Gursharan Singh, Rishik Kolli, and Sharmila Nimbkar

Dr. Trowbridge

Grand Challenges for Engineers

5 February 2021

# Opportunity Identification and Needs Analysis

## Context:

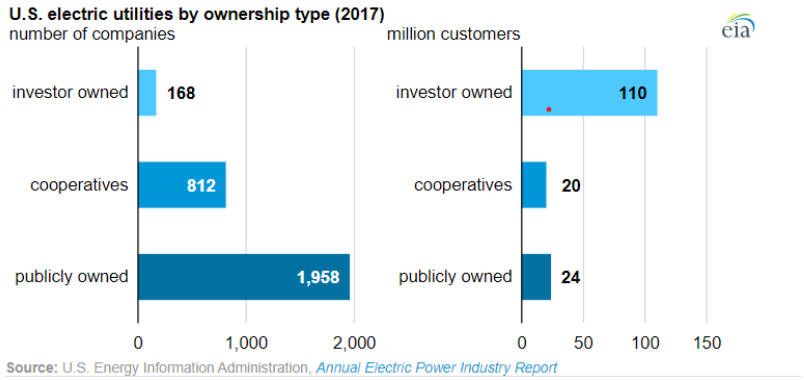
Energy fuels the nation, which is relied upon by business, individuals and government agencies. The energy which provides the infrastructure for this productivity and essential ways of life to occur has become highly vulnerable over time to foreign and domestic threats. The energy grid has become prone to cyber attacks, which can potentially debilitate the energy infrastructure in place. According to the Center for Strategic and International Studies, since 2006 the country's energy infrastructure has cracked under the pressure of an onslaught of cyberattacks from North Korea, Iran, India, China, Russia, and nefarious hacker groups [1]. The impact is not to be taken lightly; a 2015 article by Reuters illustrates that cyber attacks on the US power grid amount to $1 trillion dollars of economic losses annually [2]. There is a great need to increase security in these areas of energy in order to have a safer and protected grid. The threats posed by these foreign advisories are committing hacks into energy agencies and preventing them from providing electricity to cities, hospitals, military bases and businesses. In case of a national emergency to occur the nation should have reservoirs of energy to fallback in times of crisis. The purpose of this project is to improve energy security for government agencies, citizens, and energy providers in the US.

## Target Customers and Relevant Stakeholders:

Stakeholders include the consumers of electricity, energy corporations, and US national security agencies. The consumers of electricity include homes, industry, and businesses, who care about the costs and reliability of energy to function from day to day. These stakeholders can be characterised as concerned with the economic costs of lack of energy security. According to the Environmental Protection Agency, even a 10% increase in energy prices can result in a $393 decline in real disposable income per capita [3].

Energy corporations such as SRP, PG&E, and Duke Energy are large stakeholders in any attempt to secure the US energy grid. According to the US Department of Energy, “With 90 percent of the nation’s power infrastructure privately held, coordinating and aligning efforts between the government and the private sector is vital” [4]. These people can be characterized as also being concerned with the cost of energy security as it pertains to their business margins.

A more general stakeholder is the US government, specifically the Department of Energy, which establishes the guidelines and regulations for the private energy sectors and would be in a position to enforce any regulations.




The graphic above, from the US Department of Energy, demonstrates that investor owned businesses serve a large majority of American. However, a multitude of smaller, publicly owned federal, municipal, and county facilities serve populations on the local level (especially in rural

areas). Thus, since investor owned utilities are the vast majority of electric companies, economic incentive and cost reduction will be an important factor in any implemented solution.

Primary Target Audience:

The primary target audience would be the US government, since they oversee the impacts of international affairs as it pertains to American energy security. Additionally, any attempt to improve the cybersecurity of the American powergrid would invariably involve the CIA and FBI, who would have to approve and oversee all changes. These stakeholders can be characterized as being deeply concerned with information security, as well as the impact that foreign cyberwarfare has on energy security.

Identify Customer Needs:

The US government will have a variety of requirements and criteria for any cybersecurity solution implemented on government systems. The government is a large organization which will need a solution that is simple to implement. The government has a large amount of money to finance and energy security initiatives, however they will want it to be financially viable so they can encourage or subsidize the product or service to be used by corporate stakeholders.

Finally, the democratic nature of the government means that a solution would have to incur bipartisan support by walking the line between overregulation and leaving the US vulnerable to cyberattacks.Their organization size is vast, and any solution would have to be able to integrate seamlessly with the existing cyber-infrastructure. Additionally, the solution would have to be financially viable enough that the corporate sector would be willing to embrace it in order to come to par with more stringent government regulations on cybersecurity.

Describe Innovation Opportunity:

The sudden increase of the use of the internet and its incorporation into a variety of technologies is leaving a place for potential vulnerability to be taken advantage of by malicious actors if not protected against. This technology has sought its way into being incorporated into physical infrastructure of critical energy infrastructure. According to Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector by Mission Support Center Idaho National Laboratory August 2016 states, "Nation-states like Russia, China, and Iran and non-state actors, including foreign terrorist and hacktivist groups, pose varying threats to the power grid. A determined, well-funded, capable threat actor with the appropriate attack vector can succeed to varying levels depending on what defenses are in place" [5]. For example in the larger context the use of devices in the Internet of things, allows for potential breaches into pre existing networks. The government can purchase a multitude of products that it needs to use in order to facilitate or screen certain infrastructures. These products can pose an array of vulnerabilities because of their small size and low maintenance levels, causing uncertainty in its network architectures . Unmaintained and untested softwares and devices in the long run can be exploited by state threat actors to surveille or compromise a potential infrastructure in place. Posing potential threats to the safety of the United States. The increase of the interaction between networks and the internet, is causing cyberspace to be the new battlefield of nations.

**Provide background information about the current situation that exists.**

**Propose Requirements:**

-the design must be able to secure site materials and data

-the design must detect potential dangers

-the design must protect classified matter on both state and federal levels

-the design must be able to scale the level of threat if there is an intrusion

-the design must be user friendly and easily understandable so that employees may have appropriate knowledge

- the design must ensure the security of the site

-the design must perform at a high level

-the design must be able to oversee all users and data currently accessing the program

-the design must ensure the security of information and data

-the design must be able to protect and withstand foreign users or terrorists

-the design which threats are harmless and which have the potential for danger

-the design must effectively communicate with the user

-the design must trace back who the foreign user was who tried to access the data\

**Develop value proposition:**

Overcoming these challenges will allow for the decreasing of potential risk from attacks taking place on American soil that can harm American interests. This prevention will embolden American influence abroad and also protects from cyberthreats which ends up costing the American economy over one trillion dollars annually.

Reference

Office of Cybersecurity, Energy Security, and Emergency Response. “Cybersecurity”, US Department of Energy, 2020. <https://www.energy.gov/ceser/cybersecurity>.

Kristy Hartman. “Protecting the Nation’s Energy Infrastructure: States Address Energy Security”, National Conference of State Legislatures, 2013. <https://www.ncsl.org/documents/energy/EnergySecurityFinal-10-13.pdf>

“Investor-owned utilities served 72% of U.S. electricity customers in 2017”, US ENergy Information Administration, Aug 15 2019. <https://www.eia.gov/todayinenergy/detail.php?id=40913>

Idaho National Laboratory. “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector”.US Department of Energy, August 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>

Mark Febrizio. “Lesson For EPA: Higher Energy Prices Harm People”. Institute for Energy Research, August 20 2015. <https://www.instituteforenergyresearch.org/the-grid/lesson-for-epa-higher-energy-prices-harm-people/#:~:text=%5B12%5D%20When%20electricity%20prices%20increase,rural%20America%20would%20be%20substantial.>

*How bad are cyberattacks for the economy? This professor helped the White House assess the damage*. [Online]. Available: https://www.brandeis.edu/global/news/2020/scherbina-q-a.html. [Accessed: 05-Feb-2021].

“Significant Cyber Incidents,” *Significant Cyber Incidents | Center for Strategic and International Studies*. [Online]. Available:

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. [Accessed: 05-Feb-2021].

"Lesson For EPA: Higher Energy Prices Harm People," *IER*, 20-Aug-2015. [Online]. Available: https://www.instituteforenergyresearch.org/the-grid/lesson-for-epa-higher-energy-prices-harm-people/#:~:text=%5B12%5D%20When%20electricity%20prices%20increase,rural%20America%20would%20be%20substantial. [Accessed: 05-Feb-2021].

*Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, 2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf. [Accessed: 04-Feb-2021].

"Cyber attack on U.S. power grid could cost economy $1 trillion: report," *Reuters*, 08-Jul-2015. [Online]. Available: https://www.reuters.com/article/us-cyberattack-power-survey/cyber-attack-on-u-s-power-grid-could-cost-economy-1-trillion-report-idUSKCN0PI0XS20150708. [Accessed: 05-Feb-2021].

"Safeguards and Security Program Specific Qualification Standard," *Energy.gov*, Jul-2020. [Online]. Available: https://www.energy.gov/sites/prod/files/2020/08/f77/FTCP-PSQS-1171-2020-Safeguards-and-Security_0.pdf. [Accessed: 04-Feb-2021].