Title:

Ukraine Ministry of Energy:

Implementing Distributed Generation with Sound Cybersecurity Planning to Help Ukraine in its War Against Russia

Student Name:

Mustavi Islam

Student ID:

16334245

Section:

5573-0001, MWF 9-9:50

Team No.

3

Team Members:

Ally Ryan

Mustavi Islam

Table of content Page

Motivation: In February 2022, Russia began its attack on Ukraine by targeting Ukrainian energy infrastructure, generating facilities, and/or other elements of the Ukrainian power system with missile and drone attacks, reducing the operational integrity and resiliency across the Ukrainian power grid and leading to dangerous city-wide blackouts [1]. This disruption has caused a need for the Ukrainian energy sector to 1) first be repaired so that the Ukrainian citizens have needed resources such as electricity, heat, health care access, internet access, and clean water access, etc., and 2) once repaired and stable, become resistant to future attacks. To repair and improve the Ukrainian energy sector, we propose a strategy of distributed generation with sound cybersecurity planning. Broadly, generation is chosen for the project because during the bulk of the war when the mass destruction of Ukrainian homes and energy facilities were taking place, the Ukrainian citizens had to rely primarily on generators for heat and electricity, which were unreliable because generators rely on fuel, which is not accessible for purchase when a sheltering order is in place. More specifically, by utilizing distributed generation, Ukraine ensures that its power system is not reliant on one central energy facility, but rather on many across each city and home. Further, by utilizing distributed generation, which modernly uses solar energy (i.e., renewable energy), the Ukraine would no longer depend on fuel to generate power, but rather on unlimited, natural sources.

Challenges: The following are common cybersecurity challenges of Distributed Energy Resources (DER's) that we 1) expect to encounter and 2) will seek to mitigate and solve as we aim to modernize Ukraine's energy sector [2]. Because we believe it is in Ukraine's best interest to employ a distributed generation strategy, the cybersecurity concerns, while solvable, automatically become more complex due to the decentralized nature of having many smaller, and not just one major source of power. As such, it will be of great importance to account for the below challenges, as an infection to the entire distributed system could prove to be fatal to the Ukrainian power system and in turn cause many Ukrainian citizens to endure the harsh realities of power outages, and thus limited heat, water, healthcare access, and internet access, etc. However, if appropriately planned, then Ukraine will have an energy system that is resilient to Russian (or other malicious) attacks in the future.

1) **DER supply chain compromise:** The installation and operational function of distributed energy resources are dependent on the advice, communication, and supplies provided by external third-parties and vendors. It is possible that these external parties can be disrupted by a cybersecurity attack, leaving them unable to fulfill their roles for their clients.

2) **DER botnet:** A DER botnet attack is when malware takes control of the distributed energy systems' operational functions, leaving them vulnerable to not just a single DER disruption, but mass power outages and grid instability.

3) **DER worm:** A DER worm is likely to start infecting one component of one DER, but then will likely infect the entire DER system and then will spread to other systems with an internet connection to the "original" DER.

4) **DER ransomware:** DER ransomware is when a malicious software blocks access, usually by means of encryption, to the operational software of the distributed energy components until a requested amount of money is paid.

5) **DER denial-of-service:** A DoS attack is when malware makes all resources on a machine inaccessible to the legitimate users.

In addition to noting the common cybersecurity challenges that we expect to encounter, we feel that it is important to note the main challenges that are specific to just this project and will be extremely pertinent to account for. Challenges unique to this project can be found below:

1) Ukraine is currently at war with Russia, and some areas with vital energy infrastructure are still under Russian control. As such, it is difficult to assess the complete state of the Ukraine's energy sector as it currently stands.

2) Employing a distributed generation strategy means there will be many smaller systems to manage and operate, rather than just one large system. While it will be more difficult to take down most or all of the smaller systems at once, it is still possible. If there were to be a successful cybersecurity attack to many components of the distributed system, it would be a challenge to quickly and efficiently revitalize each system to full working capacity, as each of those tasks would have to be done separately. In general, the many components of DER's require a very organized system that 1) manufactures, builds, distributes, and sets up, etc., each DER at what could be many different locations, and 2) operates and monitors each DER. Simply, to develop a distributed generation strategy for the entire country of Ukraine is a monstrous engagement that will be very expensive and take very careful planning and a long amount of time.

3) The main purpose of this project is to modernize Ukraine's power grid so that the Ukrainian citizens do not have to endure forced (due to the destruction of their central generation facility) or government sanctioned blackouts. During these blackouts, the Ukrainian citizens had to utilize fuel-reliant generators for needs

such as heat, electricity, and healthcare. However, since fuel is 1) expensive and, more notably, 2) not accessible for purchase under stay-at-home and/or sheltering orders, the most reasonable strategy is to distribute “renewable energy generators” across the country, which can be achieved through solar panels and/or photovoltaic energy generation. The challenge with this strategy is that both solar panels and photovoltaics (PVs) are extremely expensive. While this project is only meant to develop the plan and strategy of distributed generation with sound cybersecurity planning and will not handle the implementation of DER’s or physical assets at generational facilities, it will need to implement a plan that the Ukrainian government is willing and able to install and implement.

4) As a general class note, this project has the potential to be very detailed and extremely interesting and impactful. However, due to limited time, resources, communication contracts, technical abilities and knowledge, as well as limited manpower on this project, the detail, accuracy, and thoroughness will have to match accordingly. If this were a real-world implementation, it would take a significant taskforce and amount of money. Despite this, we will take on the challenge of forming a snapshot of what this real-world implementation would look like.

Proposed Proposal: The proposal section is divided into the following categories: policy (including a more detailed risk management and contingency plan), roles, top-down approach

diagram, technologies used, information assets used, threats to information assets, and general information security guidelines.

1. **Policy:** The United States Department of Energy (U.S. DOE) created the Distributed Energy Resources Cybersecurity Framework (DERCF), which was the first framework to adopt the full span of controls necessary to protect a DER system. The DERCF is compliant with the National Institute of Standards and Technology (NIST), as a best practice for government organizations. Within the DERCF, there are three main areas prioritized for optimal cybersecurity protection (governance, technical management, and physical security), as well as subdomains within each of those three categories that specifically address the necessary controls needed for protection [3]. For this project, objectives were summarized from the DERCF to form policies. The policies, organized by their relevant subdomains, can be found below:

Governance Policy	
Subdomain	Policy
Risk Management	1) Document a cybersecurity risk-management strategy. 2) Document and identify all cybersecurity risks. 3) Perform risk assessments to identify the level of each cybersecurity risk. 4) Follow all documented procedures in the risk-management strategy when managing risk. 5) Identify and involve the appropriate stakeholders when managing risk. 6) Update the risk-management strategy frequently.
Asset, Change, and Configuration Management	1) Maintain a current inventory of assets and a list of each asset's main attributes. 2) Maintain configuration baselines for inventoried assets. 3) If an asset is inventoried, ensure that changes are tested and the appropriate stakeholders are consulted, informed, and in agreeance with the change before the change is implemented. Any change to an inventoried asset should be logged. 4) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to asset inventory, configuration, and change-management activities.

Identity and Access Management	1) Ensure that the identities of personnel, services, or devices who require access to assets are validated, that individuals are only allowed access to assets when they have been appointed to conduct a task, and that the individuals allowed to access the assets are provided with the appropriate credentials to gain access to the relevant systems. 2) Control access to assets by developing a list of access requirements and grant access to assets only when all the requirements are met. 3) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to establishing and maintaining identities and control access.
Threat and Vulnerability Management	1) Identify, document, analyze, assess, address, and identify the priority of all threats and vulnerabilities for each cybersecurity function. 2) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to threat and vulnerability management activities.
Situation Awareness	1) Define and follow log requirements for each asset. 2) Continuously monitor for cybersecurity events or any anomalous activity and always maintain an updated record of the current cybersecurity posture. 3) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to logging, monitoring, and the common operating picture.
Information Sharing and Communications	1) Ensure that information is only shared with appointed individuals, stakeholders, or organizations in a secure manner. 2) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to information sharing activities.
Event and Incident Response	1) Ensure that cybersecurity events and cybersecurity event escalation are detected, reported, logged, and that there are appropriate criteria for the detection, reporting, and logging process. 2) Assign roles to personnel in the event of a cybersecurity incident and ensure that the personnel assigned to roles are trained according to the incident response plan. 3) In the event of a cybersecurity incident, develop a continuity plan to return to normal operations as quickly and safely as possible. 4) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to cybersecurity event and incident response, and for the continuity of operation activities.
Supply Chain Enterprise Data Management	1) Ensure that supplier and customer dependencies are identified based on relevant guidelines. 2) Ensure that cybersecurity requirements and risks are considered, contracted, and accounted for when relationships with dependencies are established. 3) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to managing dependency risk.

Workforce Management	1) Assign roles and responsibilities for the workforce in charge of cybersecurity. 2) Vet and maintain strict standards for the handling of cybersecurity assets for all individuals assigned cybersecurity roles and responsibilities. 3) Provide training to and identify the knowledge gaps of all individuals assigned cybersecurity roles and responsibilities. 4) Require that all individuals assigned cybersecurity roles and responsibilities participate in activities that increase their cybersecurity awareness. 5) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to cybersecurity management workforce activities.
Cybersecurity Program Management	1) Document a cybersecurity program strategy that contains insight regarding the implementation of governance, and the structure and organization of the cybersecurity program. 2) Document the resources, funding, and policies for changing the cybersecurity program. 3) Ensure that a cybersecurity architecture is established and updated according to a developed plan. 4) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to cybersecurity program management activities.

Cyber-Physical Technical Management Policy	
Subdomain	Policy
Account Management	1) The number of account logins, remote connections, and guest accounts are monitored. 2) Ensure that there is role-based access control for DER controllers. 3) Ensure that there are remote access controls for remote sessions. 4) Ensure that all data collected by the DER is logged according to a developed plan. 5) Ensure that all DER information system and functions are authorized, authenticated, and accounted for.

Configuration	1) Ensure that there are access control security policies and individual access privileges in place when conducting technical management activities. 2) Ensure that cloud storage is not approved by the DER system. 3) Ensure that system settings are appropriate for optimal cybersecurity safety. 4) Ensure that there is contracted language in place when a change is implemented on a DER system, and that security audits are frequently conducted to account for such changes. 5) Ensure that only essential software and applications are installed on each DER system.
System/Device Management	1) Ensure that appropriate identification and protection software integrity mechanisms are in place. 2) Ensure that appropriate system/device management protection measures are in place, such as preventing malware injections, phishing attempts, password management, and restricting the number of access points. 3) Ensure that a fail-safe plan is in place that detects potential failure in each DER system. 4) Ensure that appropriate cryptography measures are in place to prevent unwanted external viewing of private information. 5) Ensure that the DER system can support certificate authorities and a certificate revocation list.

Physical Security Policy	
Subdomain	Policy
Administrative	1) Ensure that auditing activities and regulations such as physical access agreements, third-party physical security solutions, the assignment of roles and responsibilities to the appropriate workforce, and audit logs are in place and conducted for all DER systems. 2) Ensure that there is holistic security and contingency planning that protects the security architecture, documents the physical security plan, and manages the relevant physical security controls. 3) Ensure that the individuals with access credentials to the physical security systems act according to the personnel security plan.

Assets	1) Ensure that there is appropriate equipment installed that can help the DER connect to the main grid in the event of system failure or emergencies, and that the equipment is configured optimally to prevent destruction. 2) Ensure that assets are maintained by securing access devices and utilizing the appropriate protection mechanisms to guard from water damage, fire, temperature, and humidity.
Structure	1) Ensure that DER system components are appropriately distanced in facilities. 2) Ensure that there are appropriate safeguards in place to monitor DER system facilities. 3) Ensure that there is a protection team on site at all DER system facilities.

Risk Management Specifics: Documented above (but also included below) is the risk management policy that the Ukraine Ministry of Energy plans to implement to enable Ukraine's energy sector to be resilient against cybersecurity attacks.

Risk Management	1) Document a cybersecurity risk-management strategy. 2) Document and identify all cybersecurity risks. 3) Perform risk assessments to identify the level of each cybersecurity risk. 4) Follow all documented procedures in the risk-management strategy when managing risk. 5) Identify and involve the appropriate stakeholders when managing risk. 6) Update the risk-management strategy frequently.

The following are details of how the Ukraine Ministry of Energy specifically plans to meet the above policy objectives for risk-management:

1) **Document a cybersecurity risk-management strategy:** A main emphasize of this engagement will be to document a cybersecurity risk-management strategy for the Ukraine Ministry of Energy so that Ukraine can be resilient against cybersecurity attacks. The risk-management strategy planning and writing, for purposes of forming a high-level deliverable that will clearly depict and protect against all necessary areas of risk, will be an on-going process throughout this entire engagement. There are many people, assets, infrastructure, and documents, etc., within the Ukrainian energy sector, thus developing this deliverable while ensuring that the most up-to-date best practices are implemented is a huge task. In addition to developing a risk-management

strategy for the Ukraine Ministry of Energy, we consultants also plan to develop a sound risk-management strategy solely for our work on this engagement. The details of our work in this engagement are top secret and could be cause for an international security risk if it were to fall into the wrong hands. For example, in this engagement, we plan to develop secure access credentials for energy infrastructure facilities. The document containing this information will have to be heavily protected from cybercrime if we don't want to allow access to unauthorized individuals, and thus we will develop a plan to ensure our assets, documents, technologies, and people used in this engagement are well protected from risk as well.

2) **Document and identify all cybersecurity risks:** The Ukraine Ministry of Energy will maintain a list of all elements of the Ukrainian energy infrastructure, all people with access to the Ukrainian energy infrastructure facilities, all people who are authorized to access any asset or confidential knowledge related to the Ukrainian energy sector, and all potential foreign affairs, attacks, or natural or man-made disasters that could pose a risk to the Ukrainian energy sector. These lists will be updated every 10 minutes for all days of this engagement. An update to the list will sound an alarm, and the team member on duty will be in charge of assessing the update and following the appropriate risk assessment and approval guidelines. While the Ukraine Ministry of Energy in this case is a third-party and thus does not specifically own the energy infrastructure assets or hire the government employed workforce that accesses such assets, we are responsible for developing a resilient plan for the Ukraine Ministry of Energy, and thus will take all necessary precautions to protect the Ukrainian energy sector from all possible risks. While the scope of our engagement is to improve the resiliency of the Ukrainian energy sector by implementing sound cybersecurity planning, throughout this engagement we will also have to ensure that the assets that we, as a third-party, are using to conduct this engagement are protected. As such, we will also maintain a detailed list of all assets our company utilizes for this project. This list will contain a detailed data inventory that will include the

locations of each asset/document, who has access to each asset/document, and the purpose of the asset/document. This list will be updated and analyzed daily for important changes. It is important, for example, that Russia will not be able to unethically come across any private information or plans for this engagement, as that would thwart the purpose of this resiliency implementation. As such, there will be serious precautions in place for all discussions, plans, documents, and policies, etc., while we conduct work as consultants for the Ukraine Ministry of Energy.

3) **Perform risk assessments to identify the level of each cybersecurity risk**: Risk assessments will be performed by creating a Risk Matrix Assessment Table (RMAT). This RMAT will contain each DERCF control, and the corresponding NIST CSF control for DER systems. A thorough evidence and artifacts search will be conducted throughout the Ministry of Energy for any written documentation that supports satisfying or not satisfying each cybersecurity control. Stakeholder interviews will also be conducted to follow up on needed questions, or to find relevant evidence that may not be documented. After evidence is collected, the Ministry of Energy team working on this engagement will meet to participate in a round table discussion to determine the disposition of each control as satisfied, partially satisfied, or absent. The level of risk of each partially satisfied or absent control will also be discussed at this time. The RMAT is in the format of an extensive Excel matrix and will be a key deliverable for this engagement.

4) **Follow all documented procedures in the risk-management strategy when managing risk:** All energy infrastructure, documents, policies, procedures, assessments, and assets, etc., will be maintained by multiple team members hired to complete this engagement as consultants for the Ministry of Energy. This will ensure that there is essentially a checks and balances system that ensures that documented procedures in the risk-management strategy are followed. If a machine, energy infrastructure component, or person is found to be out of compliance with a documented procedure, the other employees in the

team will be responsible for reporting the misconduct. The employees will be trained heavily on how to report misconduct, when it is necessary to report misconduct, and who to report such misconduct to.

5) **Identify and involve the appropriate stakeholders when managing risk**: Each asset, process, and document within the Ukrainian energy sector and within our engagement for the Ukrainian Ministry of Energy will have a selected team of stakeholders responsible for managing any possible or occurring risk(s). The stakeholders for each asset, process, and document will be listed in a data inventory, along with their contact information. The stakeholders will have specific authorization capabilities based upon their qualification level and need to carry out their job. The authorization capabilities will also be noted in detail in the risk stakeholder data inventory.

6) **Update the risk-management strategy frequently:** The Risk-Management strategy for both the Ministry of Energy as a whole, and the service that we have temporarily been onboarded to conduct as consultants for the Ministry of Energy will be analyzed, assessed, and updated on a weekly basis. Obviously, we are hired to write the risk-management strategy for the Ministry of Energy, and it will be a work in progress throughout this engagement. However, the purpose of documenting here that there will be weekly updates is to ensure that at the completion of this engagement, Ukraine will have a thorough strategy with the most up-to-date, safe, and sound policies and procedures. There is little room for error when conducting international cybersecurity affairs, and thus it is a priority to maintain cybersecurity best-practices and make any needed improvements to the risk strategies throughout this engagement.

Contingency Planning Specifics: The Ukraine Ministry of Energy will develop a contingency plan to help Ukraine form an energy sector that is resilient against cybersecurity attacks. The contingency plan will be a combined form of a disaster recovery (DR) plan and an Incident Response (IR) plan. The same taskforce assigned to DR will be assigned to IR, and thus will be responsible for anything related to

contingency planning. The specific roles assigned to this contingency taskforce is TBD. In this section, we will provide general policy statements for Incident Response and Disaster Recovery. In this same section, we will also provide an example of a more specific contingency plan for physical security.

Documented above (but also included below) are the broad policy statements that the Ministry of Energy will utilize for an incident response plan. Added are policy statements for disaster recovery. Specifics of this policy will be drafted throughout the course of this project.

Disaster Recovery and Incident Response	1) Ensure that cybersecurity events and cybersecurity event escalation are detected, reported, logged, and that there are appropriate criteria for the detection, reporting, and logging process. 2) Ensure that procedures are in place that enables all harmed information systems to recover and resume operations in an alternative location. 3) Assign roles to personnel in the event of a cybersecurity incident and ensure that the personnel assigned to roles are trained according to the incident response plan. 4) In the event of a cybersecurity incident, develop a continuity plan to return to normal operations as quickly and safely as possible. 5) Document, frequently update, and identify and involve the appropriate stakeholders for all practices relating to cybersecurity event and incident response, and for the continuity of operation activities. 6) Once the incident response plan is complete, develop the appropriate procedures to maintain resilience and take action to restore any lost capabilities or services.

Documented above (but also included below) is the specific contingency planning policy for physical security that the Ukraine Ministry of Energy plans to implement to enable Ukraine's energy sector to be resilient against cybersecurity attacks. More specific details will be drafted throughout this engagement.

> "Ensure that there is holistic security and contingency planning that protects the security architecture, documents the physical security plan, and manages the relevant physical security controls."

The following are details of how the Ukraine Ministry of Energy specifically plans to meet the above policy objectives for physical security contingency planning:

1) **Contingency planning that protects the security architecture:**

    a. Changes to any aspect of Ukraine's physical security architecture will be logged on a secure platform by each member responsible for the specific asset that was changed. There will then be another person that confirms that multiple people reported the change, and that the details of the change are consistent. Once this occurs, the person confirming the change will record the reported changes on the changed/updated/added asset log, the people who reported the change, and will delete the original reports. Maintaining the most updated data on each asset will allow for the most efficient recovery after a disruption.

    b. The contingency plan will consider any dependencies on external providers, third parties, and foreign countries for relevant emergency physical security architecture disruptions. Specifically in this section of the contingency plan, we plan to discuss the obligations that the external parties must meet when receiving private information from the Ukraine Ministry of Energy, and how such information is to be stored and transferred. This plan will also discuss potential ideas for how to resolve each physical security architecture disruption with external parties, as well as when it is necessary to reach out for external help.

2) **Contingency planning that documents the physical security plan:**

    a. The contingency plan will detail how each energy infrastructure site, all energy assets, and all sites containing assets and documents that are used for this engagement will be protected in the event of a disruption. These protection methods may be by locking doors, setting an alarm, and requiring multi-factor authentication for further entrance into rooms, etc.

    b. The contingency plan will be updated weekly to reflect best practices. Such changes will be approved by the relevant personnel. Such updates

will be distributed to all relevant personnel immediately upon documentation.

c. The contingency plan will include how to develop specific authorization boundaries for each system, levels of disruptions when authorization boundaries are crossed, and what to do if an authorization boundary is broken.

3) **Contingency planning that manages the relevant physical security controls:**

a. The contingency plan will include how to manage any changes to the physical security controls based upon newfound general industry best practices, as well as when it is discovered that the control does not adequately protect the Ministry of Energy's cause. In the event of an update or a disruption caused by an inadequate control, the contingency plan will contain detailed information on how to quickly update policies, procedures, and any necessary employee trainings that will allow the Ministry of Energy to safely resume operations.

2. **Roles:** This project will require ample work from many people, all of whom will be subject matter experts (SME's) regarding cybersecurity matters of distributed generation. The roles of each job title needed to carry forth this project can be found below [3]:

a. **Energy Systems Manager**: Manages all personnel handling energy systems and approves all decisions relating to energy use, energy costs, and energy efficiencies].

b. **Systems/Controls Engineer:** Researches and operates control systems to identify efficient operational methods.

c. **Site Security Manager:** Manages all personnel handling the physical security of facilities and relevant assets and approves all decisions regarding relevant physical security matters.

d. **DER System Administrator:** Tasked with ensuring computer servers and networks of DER's are fully and optimally functioning.

e. **Technology System Administrator:** Tasked with ensuring the accounts and system configuration of DER computer servers and networks are fully and optimally functioning with the appropriate safeguards.

f. **Compliance Officer:** Ensures that all standards, guidelines, and mandates are enforced and accurate in the cybersecurity plan.

g. **Information Technology Personnel:** Responsible for installing, maintaining, repairing, and securing all components of the DER's.

h. **Human Resources Personnel:** Perform administrative tasks such as hiring, onboarding, discussing benefits and sick leave, etc.

i. **Manufacturer:** Produce DER's and their components. Manufacturers will be tasked with following specific instructions with the appropriate safeguards to produce products. For this project, no goods will be purchased or produced, but contracts will be signed with the appropriate manufacturers. The manufacturers, despite being third parties, will be employed and will work closely with the system engineers and administrators to ensure needs are met.

j. **Chief Executive Officer:** Leader of the organization tasked with overseeing all operations.

k. **Chief Financial Officer:** Manages and plans the finances of the organization.

l. **Chief Information Officer:** Head strategic planner for the management of information.

m. **Chief Operating Officer:** Manages daily operations and maintains the organizational vision.

n. **Chief Information Security Officer:** Assesses, manages, and implements areas of information security within the organization.

o. **Information Security Champion:** Tasked with communicating and promoting security best practices and awareness.

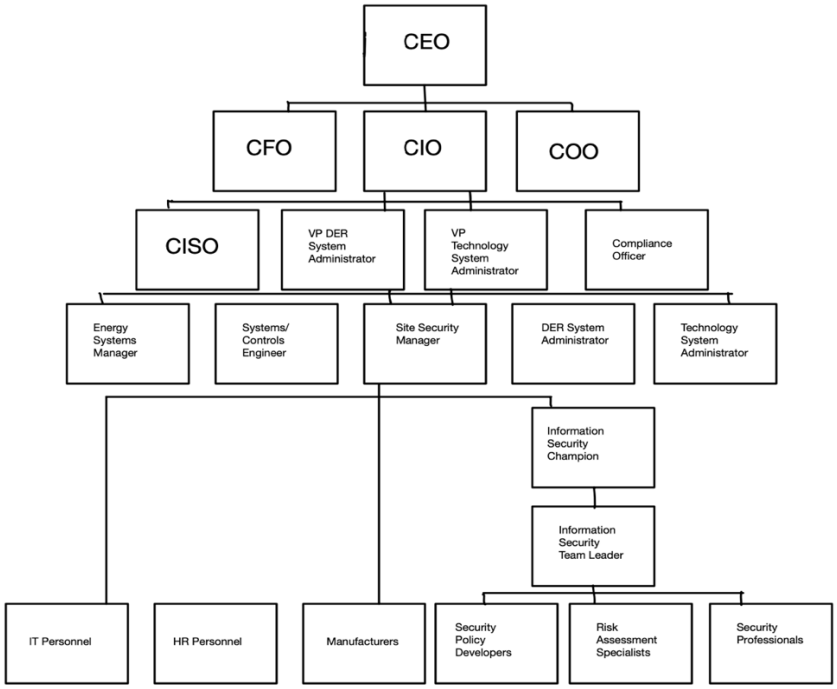
p. **Information Security Team Leader:** Leads security personnel on tasks related to a specific domain.

q. **Security Policy Developers:** Writes security policies to protect the organization and reflect mandated cybersecurity guidelines.

r. **Risk Assessment Specialists:** Tasked with identifying and protecting against organizational risk and proposing the appropriate solutions.

s. **Security Professionals:** Tasked with protecting assets from security risks.

3. **Top-Down Approach Diagram:** This project will be managed using a top-down approach. The roles of each job title needed to carry forth this project and the corresponding top-down diagram that depicts the rank of each SME can be found below:



4. **Technologies:** As this project is only concerned with the development of a sound cybersecurity plan for implementing a distributed generation strategy in Ukraine, it will not utilize any energy infrastructure, DER components, or special cybersecurity technologies (i.e., all physical components and cybersecurity technologies will be implemented, built, configured, set-up, purchased, tested, etc., in a later project stage). However, it should be noted that the energy infrastructure, DER components, and special cybersecurity technologies will be heavily discussed, analyzed, as well as contracted in this development stage. That said, the technologies used specifically for this project are as follows:

    a. **Microsoft Surface Laptop 5:** For company use only and intended for attending Zoom and/or Microsoft Teams calls, answering emails, communicating with stakeholders or coworkers, creating deliverables, researching for work functions, and performing job description tasks.

    b. **Microsoft Teams:** Used for live video calls and for storing company documents and working deliverables in a unified location and/or folder.

c. **Adapt:** Used as the organizational system of record and employee billing.

d. **OneDrive:** Safely stores documents and working deliverables in the cloud and allows employees to work on tasks simultaneously without sending documents back and forth.

e. **Microsoft Office Suite:** Consisting of Word, PowerPoint, and Excel, these platforms are intended to enable the development of documents and deliverables.

5. **Information Assets:** An information asset is any asset that contains valuable information to an organization, as well as the systems that store, transmit, or process an organization's valuable information. The list below contains deliverables that the Ministry of Energy would consider information assets. However, above in the technologies section, Microsoft Teams, Adapt, and OneDrive are also considered information assets since they serve as information storage platforms.

    a. **Risk Matrix Assessment Table (RMAT):** An RMAT is an extensive Excel Matrix deliverable that showcases the cybersecurity policy, relevant control statements, the organization's evidence and artifacts that allows them to satisfy, partially satisfy, or not satisfy the control, the location of the organization's evidence, the organization's disposition for each control, and the level of risk for each control.

    b. **Business Impact Analysis (BIA) deliverable:** A BIA will predict possible consequences that may result from a cybersecurity disruption and will aim to determine methods that would help the organization to recover in each instance. Completing a BIA requires significant evidence gathering, document searching, and many stakeholder interviews.

    c. **External Party Contracts:** External contracts will be drafted when an external party is recruited to assist the Ministry of Energy with a project or with an infrastructure need. To draft an external contract requires several

meetings with the external party to determine the purpose behind the exchange and obligations that each side will be required to meet.

d. **Asset Logs:** Asset logs will list and detail all assets that are used within the Ukrainian energy sector, at the Ministry of Energy in general, and within the Ministry of Energy for this engagement. The asset logs will detail the asset location, any updates, additions, or changes made to the asset, the asset owner, the purpose of the asset, who is authorized to use the asset, and useful documents that help in the asset configuration or risk management process, etc.

e. **Written Policies and Procedures:** This engagement will result in hundreds of detailed policies and procedures. These policies and procedures may depict a risk management strategy, a physical security policy, and (but not limited to) a disaster recovery strategy. Because the purpose of this engagement is to create a resilient energy system for Ukraine by implementing sound cybersecurity planning, a significant amount of time will be spent drafting and finetuning these deliverables.

f. **Password Files:** Because there are thousands of technologies at the Ministry of Energy, of whom is responsible for managing the entire Ukrainian energy infrastructure and all relevant cybersecurity concerns, there is a need to maintain password files so that the appropriate individuals can gain access to the needed technologies. The consultants engaged on this specific project will maintain a password file to gain access to any document drafted or used for this project.

6. **Threats to Information Assets:** A threat will be posed to information assets at the Ministry of Energy when any cybersecurity attack causes the information assets to be deleted or made inaccessible. The following threats are general cybersecurity threats and are the same as the general challenges mentioned above, except they are tied to information assets rather than to DER systems. It

should be noted that at the Ministry of Energy, company computers are the only technologies that an employee can use to access information assets.

a. **Supply chain compromise:** The installation and operational function of hardware and software at the Ministry of Energy are dependent on the advice, communication, and supplies provided by external third-parties and vendors. It is possible that these external parties can be disrupted by a cybersecurity attack, leaving them unable to fulfill their roles for the Ministry of Energy. Since a Ministry of Energy employee can only access information assets via company computers, a supply chain disruption would prohibit employees from doing their work and accessing needed materials.

b. **Botnet:** A botnet attack is when malware takes control of computers' operational functions, leaving an organization vulnerable to not just a single disrupted computer, but a disruption to the organization's entire network of computers. A botnet attack across the Ministry of Energy would make important information assets inaccessible.

c. **Worm:** A worm is likely to start infecting one component of one computer, but then will likely infect the Ministry of Energy's entire networking system, eventually attacking all systems attached to the same network as the initial computer disrupted. This has potential to not only make the Ministry of Energy's information assets inaccessible, but also to disrupt the personal devices of the Ministry of Energy's employees and thus yield a personal information privacy concern.

d. **Ransomware:** Ransomware is when a malicious software blocks access, usually by means of encryption, to the Ministry of Energy's operational software until a requested amount of money is paid. This would make the Ministry of Energy's information assets inaccessible.

e. **DER denial-of-service:** A DoS attack is when malware makes all resources on a machine inaccessible to the legitimate users, which would include the Ministry of Energy's information assets.

7. **Information Security:** The foundation of information security policies are based on the CIA Triad. Though further information can be found in the policies section of this proposal, below is a general description of how the Ukraine Ministry of Energy will strive to satisfy the CIA Triad:

    a. Confidentiality: The MoE will ensure that only authorized users have access to data.

    b. Integrity: The MoE will ensure that any data collected or used is reliable and authentic. Any attempts to change, update, alter, or delete data will be detectable and documented in detail.

    c. Availability; The MoE will take extreme precautions to ensure that data is available to all MoE employees that need information to do their work and whom are authorized to access such data.

Project Goals: The primary goal of this project (from the perspective of the real-world implementation, not the class project goals) is to develop a distributed generation

strategy that will enable Ukraine to form a resilient power system that will 1) help them to win their war against Russia and 2) prevent future attacks relating to cybersecurity and the energy sector. The following are detailed objectives that this project aims to obtain:

1) Develop a strategy that will be approved as well as financially attainable by the Ukrainian government.
2) Develop a strategy that will make Ukraine's energy sector resilient to cybersecurity attacks through modern techniques that will serve as a model to the rest of Europe and the world.
3) Utilize solar energy and photovoltaics as much as possible to reduce reliance on fuel.
4) Develop a distributed generation plan across all cities in Ukraine at the widest distribution capacity possible that Ukraine and modern techniques are able to obtain.
5) Ensure that all DERCF and NIST controls are fully documented and thoroughly reviewed before completing this project.
6) Ensure that the plan to implement the strategy (i.e., purchase, build, configure, install, etc., DER's and generational facilities) is sound and fully complete.
7) Train as many Ukrainian citizens as possible on issues pertaining to cybersecurity and improve cybersecurity awareness country wide.

Project budget and Timeline: This project, which is purely developing a sound distributed generation cybersecurity plan for Ukraine (to be implemented in a later stage) is expected to cost $50 million. This project will be finalized in two (2) years, which is quick given the magnitude of this engagement, as Ukraine is in a state of urgency. This will be achieved by hiring a large workforce, as well as by contracting employees to work 60-hour weeks.

This project will be broken up into the following nonexclusive list of tasks. Deadlines for task completions are to be determined (TBD). The order of completion of these tasks is TBD. We reserve the right to be flexible to account for time and budget constraints, as well as to optimally satisfy ever-changing best practices.

1) Hire and onboard any extra workforce members needed.
2) Conduct an in-depth review of best practices for DER systems.
3) Conduct stakeholder interviews.
4) Draft and review policies and procedures.
5) Conduct Risk Assessments.
6) Understand the budget of implementing this strategy for stage 2 of this project.
7) Create deliverables.

Summary: As a result of the Russia-Ukraine war, it has become imperative that Ukraine improve and modernize its energy sector by implementing sound cybersecurity planning and a distributed generation strategy. Generation is of utmost importance to Ukraine at the moment, as a disruption to generation places an unobtainable reliance on fuel and thus a loss of needed resources to live (i.e., heat, healthcare, clean water, the ability to communicate in emergencies, etc.) for the Ukrainian citizens. By accounting for the specific challenges that are expected within a distributed generation strategy, as well as challenges that we expect to encounter as a result of planning for a country-wide energy sector update, we have taken the first steps in deciding important problems to solve. By developing our own policies created and recommended by DERCF and approved by NIST, we have developed the baseline objectives of which we need to plan for and implement procedures for. Lastly, by listing the roles of the workforce that will be needed to carry out this project, we will be able to hire and employ the appropriate and most qualified subject matter experts in the field.

Citation:

[1] A. Dawes, J. Majkut. (2022). “Responding to Russian Attacks on Ukraine’s Power Sector.” CSIS. (Online Article). https://www.csis.org/analysis/responding-russian-attacks-ukraines-power-sector

[2] U.S. Department of Energy. (2022). “Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid. (Online Article). https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf. p. 10

[3] C. Powell, K. Hauck, A. Sanghvi, et al. (2019). “Guide to the Distributed Energy Resources Cybersecurity Framework.” NREL. (Online Article). https://www.nrel.gov/docs/fy20osti/75044.pdf. p. 1, 17-39.