding may lead to decreased program quality and lower student success rates, directly undermining HBCUs' competitive advantage. Furthermore, disruption of the current funding mechanisms could erode the industry linkages that are vital for placement rates and career outcomes for minority graduates (Ellis et al., 2020; Anderson & Holloway, 2020).

Power and Influence theory examines how power dynamics shape decision-making and resource allocation within organizations. In the context of education, these dynamics can determine which programs receive funding, what resources are prioritized, and how policies impact marginalized groups.

Johnson and Thompson (2021) argue that power relations in educational policymaking significantly influence the sustainability and success of programs serving minority populations, such as those at HBCUs. Lewis and Burrell (2023) emphasize that power dynamics between federal agencies, academic institutions, and industry partners are crucial in determining the development and funding of cybersecurity programs. Forced regulation proposes to eliminate the Department of Education, which could shift power from federal agencies to state governments, altering the way resources are allocated and policies are enforced. As Roy et al. (2022) explain, this transfer of power could deprive HBCUs of crucial decision-making authority over program development and funding. Streit (2023) warns that such a shift could reduce HBCUs' ability to support their specialized cybersecurity programs, as state agencies may prioritize different initiatives or allocate fewer resources to institutions serving minority students. Goldstein (2020) further asserts that power imbalances in education often disproportionately affect institutions that support marginalized communities. Shifting power dynamics could undermine HBCUs' ability to negotiate for the resources needed to maintain high-quality cybersecurity education.

Together, the RBV, Competitive Advantage, and Power and Influence theories provide a comprehensive framework for assessing the potential impacts of forced regulation on HBCUs' cybersecurity programs. Each theory highlights the critical role of resources—whether financial, cultural, or institutional—in maintaining program quality and institutional success. As Diverse (2023) notes, understanding how resources are distributed and how power relations affect policy implementation is crucial for predicting how HBCUs will fare under forced regulation. These frameworks also emphasize the importance of maintaining a competitive advantage, particularly in the face of shifting power dynamics and funding cuts. The combined application of these theories suggests that forced

regulation's proposed policy changes could significantly disrupt HBCUs' cybersecurity programs by reducing access to key resources, weakening their competitive position, and shifting power away from institutions serving minority populations. As Anderson and Holloway (2020) highlight, any disruption to the resource supply could undermine the ability of HBCUs to continue providing specialized education in cybersecurity. However, these theoretical frameworks also provide insights into how HBCUs might adapt to these changes by exploring alternative funding sources, strengthening industry partnerships, and leveraging their unique institutional strengths to maintain their competitive advantage.

Methodology

The primary aim of this paper is to examine how forced regulation affects minority Science, Technology, Engineering, and Mathematics (STEM) and cybersecurity programs in underserved communities. To achieve this, a qualitative exploratory research approach is employed to gather data on individuals' lived experiences. The researcher will conduct a semi-structured constructivist focus group study, surveying twenty-six individuals. Each participant will respond to the key questions from the study. After collecting all responses, the researcher will analyze themes and patterns to present findings and results.

The exploratory research methodology using focus groups strongly aligns with process theory, which conceptualizes the world in terms of situations, events, people, and the processes that link them (Mohr, 1982; Maxwell, 1996). According to Maxwell (1996), process theory explains how situations and events influence one another. This approach is particularly relevant for understanding the perspectives of underserved communities through their lived experiences (Lyon, 2020). The qualitative research method utilizing focus groups allows researchers to investigate specific phenomena in-depth, assessing context, implementation, and outcomes (Cronon, 2014; Lyon, 2020). A focus group typically consists of a small group of individuals who are interested in the topic and willing to contribute constructively (Krueger, 1994; Robinson, 2002; Lazar et al., 2017). Homogeneous groups of individuals with shared backgrounds and experiences can enhance discussions and provide insights that reflect a common context (Lazar et al., 2017).

The focus group method enables researchers to collect diverse opinions and perspectives, which are essential for comprehending complex issues. The use of focus groups in exploratory research remains closely tied to process theory, emphasizing the interconnections between situations, events, and people (Maxwell, 1996). By analyzing these relationships, researchers gain valuable insights into the experiences of underserved communities. Focus groups offer an opportunity for an in-depth investigation of phenomena while considering contextual factors, implementation, and outcomes. To facilitate meaningful discussions, scholars such as Lazar et al. (2017), Krueger (1994), and Robinson

(2002) advocate for smaller group sizes and the selection of participants who are genuinely interested in contributing constructively. Additionally, Lazar et al. (2017) highlight that homogeneous groups foster discussion by providing a shared context and experience. These approaches ultimately support inclusive dialogue and enable a comprehensive understanding of complex research topics.

Findings and Results

The findings and results from the focus group consist of qualitative exploratory research design responses. See Table 1.

Table 1. Respondents, Position Description, Ethnicity, and Number of Work Years

Survey respondents			
Respondents	**Position description**	**Ethnicity**	**Number of work years**
Respondent 1	Security Assistance Program Manager (SAPM)	African-American	12
Respondent 2	Security Assistance Specialist (SAS)	White-American	2
Respondent 3	Security Assistance Specialist (SAS)	Latino-American	1
Respondent 4	Security Assistance Program Manager	White-American	7
Respondent 5	International Program Manager	Asian-American	15
Respondent 6	Cyber Security Technician	White-American	3
Respondent 7	Security Assistance Program Manager	African-American	5
Respondent 8	International Program Manager	White-American	13
Respondent 9	Program Analyst	White-American	8
Respondent 10	Program Analyst	White-American	3
Respondent 11	Database Administrator	African-American	6
Respondent 12	Database Security Manager	White-American	7
Respondent 13	Security Assistance Program Manager	Asian-American	10
Respondent 14	Cybersecurity Specialist	Latino-American	9
Respondent 15	International Program Manager	African-American	6
Respondent 16	Security Assistance Specialist (SAS)	White-American	3
Respondent 17	Security Assistance Specialist (SAS)	White-American	4
Respondent 18	Budget Analyst	Latino-American	11
Respondent 19	International Program Manager	African-American	16
Respondent 20	Security Assistance Specialist (SAS)	Asian-American	3
Respondent 21	Program Analyst	Latino-American	1
Respondent 22	Budget Analyst	African-American	7
Respondent 23	Cyber Security Technician	White-American	1
Respondent 24	Program Analyst	Latino-American	2
Respondent 25	Budget Analyst	African-American	4
Respondent 26	Cyber Security Technician	White-American	2

Ethnicity tables

The ethnicity tables from the focus group consists of respondent information distributed by ethnicity. See Tables 2-5.

Table 2. Demographic: White-American. Respondents, Position Description, Ethnicity, and Number of Work Years

Survey Respondents			
Respondents	**Position description**	**Ethnicity**	**Number of work years**
Respondent 2	Security Assistance Specialist (SAS)	White-American	2
Respondent 4	Security Assistance Program Manager	White-American	7
Respondent 6	Cyber Security Technician	White-American	3
Respondent 8	International Program Manager	White-American	13
Respondent 9	Program Analyst	White-American	8
Respondent 10	Program Analyst	White-American	3
Respondent 12	Database Security Manager	White-American	7
Respondent 16	Security Assistance Specialist (SAS)	White-American	3
Respondent 17	Security Assistance Specialist (SAS)	White-American	4
Respondent 23	Cyber Security Technician	White-American	1
Respondent 26	Cyber Security Technician	White-American	2

Table 3. Demographic: African-American. Respondents, Position Description, Ethnicity, and Number of Work Years

Survey Respondents			
Respondents	**Position Description**	**Ethnicity**	**Number of work years**
Respondent 1	Security Assistance Program Manager (SAPM)	African-American	12
Respondent 7	Security Assistance Program Manager	African-American	5
Respondent 11	Database Administrator	African-American	6
Respondent 15	International Program Manager	African-American	6
Respondent 19	International Program Manager	African-American	16
Respondent 22	Budget Analyst	African-American	7
Respondent 25	Budget Analyst	African-American	4

Table 4. Demographic: Latino-American. Respondents, Position Description, Ethnicity, and Number of Work Years

Survey respondents			
Respondents	**Position description**	**Ethnicity**	**Number of work years**
Respondent 3	Security Assistance Specialist (SAS)	Latino-American	1
Respondent 14	Cybersecurity Specialist	Latino-American	9
Respondent 18	Budget Analyst	Latino-American	11
Respondent 21	Program Analyst	Latino-American	1
Respondent 24	Program Analyst	Latino-American	2

Table 5. Demographic: Asian-American. Respondents, Position Description, Ethnicity, and Number of Work Years

Survey Respondents			
Respondents	**Position Description**	**Ethnicity**	**Number of work years**
Respondent 5	International Program Manager	Asian-American	15
Respondent 13	Security Assistance Program Manager	Asian-American	10
Respondent 20	Security Assistance Specialist (Sas)	Asian-American	3

The findings and results from the focus group consist of qualitative exploratory research design responses. See Table 6-10.

Question 1: How likely do you think the abolishment of the Department of Education will hinder career advancement for minorities in cybersecurity? See Table 6.

Table 6. Respondents, Rating

Career Advancement Concerns	
Respondents	**Rating: (1) Very Unlikely, (2) Unlikely, (3) Neutral, (4) Likely, (5) Very Likely**
Respondent 1	5
Respondent 2	2
Respondent 3	3
Respondent 4	1
Respondent 5	4
Respondent 6	5
Respondent 7	5
Respondent 8	2
Respondent 9	1
Respondent 10	1
Respondent 11	5
Respondent 12	2
Respondent 13	4
Respondent 14	3
Respondent 15	5
Respondent 16	1
Respondent 17	4
Respondent 18	3
Respondent 19	5
Respondent 20	3
Respondent 21	4
Respondent 22	5
Respondent 23	1
Respondent 24	2
Respondent 25	4
Respondent 26	1

Analysis of the respondent response(s) to Question 1:

(1) How likely do you think the abolishment of the Department of Education will hinder career advancement for minorities in cybersecurity?

Table 7. Rating, Number of Respondents, Ratio Percentage, Analysis of the Data Set

Analysis of the Respondent Response to Question 1			
Rating	**Number of respondents**	**Ratio percentage**	**Analysis of the data set**
Respondents Rating of 5	7 / 26	27%	Very Likely
Respondents Rating of 4	5 / 26	19%	Likely
Respondents Rating of 3	4 / 26	15%	Neutral
Respondents Rating of 2	4 / 26	15%	Unlikely
Respondents Rating of 1	6 / 26	23%	Very Unlikely

In response to the question, 7 out of 26 respondents (27%) deemed the abolishment of the Department of Education will potentially hinder career advancement for minorities in cybersecurity. Based on the data set, the second anomaly consisted of 6 out of 26 respondents (23%) assumed it is "unlikely" there will be an effect of minority development in this career area. The findings further provide clarity into the ethnic demographics (7 Respondents of "Very Likely") 6 of the Respondents were African American and 1 Respondent White-American representing the majority of African Americans determine the career advancement of minorities will be limited.

Question 2: How significant do you think the impact of proposed policies found in forced regulation will be on workforce diversity in the cybersecurity sector? See Table 8.

Table 8. Respondents, Rating

Workforce Diversity Impact	
Respondents	**Rating: (1) Very Significant, (2) Somewhat Significant, (3) Neutral, (4) Somewhat Insignificant, (5) Very Insignificant**
Respondent 1	5
Respondent 2	1
Respondent 3	2
Respondent 4	3
Respondent 5	1
Respondent 6	1
Respondent 7	5
Respondent 8	1

Respondent 9	1
Respondent 10	2
Respondent 11	5
Respondent 12	2
Respondent 13	3
Respondent 14	3
Respondent 15	5
Respondent 16	1
Respondent 17	1
Respondent 18	3
Respondent 19	5
Respondent 20	4
Respondent 21	2
Respondent 22	5
Respondent 23	1
Respondent 24	3
Respondent 25	5
Respondent 26	1

Analysis of the respondent response(s) to Question 2:

(2) How significant do you think the impact of proposed policies found in forced regulation will be on workforce diversity in the cybersecurity sector?

Table 9. Rating, Number of Respondents, Ratio Percentage, Analysis of the Data Set

Analysis of the respondent response to question 2			
Rating	**Number of respondents**	**Ratio percentage**	**Analysis of the data set**
Respondents Rating of 5	7 / 26	27%	Very Insignificant
Respondents Rating of 4	1 / 26	4%	Somewhat Insignificant
Respondents Rating of 3	5 / 26	19%	Neutral
Respondents Rating of 2	4 / 26	15%	Somewhat Significant
Respondents Rating of 1	9 / 26	35%	Very Significant

In response to the question, 9 out of 26 respondents (35%) deemed the impact of proposed policies found in forced regulation will be very significant on workforce diversity in the cybersecurity sector. Based on the data set, the second anomaly consisted of 7 out of 26 respondents (27%) assumed the impact of proposed policies found in forced regulation will be "insignificant" on workforce diversity in the cybersecurity sector. The findings further provide clarity into the ethnic demographics: (9 Respondents of "Very Significant") 8 of the Respondents were White American and 1 Respondent Asian-American representing the majority of White Americans determine the workforce diversity will be impacted very significantly.

The thematic analysis from the focus group consists of qualitative exploratory research design responses. See Table 10.

Table 10. Theme/Pattern, Total Responses, Ethnic Distribution, Position Distribution, Key Findings

Theme/ Pattern	Total Responses	Ethnic Distribution	Position Distribution	Experience Level Distribution	Key Findings
Career Advancement Concerns	Very Likely (26.9%) Very Unlikely (23.1%) Likely (19.2%)	African-American: 85.7% very likely, Latino-American: 75% neutral, Asian-American: 40% likely, White-American: 100% very unlikely	Management Roles: 57% high concern, Technical Roles: 33% low concern, Analysts: Mixed responses	>10 years: 29% high concern, 5-10 years: 57% high concern, <5 years: 68% low concern	Respondents who assumed "Very Likely" were predominantly African-American in management roles with 5–10 years of experience, while those who assumed "Very Unlikely" were exclusively White-American analysts with less than 5 years of experience.
Workforce Diversity Impact	Very Significant (34.62%) Very Insignificant (26.92%) Neutral (19.23%)	African-American: 100% very insignificant, Latino-American: 60% neutral Asian-American: Mixed responses White-American: 72.73% very significant	Management Roles: 40% very significant, Technical Roles: 50% very insignificant, Analysts: Mixed responses	>10 years: 55.56% very insignificant 5-10 years: 57.14% neutral <5 years: 60% very significant	Respondents with less than 5 years of experience, particularly White-American analysts and managers, were most likely to rate the factor as "Very Significant," while those with over 10 years of experience, especially African-American and Asian-American respondents, were more likely to consider it "Very Insignificant."

Themes and Patterns

Career advancement concerns

The survey results reveal several issues regarding career advancement challenges in cybersecurity under forced regulation. On the nature of career challenges, African-American and Latino-American participants rated the likelihood of such impediments as highly probable, mirroring the trends observed in the Namukasa et al. (2023) study on the representational diversity of the cybersecurity workforce. This inclination is even more pronounced among the Security Assistance Program Managers personnel with more than 10 years of business experience. The results show a link between ethnic origin and perceived career difficulties. African-American respondents, particularly those in senior positions, repeatedly expressed

concern about future professional advancement. Latino-American professionals showed significant worry about potential constraints on progression opportunities. The statistics show a significant disparity in perspective among white American respondents, who gave varying rates across the evaluation scale. This diversity reflects various experiences and perspectives on the possible impact of proposed policy changes on professional development possibilities, a pattern that aligns with McGee's (2020) research on structural racism in STEM fields. Experience level was identified as a crucial element in forming these attitudes. Professionals with more experience in the business showed more excellent knowledge of potential career development constraints. According to the statistics, senior-level minority professionals expect more severe hurdles in their career growth due to the planned adjustments.

Workforce diversity impact

The data analysis provides several perspectives on forced regulation's possible impact on cybersecurity workforce diversity. Minority respondents in senior leadership positions consistently rated the influence as extremely important to the future makeup of the workforce, supporting concerns raised by Justice and Sample (2022) regarding future workforce needs. Their comments show a considerable concern for ensuring diverse representation at all organizational levels. Senior individuals with substantial industry experience exhibited an excellent knowledge of diversity difficulties. This tendency was consistent across ethnic groups and among responders with more than ten years of professional experience. Their assessments demonstrate a thorough awareness of industry dynamics and historical trends in workforce representation. Technical personnel presented different perspectives than their managerial colleagues, aligning with Blažič's (2022) findings on changing landscapes in cybersecurity education. Cybersecurity Specialists and Security Technicians usually give neutral views of possible diversity implications. Their moderate scores indicate a range of viewpoints based on role-specific industry experiences. The response patterns strongly correlate between professional jobs and perceived influence on workforce diversity. Management-level respondents were more concerned about ensuring diverse participation, particularly in leadership roles. These viewpoints differ significantly from those of technical role holders, who predicted milder effects on the workforce mix. The research reveals that position level substantially impacts how professionals perceive future changes to diversity in cybersecurity.

Overall Patterns

The study results show consistent patterns across experience levels, jobs, and ethnic origins in cybersecurity. Senior professionals with over 10 years of experience shared concerns about forced regulation, reflecting patterns that

Hamburg (2023) identified regarding diversity and inclusion challenges. Their comments highlighted diversity and inclusion hurdles. However, early-career professionals shared their experiences and perspectives. Professional responsibilities had a considerable effect on response patterns. Management-level responders showed significant worry about long-term industry effects. Throughout the poll, technical professionals provided balanced judgments, expressing various points of view based on their role-specific experiences. Program analysts provided the most diversified set of replies to all questions. Ethnic heritage has emerged as an important component in determining opinions, supporting findings from McGee's (2020) research on structural racism in STEM fields. African-American professionals in leadership positions consistently expressed significant levels of worry across survey areas. White-American respondents gave varying opinions, indicating various experiences in the sector. Asian-American and Latino-American professionals mainly provided modest assessments of possible implications. Organizational roles exhibited diverse reaction patterns. Security Assistance Program Managers with substantial expertise reported the most serious worries about potential adjustments. Throughout the assessments, international program managers maintained a balanced attitude. Technical occupations were more consistent across ethnic origins than management ones. Professional experience has a major impact on response patterns. Senior executives displayed shared viewpoints on possible implications. Entry-level employees from all ethnic groups were hopeful about future industry circumstances. The results show that experience level considerably affects how professionals perceive prospective improvements to diversity and inclusion in cybersecurity.

Future research on the subject

Future studies on forced regulation's influence on minorities in cybersecurity will require broader analytical techniques. To provide significant insights, the study scope should span a variety of geographic locales, organizational contexts, and professional hierarchies (Namukasa et al., 2023). Longitudinal studies of minority cybersecurity experts' career advancement patterns may indicate major trends and issues (Hamburg, 2023). To evaluate the impact of policy changes on professional development prospects, research techniques should integrate quantitative and qualitative analysis (Blažič, 2022). This technique would give a more in-depth knowledge of the barriers and opportunities to minority career growth. Furthermore, a thorough review of support systems, such as mentoring programs and professional development efforts, would identify successful minority inclusion measures (Pierszalowski et al., 2021). Institutional frameworks that encourage or impede minority progress in cybersecurity professions should be investigated (Cain, 2022). The study should determine program efficacy and successful

intervention options. This study would improve our understanding of how policy changes affect minority participation in cybersecurity leadership roles.

Future studies should examine the relationships between educational policy changes and cybersecurity workforce diversity. Federal education funding should also be discussed in terms of how the shifts influence the participation and retention of minority students in cybersecurity education programs (Armeen & Das, 2023). It should also look at different sources of financial support, business partnerships, and targeted training initiatives that assist minorities in their quest for education. In the past, Black colleges and universities, in particular, have received special study consideration because of their important function in developing cybersecurity human capital for racially minoritized groups (Atkins & Lawson, 2021). These colleges offer a good opportunity for minorities to get into the cybersecurity field. The study should examine how these universities are affected by reduced government funding in sustaining efficient cybersecurity programs (Justice & Sample, 2022). This study would provide helpful information on how to enable minority students to have an opportunity to study cybersecurity even if funding is altered.

Research demands more focus on organizational culture and diverse minority cybersecurity personnel turnover matters. Research should examine how legislative changes affect working context, promotion opportunities, and fulfillment among minoritized workers (Crumpler & Lewis, 2022). This study must propose strategies for how corporations can build diverse and inclusive organizational cultures that retain diverse employees. An evaluation of effective diversity programs, mentoring schemes, and professional development could be of value to business leaders and policymakers (Lyon, 2020). The study should investigate specific organizational support promoting minority retention in cybersecurity roles (Justice & Sample, 2022). Such a study would reveal important factors for mainstreaming diversity at different organizational hierarchies. This study path requires a critical evaluation of existing programs and the development of standard procedures for minority professional development (Namukasa et al., 2023). Knowledge of these organizational factors is still important when formulating policies that will foster the growth of the minority in cybersecurity careers. Future studies should examine the economic consequences of legislative changes affecting minority participation in cybersecurity leadership.

Studies must investigate how government program changes affect minority access to executive roles and company ownership changes (Koukakis, 2024). The research could examine pay discrepancies, progression trends, and executive training programs to determine industry challenges. A thorough examination of profitable minority-owned cybersecurity firms would uncover critical success factors for legislative changes (Hamburg, 2023). The research must uncover particular aspects that promote business growth and sustainability in minority-led firms (Justice & Sample, 2022). Understanding these success patterns might help

shape future legislation and support measures. The study should concentrate on the economic progression trends of minority cybersecurity experts (Crumpler & Lewis, 2022). This investigation aims to uncover successful tactics for professional progression and financial success in cybersecurity. The findings help shape policies to minimize economic inequality in the business.

Future studies should examine how technological advancement influences minority representation in specific cybersecurity careers. It is important to look into the relationship between the advent of new technologies, required competencies, and career opportunities for minorities (Hamburg, 2023). The research should also look into training activities, certification criteria, and skill enhancement programs that help minorities perform successfully in technical jobs. A thorough examination of minority employment in higher technical jobs would reveal general efficacy and problems (Justice & Sample, 2022; Turner, Turner, & Ashe, 2022). The study should uncover characteristics that permit or impede minority professionals' search for specialized employment (Namukasa et al., 2023). Understanding these characteristics is essential when building successful support structures and tactics. The study must address access and advancement barriers in specific and specialized areas of cybersecurity (McGee, 2020). This study would aid in developing particular intervention strategies to enhance the percentage of minority individuals in technologically focused managerial positions.

The findings help policymakers make decisions on how to reduce technical specialization shortages. As a result, there is a need to evaluate research findings on the impact of minority engagement in cybersecurity programs. To support domestic policy, research should compare diversity-promoting measures in different countries (Atkins & Lawson, 2021). It should also examine a variety of educational paradigms, financial arrangements, and working practices that influence minorities' engagement in cybersecurity. A cross-sectional evaluation of practical diversity promotion techniques could uncover many distinct inclusion initiatives (Justice & Sample, 2022). Further research should determine the specific successful tactics used in various cultural settings. This study may provide best practice ways for increasing minority engagement in cyberspace. The project should investigate cross-border cooperation opportunities and their impact on minority career advancement (Crumpler & Lewis, 2022). Knowledge of how global collaboration affects minorities' prospects of professional advancement is critical to policy improvement. Such knowledge could help build more effective global initiatives to boost minority engagement in cybersecurity. Research should prioritize translating results into practical policy and implementation methods. Studies must assess successful techniques for translating research findings into practical programs and activities (Justice & Sample, 2022).

The research should identify implementation issues and use trustworthy indicators to assess program performance. To develop research-based recommendations, a thorough examination of program results and efficacy is

required (Koukakis, 2024). Studies should provide unambiguous direction for policymakers, educational institutions, and industry decision-makers. This method ensures that research findings lead to substantial changes in minority representation. The study must provide credible methodologies for monitoring policy impacts and program success (McGee, 2020). Understanding how various assessment methodologies impact program evaluation is critical for ongoing development. These findings would aid in developing more effective strategies to promote minority participation in cybersecurity jobs.

Conclusion

The potential abolishment of the Department of Education raises significant concerns about the future of career advancement for minorities in the cybersecurity field (Atkins & Lawson, 2021; Armeen & Das, 2023; Admass, Munaye, & Diro, 2024; Justice & Sample, 2022). Education and training are crucial for developing the skills necessary for success in this rapidly evolving industry (Domingo et al., 2022; Pitman et al., 2022; Koukakis, 2024). Without the support and resources provided by the Department of Education, which plays a pivotal role in funding programs and initiatives aimed at improving access to education for underrepresented groups, there is a risk that minorities may face increased barriers in pursuing cybersecurity careers (Turner, Turner, & Ashe, 2022). One of the primary functions of the Department of Education is to ensure equitable access to quality education and training programs. These initiatives often focus on providing resources to historically marginalized communities, including minorities (Namukasa et al., 2023). If the Department were to be abolished, funding for these programs could be jeopardized, leading to a lack of resources and support for minorities seeking to enter the cybersecurity workforce (Atkins & Lawson, 2021; Armeen & Das, 2023; Admass, Munaye, & Diro, 2024; Botha-Badenhorst & Veerasamy, 2023). Moreover, career advancement in cybersecurity heavily relies on access to education, mentorship, and networking opportunities (Armeen & Das, 2023; Admass, Munaye, & Diro, 2024; Justice & Sample, 2022; Pitman et al., 2022). The Department of Education offers grants and programs aimed at fostering diversity in technology fields (Domingo et al., 2022; Namukasa et al., 2023). The loss of such initiatives could diminish opportunities for minorities, creating a less inclusive environment in the cybersecurity workforce, which is already facing a diversity gap.

In conclusion, the implications of abolishing the Department of Education, alongside the proposed policies regulating education access, suggest a worrying trend for minority representation in cybersecurity (Atkins & Lawson, 2021; Justice & Sample, 2022; Admass, Munaye, & Diro, 2024; Koukakis, 2024). Unless alternative support mechanisms are established, the risks to career advancement for minorities are significant (Domingo et al., 2022; Pitman et al.,

2022). Efforts to sustain and expand educational resources and support for underrepresented groups will be essential in ensuring equitable opportunities and fostering a diverse cybersecurity workforce (Justice & Sample, 2022; Botha-Badenhorst & Veerasamy, 2023; Koukakis, 2024). To address these potential challenges, stakeholders within the cybersecurity industry, educational institutions, and advocacy groups must collaborate on creating initiatives that prioritize diversity and inclusion (Atkins & Lawson, 2021; Pitman et al., 2022). Proactive measures can counteract the negative impacts of the Department of Education's potential abolishment and ensure that all individuals, regardless of background, can thrive in the cybersecurity field.

References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, Challenges and Future Directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Alvarez, P. (2022, July 8). Border Patrol agents on horseback used "unnecessary" force in the Del Rio incident, but the investigation found no evidence they struck migrants with reins, a CBP report states. *CNN*. https://edition.cnn.com/2022/07/08/politics/border-patrol-del-rio-horse-investigation/index.html

Anderson, K. T., & Holloway, J. (2020). Discourse analysis as theory, method, and epistemology in studies of education policy. *Journal of Education Policy*, 35(2), 188-221.

Armeen, I., & Das, S. (2023). Exploring Differential Cybersecurity Vulnerabilities using Intersectionality Theory. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1001&context=aiswn2023

Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: Cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1), tyab024. https://doi.org/10.1093/cybsec/tyab024

Bell, L. (2023, August 16). *College Affordability Still Out of Reach for Students with Lowest Incomes, Students of Color*. IHEP. https://www.ihep.org/college-affordability-still-out-of-reach-for-students-with-lowest-incomes-students-of-color/

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, *27*(3), 3011-3036. https://doi.org/10.1007/s10639-021-10704-y

Botha-Badenhorst, D., & Veerasamy, N. (2023). Examining barriers to entry: Disparate gender representation in cybersecurity within Sub-Saharan Africa. *International Conference on Gender Research*, 6(1), 47–55. https://doi.org/10.34190/icgr.6.1.1148

Burrell, D. N., & Mcandrew, I. (2023). Addressing Bio-Cybersecurity Workforce Employee Shortages in Biotechnology and Health Science Sectors in the US. *Scientific Bulletin*, 28(2), 127-141. https://intapi.sciendo.com/pdf/10.2478/bsaft-2023-0014

Cain, C. C. (2021). Establishing a research agenda for broadening the participation of Black men in computing, informatics, and engineering. *Technology in Society*, p. *67*, 101790. https://doi.org/10.1016/j.techsoc.2021.101790

Cain, C. C. (2022). A shifting research agenda: Historically Black colleges and universities must prepare students for careers in computing, informatics, and engineering. *Journal of Information Systems Education*, *33*(1), 41. https://jise.org/Volume33/n1/JISE2022v33n1pp41-50.pdf

Crosby, J. (2023). An Athletic Financial Analysis Comparing HBCUs and PWIs [Doctoral dissertation, Tennessee State University]. https://www.proquest.com/openview/aa16e9ff46f4743672321b2c3e87cd7a/1?pq-origsite=gscholar&cbl=18750&diss=y

Crumpler, W., & Lewis, J. A. (2022). *Cybersecurity Workforce Gap* (p. 10). Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

Danner, P. A. (2020). Disparities in Enrollment, Funding, and Advanced Degree Patterns between Historically Black Colleges and Universities (HBCUs) and Predominantly White Institutions (PWIs): A Replication Study [Doctoral dissertation, Tennessee State University].

Davis Jr, M. C. (2024). The Impact of COVID-19 on Leadership at a Historically Black University (HBCU) [Doctoral dissertation, Tennessee State University].

Diverse, B. A. (2023). Cybersecurity talent ecosystem. https://www.bhef.com/sites/default/files/2018BHEFUSMCaseStudy.pdf

Domingo, C. R., Gerber, N. C., Harris, D., Mamo, L., Pasion, S. G., Rebanal, R. D., & Rosser, S. V. (2022). More service or advancement: Institutional barriers to academic success for women and women of color faculty at a large public comprehensive minority-serving state university. *Journal of Diversity in Higher Edu*cation, 15(3), 365. https://psycnet.apa.org/manuscript/2020-72084-001.pdf

Elliott, K., & Kellison, T. (2021). Perceptions of the fiscal challenges facing athletic departments of historically black colleges and universities. *Journal of Intercollegiate Sport*, 14(1). https://journals.ku.edu/jis/article/view/13469/13725

Ellis, V., Jenkins, P., & Pogue, T. D. (2020). Enhancing HBCU Teacher Education Experience through Authentic University-School Partnerships. *Georgia Educational Researcher*, 17(2), 4. https://files.eric.ed.gov/fulltext/EJ1262455.pdf

Escobar, M., Qazi, M., Majewski, H., Kotoye, C., & Barfield, J. (2023). Barriers and facilitators to obtaining external funding at Historically Black Colleges and Universities (HBCUs). *Journal of STEM Education: Innovations and Research*, 24(1). https://jstem.org/jstem/index.php/JSTEM/article/view/2606/2310

Esterline, C. (2024, February 20). Project 2025: Unveiling the far right's plan to demolish immigration in a second Trump term - Niskanen Center. *Niskanen Center -* Improving Policy, Advancing Moderation. https://www.niskanencenter.org/project-2025-unveiling-the-far-rights-plan-to-demolish-immigration-in-a-second-trump-term/

Goldstein, A. D. (2020). HBCUs and Prior Learning Assessments. Recognition of Prior Learning in the 21st Century. Western Interstate Commission for Higher Education. https://files.eric.ed.gov/fulltext/ED611064.pdf

Grim, R. (2020, August 20). The Trump Administration Is Giving Political Appointees Power Over Apportioning Federal Funds. *The Intercept*. https://theintercept.com/2020/08/20/federal-funds-omb-apportionment-trump/

Hamburg, I. (2023). Supporting Interdisciplinarity, Diversity and Inclusion in Cybersecurity. In *INTED2023 Proceedings* (pp. 106–111). IATED. https://doi.org/10.1109/EDUCON46332.2021.9453894

Hubbard, K., Mizelle, S., & Quinn, M. (2024, May 10). Trump says he wouldn't sign a federal abortion ban. Could he limit abortion access in other ways if reelected? - *CBS News*. Www.cbsnews.com. https://www.cbsnews.com/news/trump-federal-abortion-ban-limit-abortion-access/

ISC2. (2023). *Cybersecurity Workforce Study, 2023*. https://www.isc2.org/Research/Workforce-Study

Johnson, M. S., & Thompson, S. (2021). Covid-19 crisis management at historically Black colleges and universities (HBCUs): A contemporary approach to governance and leadership. *Journal of Underrepresented & Minority Progress*, 5(SI).

Justice, C., & Sample, C. (2022, March). Future needs of the cybersecurity workforce. In *International Conference on Cyber Warfare and Security* 17 (1), 81–91.

Kononets, N., Ilchenko, O., & Mokliak, V. (2020). Future teachers resource-based learning system: experience of higher education institutions in Poltava city, Ukraine. *Turkish Online Journal of Distance Education*, 21(3), 199-220. https://dergipark.org.tr/en/download/article-file/1181911

Koukakis, L. G. (2024). National Security, Foreign Policy, Intelligence, Cybersecurity, National Defense, Maritime Security, Risk Analysis, and Foresight Strategic Documents Issued by Regional and International Actors in 2023. https://kedisa.gr/wp-content/uploads/2024/02/research-paper-no-104-Koukakis.pdf

Lewis, E. J., & Burrell, D. N. (2023). The Sustainability of Historically Black Colleges and Universities (HBCUs) in the Post-COVID-19 World and Beyond. *HOLISTICA–Journal of Business and Public Administration*, 14(1), 39-62. https://intapi.sciendo.com/pdf/10.2478/hjbpa-2023-0004

Lyon, V. (2020). *Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals* [Doctoral dissertation, Walden University].

Mallory, C. (2021). Nonacademic Factors Affecting Retention and Academic Success at Historically Black Colleges and Universities [Doctoral dissertation, Walden University].

McGee, E. O. (2020). Interrogating structural racism in STEM higher education. *Educational Researcher*, *49*(9), 633–644. https://doi.org/10.3102/0013189X20972718

McGee, E. O., Parker, L., Taylor, O. L., Mack, K., & Kanipes, M. (2021). HBCU presidents and their racially conscious approaches to diversifying STEM. Journal of Negro Education, 90(3), 288-305. https://drive.google.com/file/d/1X_j1FKKzdQWItFc86WCtN7Nj0rOHJWD-/view

Millhiser, I. (2024, March 21). The Supreme Court's abortion pills case, explained. *Vox*. https://www.vox.com/scotus/2024/3/21/24105984/supreme-court-mifepristone-abortion-pills-fda-alliance-hippocratic-medicine

Millhiser, I. (2024, May 27). The Comstock Act, the long-dead law Trump could use to ban abortion, explained. *Vox*. https://www.vox.com/abortion/351678/the-comstock-act-the-long-dead-law-trump-could-use-to-ban-abortion-explained

Mills Jr, G. G. (2023). Impact of California Community Colleges Student Centered Funding Formula on First-Generation College Students at Minority Serving Institutions: An Exploration of the Perspectives of Student Services Professionals [Doctoral dissertation, California Baptist University]. https://share.calbaptist.edu/server/api/core/bitstreams/03467581-71ef-4865-8524-cc2206afa7a9/content

Moore, A. W. (2021). Socioeconomics as a Factor Impacting Graduation Rates of African Americans at Historically Black Colleges and Universities and Predominantly White Institutions [Doctoral dissertation, Florida Agricultural and Mechanical University].

Morel, G. M., & Spector, J. M. (2022). *Foundations of educational technology: Integrative approaches and interdisciplinary perspectives*. Routledge.

Namukasa, M., Ficke, C., & Piasecki, I. (2023). Understanding how to diversify the cybersecurity workforce: A qualitative analysis. *Journal of Cybersecurity Education, Research and Practice*, *2023*(2), 4. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1145&context=jcerp

National Center for Science and Engineering Statistics. (2023, January 30). *Diversity and STEM: Women, Minorities, and Persons with Disabilities 2023 | NSF - National Science Foundation*. Ncses.nsf.gov. https://ncses.nsf.gov/pubs/nsf23315/report

National Science Foundation. (2023). *Diversity and STEM: Women, Minorities, and Persons with Disabilities 2023 | NSF - National Science Foundation*. Ncses.nsf.gov. https://www.nsf.gov/reports/statistics/diversity-stem-women-minorities-persons-disabilities-2023

Office of the National Cyber Director. (2024). *2024 Report on The Cybersecurity Posture of the United States Office of the National Cyber Director Executive Office of the President*. https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

Okechukwu, L. (2024). *How Much Does It Cost to Study Stem Courses In the USA?* After School Africa; After School Africa. https://www.afterschoolafrica.com/75626/how-much-does-it-cost-to-study-stem-courses-in-the-usa/

Pettersson, F. (2021). Understanding digitalization and educational change in school by means of activity theory and the levels of learning concept. Education and Information Technologies, 26(1), 187-204. https://link.springer.com/article/10.1007/s10639-020-10239-8

Philips, A. (30 July 2024). What is Project 2025? *The Washington Post*. https://www.washingtonpost.com/politics/2024/07/12/project-2025-summary-trump/

Pierszalowski, S., Bouwma-Gearhart, J., & Marlow, L. (2021). A systematic review of barriers to accessing undergraduate research for STEM students: problematizing under-researched factors for students of color. *Social Sciences*, *10*(9), 328. https://doi.org/10.3390/socsci10090328

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal*, 18(3), 44-53. https://files.eric.ed.gov/fulltext/EJ1258205.pdf

Pinnock, C., Rothen, J., Carlough, T., & Shah, N. R. (2023). Improving value for underserved populations with a community-based intervention: a retrospective cohort study. *Archives of Public Health*, *81*(1). https://doi.org/10.1186/s13690-023-01117-z

Pitman, L., Payne, B. K., Vandecar-Burdin, T., & Thorbjornsen, L. (2022). Toward a Student-Ready Cybersecurity Program: Findings from a Survey of STEM-Students. Journal of Cybersecurity Education, Research and Practice, 2022(2). https://files.eric.ed.gov/fulltext/EJ1387219.pdf

Prokop, A. (30 July 2024). Politics. Project 2025: The myths and the facts. https://www.vox.com/politics/360318/project-2025-trump-policies-abortion-divorce

Quinn, M. (2022, June 24). Supreme Court strikes down Roe v. Wade in seismic shift for abortion rights. *CBS News*. https://www.cbsnews.com/live-updates/supreme-court-roe-v-wade-abortion-rights/

Ramirez, G., Covarrubias, R., Jackson, M., & Son, J. Y. (2021). Making hidden resources visible in a minority-serving college context. *Cultural Diversity and Ethnic Minority Psychology*, 27(2), 256.

Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, *3*(5), 346. https://doi.org/10.1007/s42979-022-01239-1

Rosen, J., & Quinn, M. (2024, July 30). Head of pro-Trump Project 2025 steps down as Democrats ramp up attacks. Cbsnews.com; *CBS News*. https://www.cbsnews.com/news/project-2025-paul-dans-steps-down-heritage-foundation/

Roy, S., Kreidl, O. P., Umapathy, K., Prodanoff, Z. G., & Vakilinia, I. (2022, December). Building Framework and Infrastructure to Assist a Minority Serving Institution (MSI) in Cybersecurity Program Development. In *2022 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 2137-2139). IEEE. https://american-cse.org/csci2022-ieee/pdfs/CSCI2022-2lPzsUSRQukMlxf8K2x89I/202800c145/202800c145.pdf

Shrestha, A. (2023, May 18). *Cyber Security Course in USA*. Studyinfocentre.com; Study Info Centre. https://studyinfocentre.com/blog/usa/country/cyber-security-course-in-usa

Strauss, P. (2022, October). *Due Process*. Cornell Law School. https://www.law.cornell.edu/wex/due_process#:~:text=The%20Fifth%20Amendment%20says%20to

Streit, H. M. (2023). *Categorical Allocations of Title 1 Funding and Student Achievement.* University of South Dakota.

Taylor, I. R. (2020). *Understanding the role of HBCU boards of trustees in advancing institutional quality and ensuring HBCU survival*. University of Pennsylvania.

The Heritage Foundation. (2023). *Mandate for Leadership: the Conservative Promise*. https://static.project2025.org/2025_MandateForLeadership_FULL.pdf

Thomas, C. N. (2024). *Cybersecurity education praxis and broadening participation in cybersecurity: Pieces of the same puzzle*. https://ir.library.louisville.edu/cgi/viewcontent.cgi?article=5598&context=etd

Tisler, D., & Norden, L. (2024, July 17). *Project 2025's Plan for Cybersecurity Agency Threatens Election Security*. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/project-2025s-plan-cybersecurity-agency-threatens-election-security

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573-586. https://doi.org/10.3390/jcp2030029

Turner, C. B., Turner, C., & Ashe, A. (2022). Establishing the Sociology and Cybersecurity Nexus Through Experiential Learning: Cybersecurity Innovation on an HBCU Campus. *Journal of Negro Education*, 91(2), 213-224. https://par.nsf.gov/servlets/purl/10429311

United Nations. (2023). *Recognizing Need to Bolster Indigenous Peoples' Rights, Third Committee Underscores Importance of Respecting Traditional Lands, Valuable Conservation Knowledge | UN Press*. Press.un.org. https://press.un.org/en/2023/gashc4379.doc.htm

Valant, J., Meyer, K., & Perera, R. M. (2024, August 12). Project 2025 *and education: A lot of bad ideas, some more actionable than others*. Brookings. https://www.brookings.edu/articles/project-2025-and-education-a-lot-of-bad-ideas-some-more-actionable-than-others/

Vargas, N., Villa-Palomino, J., & Davis, E. (2020). Latinx faculty representation and resource allocation at Hispanic serving institutions. *Race Ethnicity and Education*, 23(1), 39-54.

Weible, C. M. (Ed.). (2023). *Theories of the policy process*. Taylor & Francis.

Wendling, M. (16 August 2024). Project 2025: A wish list for a Trump presidency explained. *BBC.com*. https://www.bbc.com/news/articles/c977njnvq2do

Williams, E. R. (2022). *Performance Measurement Indicators and Their Impact on Historically Black Colleges and Universities* [Doctoral dissertation, Walden University].