Strengthening National Security: Assessing the Adequacy of the U.S. Federal Government Efforts in Securing Public Infrastructure

Brad Voris

Wilmington University

ENG122: English Composition II

Professor Ashley Mortimer

4/28/2024

Strengthening National Security: Assessing the Adequacy of the U.S. Federal Government Efforts in Securing Public Infrastructure

In an era marked by unprecedented technological innovations, and emerging threats, the security of public infrastructure stands as a cornerstone of national resilience and prosperity. From transportation networks facilitating the movement of goods and people to energy grids powering homes and industries, and communication systems enabling global connectivity, public infrastructure defines every aspect of modern society. The integrity of these critical assets is increasingly jeopardized by an array of hazards, ranging from cyberattacks and natural disasters to physical sabotage and terrorism. The efficiency of governmental efforts in securing public infrastructure emerges as an incredible concern, shaping the resilience of our nation and the well-being of our citizens. Public infrastructure includes a myriad of physical and virtual assets that are essential for the functioning of society and the economy. This includes but is not limited to roads, bridges, railways, airports, ports, energy generation and distribution facilities, water supply systems, telecommunications networks, and digital infrastructure. The interconnected nature of these systems to the internet fosters efficiency and convenience but also introduces vulnerabilities, where disruption or compromise in one sector can cascade issues and have repercussions across multiple domains. Ensuring the security and resilience of public infrastructure is not merely a matter of protecting tangible assets but safeguarding the very fabric of national security and societal stability. Against this backdrop, the role of the U.S. Federal Government in securing public infrastructure looms large, entrusted with the responsibility of devising and implementing strategies to mitigate risks and enhance resiliency. Federal agencies such as the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security

Agency (CISA), the Department of Transportation (DOT), the Department of Energy (DOE), and the Federal Emergency Management Agency (FEMA) are tasked with coordinating efforts, developing regulations, and providing support to state and local authorities and private sector partners. Regulatory frameworks such as the National Infrastructure Protection Plan (NIPP) and the Critical Infrastructure Protection (CIP) program provide overarching strategies for safeguarding infrastructure assets against various threats. Despite these programs, there are concerns regarding the adequacy and efficiency of government actions in securing public infrastructure. The increasingly frequent and sophisticated nature of cyberattacks targeting critical systems, the vulnerability of aging physical infrastructure to natural disasters and the evolving threat landscape of geopolitical tensions highlights a dynamic challenge. Constraints such as limited funding, bureaucratic inefficiencies, regulatory complexities, and the rapid pace of technological innovation pose additional challenges to achieving comprehensive infrastructure security. This research seeks to define the extent to which the U.S. Federal Government fulfills its mandate of securing public infrastructure. By examining existing policies, initiatives, and operational practices, as well as analyzing case studies and expert opinions, the aim of this paper is to show the strengths, weaknesses, and areas for improvement in governmental efforts. Through a granular understanding of the complexities in infrastructure security and the broader geopolitical context, this research hopes to contribute to informed discourse and policymaking aimed at enhancing resiliency and safeguarding national infrastructure.

The Public Infrastructure We All Rely On

What is public infrastructure? According to the American Society of Civil Engineers (ASCE) Infrastructure Report Card, in 2021:

> Infrastructure supports nearly every aspect of life. Our pipes deliver drinking water to homes and hospitals. Airports, railroads, and inland waterways transport goods from farms and manufacturing plants to store shelves. The roads that crisscross the country allow us to get to work and school safely, and the network of transmission and distribution lines keeps the lights on and our electronics charged. Dams enable consistent water supply in arid climates and levees hold back floodwaters to protect rain-soaked communities.

Public infrastructure is the backbone of services that support daily life in the United States, without these services adequately protected they will fall to threats and incidents. (p.1)

Evaluation of Current Government Efforts in Securing Infrastructure

The U.S. Federal Government has implemented various policies and initiatives aimed at securing public infrastructure, yet concerns persist regarding their adequacy and effectiveness. According to an article in The Washington Post, a senior Biden administration official stated, (Marks, 2021)," The absence of mandated cybersecurity requirements for critical infrastructure is what in many ways has brought us to the level of vulnerability we have today…". This a key reason for current efforts in developing security regulation for critical infrastructure. An effort by the Federal Government is the National Infrastructure Protection Plan (NIPP). The NIPP outlines

strategies for identifying and mitigating risks to critical infrastructure. Critics argue that the NIPP lacks specificity and fails to address emerging threats adequately. For example, a report by the Government Accountability Office (GAO) (2018), highlighted deficiencies in DHS's implementation of the NIPP, citing issues such as inconsistent risk assessments and insufficient coordination among stakeholders. This indicates a gap between policy creation and implementation. It also undermines the overall effectiveness of government efforts. In an article by the Washington Post (2018), the same official also stated (Marks, 2018): “Short of legislation, there isn’t a comprehensive way to require deployment of security technologies and practices that address really the threat environment we face.” This comment highlights the shortfalls of consistent and comprehensive deployment capabilities of security technology in the critical infrastructure and without strong legislative enforcement.

Another key aspect of government initiatives is cybersecurity, given the increasing prevalence of cyber threats targeting critical infrastructure. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) plays a central role in this domain, providing guidance, threat intelligence, and incident response capabilities to protect vital systems. However, cybersecurity experts argue that existing measures are insufficient to address the evolving nature of cyber threats. According to Harvard Business Review (Kenny & Nagle, 2024), the SolarWinds cyberattack in 2020 exposed vulnerabilities in government networks, highlighting the need for enhanced cybersecurity measures and greater collaboration between government agencies and the private sector. Without proactive measures to bolster cyber defenses, critical infrastructure remains susceptible to disruptive cyber incidents.

The Federal Emergency Management Agency (FEMA) plays a crucial role in disaster preparedness and response, particularly in safeguarding infrastructure against natural disasters.

FEMA's Hazard Mitigation Assistance (HMA) programs provide funding for projects aimed at reducing the risk of future disasters and enhancing infrastructure resilience. According to FEMA (2023), their mission is “helping people before, during, and after disasters.” Critics argue that FEMA's approach is reactive rather than proactive, focusing primarily on post-disaster recovery rather than pre-disaster mitigation. Communities affected by Hurricane Katrina faced significant challenges in rebuilding infrastructure and mitigating future risks, despite FEMA's assistance. This highlights the need towards proactive risk management strategies to enhance infrastructure resilience and minimize the impact of future disasters.

Challenges and Limitations

Despite the government's efforts, several challenges hinder the effective security of public infrastructure. One such challenge is inadequate funding and resource allocation, which limits the implementation of robust security measures. For instance, a study by the American Society of Civil Engineers (ASCE) (2021), found that the U.S. faces a substantial infrastructure investment gap, with an estimated $2.6 trillion needed by 2029 to address critical infrastructure needs. Without sufficient funding, agencies struggle to prioritize security enhancements and address emerging threats effectively.

Bureaucratic inefficiencies and regulatory complexities impede coordination and collaboration among government agencies and stakeholders. The fragmented nature of infrastructure governance, with responsibilities dispersed across multiple agencies and levels of government, complicates decision-making and hampers the implementation of cohesive security strategies. Overlapping jurisdictional boundaries and conflicting regulatory frameworks can impact information sharing and hinder the timely response to security threats. Addressing these

structural barriers requires streamlining governance structures and enhancing intra-agency cooperation to facilitate more coordinated responses to emerging threats and threat actors.

The rapid pace of technological innovation presents challenges in securing increasingly interconnected and digitized infrastructure systems. The Internet of Things (IoT), cloud computing, and other emerging technologies offer numerous benefits but also introduce new vulnerabilities and attack vectors. For example, the proliferation of IoT devices in critical infrastructure sectors such as energy and transportation expand the attack surface and creates potential entry points for threat actors. Without robust cybersecurity measures and vigilant risk management practices, these technological advancements can exacerbate existing vulnerabilities and increase the likelihood of disruptive cyber incidents.

Addressing the Opposition

While critics raise valid concerns about the adequacy of government efforts to secure public infrastructure, it is essential to acknowledge the progress made and the complexities inherent in addressing evolving threats. Government agencies have taken significant steps to enhance infrastructure security, including the development of risk assessment methodologies, the establishment of information-sharing mechanisms, and the promotion of public-private partnerships. For example, initiatives such as the Transportation Security Administration's (TSA) Pipeline Security Guidelines, and the Department of Energy's (DOE) Cybersecurity Capability Maturity Model (C2M2) provide valuable resources and guidance to enhance sector-specific security practices. The examples provided by each of these entities encompass appropriate security control alignment with best practices.

The American Society of Civil Engineers stated (2021), that “the elected officials and members of the public who have improved infrastructure policy and supported additional funding are applauded. We’re seeing the benefits of this action in drinking water, inland waterways, and airports. The private sector has invested in the electric grid, freight rail, and more.” This demonstrates that government and private sectors have been successful in collaboration and facilitating the security of public infrastructure with policy enforcement.

It is important to recognize the inherent trade-offs between security and other policy objectives, such as economic efficiency and individual privacy. The World Economic forum suggests, (*WEF,* 2022), “The mission seems clear: to setup comprehensive public-private cooperation models that help assure the provision of essential services to the government, the economy and the public.” Striking the right balance requires careful consideration of competing interests and the adoption of risk-based approaches to prioritize security investments effectively. The implementation of resilient design principles in infrastructure planning and development can enhance infrastructure security while minimizing the impact on cost and functionality.

While challenges persist, the U.S. Federal Government has made significant strides in securing public infrastructure against a myriad of threats. By addressing deficiencies in policy formulation, enhancing collaboration stakeholders, and embracing innovative approaches to risk management, the government can strengthen the resilience of critical infrastructure and ensure the continued prosperity and security of the nation.

Conclusion

In conclusion, the U.S. federal government's efforts to secure public infrastructure have seen progress, including the development of risk assessment methodologies, the establishment of

information-sharing mechanisms, and the promotion of public-private partnerships. These measures have played a pivotal role in enhancing the overall security of public infrastructure. Significant challenges such as limited funding, bureaucratic inefficiencies, and the rapid pace of technological innovation continue to impede the effectiveness of security controls and the government's ability to adapt to emerging threats.

To strengthen the resilience of critical infrastructure, the government must focus on continuous assessment and improvement of strategies and initiatives. This includes addressing deficiencies in policy formulation and enhancing collaboration with stakeholders. Shifting from reactive to proactive risk management strategies is essential for building resilient infrastructure systems. By balancing security with other policy objectives such as economic efficiency and individual privacy, the government can adopt a holistic approach that promotes the sustainable protection of public infrastructure. Ultimately, the federal government must take decisive action to enhance collaboration, funding, and risk management to ensure the continued safety and prosperity of the nation.

References

Joseph Marks, (2021, July 28), *The Cybersecurity 202: Biden plans to expand government's role protecting key industries from cyberattacks.* Washingtonpost.com, NA. https://link-gale-com.mylibrary.wilmu.edu/apps/doc/A669906476/OVIC?u=new90507&sid=bookmark-OVIC&xid=f0520b39

World Economic Forum, (2022, May 24), *Here's why securing critical infrastructure is so important*. https://www.weforum.org/agenda/2022/05/securing-systemically-important-critical-infrastructure/

Government Accountability Office (GOA), (2018, June 14), *Critical Infrastructure Protection Progress and Challenges in DHS's Management of Its Chemical Facility Security Program GAO-18-613T,* https://www.gao.gov/assets/700/692889.pdf

DAMS SECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). (2022). https://www.cisa.gov/sites/default/files/publications/dams-c2m2-2022-508_0.pdf

American Society of Civil Engineers, (2021) *A Comprehensive Assessment of America's Infrastructure.* Reston. https://infrastructurereportcard.org/wp-content/uploads/2020/12/2021-IRC-Executive-Summary-1.pdf

Pipeline Security Guidelines. (2018). https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

Kenny, B. & Nagle, F. (Hosts). (2024, January 16). *How SolarWinds Responded to the 2020 SUNBURST Cyberattack* (No. 222). In Cold Call. Harvard Business Review.

https://hbr.org/podcast/2024/01/how-solarwinds-responded-to-the-2020-sunburst-cyberattack#:~:text=In%20December%20of%202020%2C%20SolarWinds

FEMA. (2023). About us. Www.fema.gov. https://www.fema.gov/about