October 29, 2018

Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors

A Risk Assessment Study of Solar Inverter Technology

Prepared for:

PROTECT OUR POWER

Authors: **Raymond Watts**
Brian Kline

Contributing Author: **Tom Ridge**

RIDGE GLOBAL
1140 CONNECTICUT AVE. NW | SUITE 510 | WASHINGTON, DC 20036 | UNITED STATES
P +1 202-833-2008 | F +1 202-833-2009 | W ridgeglobal.com

October 29, 2018

i. Abstract

Amid the revolutionary changes wrought by the Internet of Things, the dynamic growth of renewable energy technologies, and the increasingly "distributed" nature of the electric grid, it is vital that electrical equipment associated with these developments be subject to increasingly rigorous manufacturing and deployment standards. More importantly, as the nation focuses on strengthening our existing electric grid, we need to be ever vigilant that we not repeat known vulnerabilities, or add new ones, as we enhance, upgrade and modernize the grid to accommodate new energy sources and meet future demand for electric power.

Toward that end, this report explores concerns related to potential threats posed to the U.S. electric grid using inverters to convert direct current (DC) power produced by solar photovoltaic (PV) panels to alternating current (AC) for integration into the grid, and to facilitate the flow of power from the grid back to the photovoltaic array.

The Yale School of Forestry & Environmental Studies (Yale, 2018) reports that the global solar market grew 29 percent in 2017, with nations installing 98.9 gigawatts (GW) of new generation capacity. The United States, second in new solar power installations globally, accounted for 10.7 GW of new installed capacity in 2017. The projected future U.S. growth in solar energy requires rigor in identifying potential threats and mitigating vulnerabilities posed by the continued large-scale integration of photovoltaic electric generation systems so that appropriate risk mitigation measures can be taken to prevent or limit significant damage to the U.S electrical grid and other critical infrastructure. We acknowledge that all software and hardware, including inverters, used to facilitate the transfer of electricity from generation systems to the grid at both the Bulk Electric Systems (BES) and Distribution Grid levels, are vulnerable to threats and pose potential risks. This report, however, specifically focuses on photovoltaic inverters because of their widespread current use and the projected growth of solar energy.

The report utilizes a modified analytical process published by the U.S. Department of Energy, known as the Electricity Subsector Cybersecurity Risk Management Process (DOE, 2012), which was designed to help energy sector risk management organizations develop detailed cybersecurity risk information for affected stakeholders.

The report was prepared for Protect Our Power; an independent, non-partisan, not-for-profit organization established to build consensus among government and industry to strengthen the electric infrastructure against all potential attacks, whether cyber or physical, and to identify the priorities and resources needed for success in a timely manner.

Keywords: solar, inverter, photovoltaic, critical infrastructure, electrical grid, cybersecurity

ii. Executive Summary

Similar to the policymaking community at large, Protect Our Power has two fundamental goals relative to the protection of the U.S. electrical grid:

1) Use technology, ingenuity, and knowledge of evolving best practices to upgrade and improve the existing grid, i.e., make the grid more robust and resilient; and,
2) Ensure that all software, hardware or firmware upgrades, improvements, and additions to the grid do not introduce new vulnerabilities and/or new pathways of a potential attack. Put simply, grid upgrades should not increase the attack surface

The rapid growth of the IoT, a term coined by technology executive Kevin Ashton of the United Kingdom nearly 20 years ago, presents significant challenges in meeting these two goals. The addition of tens of billions of devices interconnected to the Internet, many of which also connect directly to the electric grid and have two-way flows of power, potentially adds billions of new pathways for rogue actors to infiltrate and manipulate the U.S. electricity supply. Because the IoT is vital to the technological and economic growth of modern society, its role in the day-to-day lives of people and enterprises around the globe is unlikely to slow for decades, if ever. This growth trajectory makes it critical that IoT growth does not introduce new vulnerabilities to the electric grid or other critical infrastructure that intersects with the grid.

An increasing number of alternative, de-centralized sources of electric generation are being connected to the grid. These new sources of power generation are important in myriad ways, including: making greater and more efficient use of renewables; reducing carbon emissions; further diversifying the power supply; supporting the growth of microgrids that add resilience to the grid; fostering economic growth; creating jobs; and, conserving water resources.

But with these benefits comes the fact that connecting large numbers of de-centralized energy sources to the grid has the potential to introduce new vulnerabilities. Prime examples of this circumstance can be found in the growth of wind and solar power, both of which use grid-connected inverters to maximize efficiency and control the flow of power to and from the grid. Recent statistics on wind and solar growth provide perspective:

- The U.S. distributed wind market added 1,076 megawatts of installed capacity between 2003 and 2017, or approximately seven percent of U.S. electricity supply, according to the *2017 Distributed Wind Market Report* issued in August 2018 by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy.

- The added capacity came from more than 81,000 wind turbines generating power in all 50 U.S. states and possessions.
- In the first half of 2018, 29 percent of all new electricity generating capacity brought online in the U.S. came from solar photovoltaics (PV). (Perea, 2018)
- Total installed U.S. photovoltaic capacity is expected to more than double during the next five years, according to the most recent *U.S. Solar Market Insight Report* from Wood Mackenzie Power & Renewables and the Solar Energy Industries Association.
- By 2023, more than14 GW of photovoltaic capacity will be installed annually.
- From 2020 to 2050, utility-scale wind capacity is projected to grow by 20 gigawatts annually, and utility-scale solar PV capacity is projected to grow by 127 gigawatts annually, according to the U.S. Energy Information Administration's *Annual Energy Outlook 2018.*

The current and projected growth in solar energy presents a relevant opportunity to examine its impact on the electric grid and grid security. The growth in solar involves numerous large, utility-scale power plants, as well as millions of rooftop and home installations. A photovoltaic system converts sunlight into electricity, and the photovoltaic system uses several components, including solar panel arrays, cables, batteries, meters, and inverters. As such, each individual installation must interface with the grid through one or more inverters, each of which provides multiple avenues of potential exploitation by a threat actor due to the inverter's ability to monitor and control the photovoltaic system.

The specific concern is that a hacker could access thousands of web-connected inverters and significantly alter the flow of power from them to the grid. In a worst-case scenario, a hacker could cause large, sudden spikes or dips in electricity supply, disrupting a local, state or national grid's balance and potentially causing a widespread power outage.

The potential vulnerability of inverters has been highlighted in California during a series of wildfires:

- Examining the impacts of the October 2017 Canyon 2 fire, a February 2018 joint report by the North American Electric Reliability Corporation (NERC) and Western Electricity Coordinating Council (WECC) staff (NERC, 2018) found that, due to transmission system faults, "Approximately 900 MW of solar PV resources were lost as a result of these events, and six solar PV plants accounted for most of the reduction in generation. In general, most of the inverter tripping was caused by sub-cycle transient over-voltages and instantaneous protective action at the inverters to disconnect them from the grid. A significant number of inverters also entered momentary cessation during and following the fault events."
- Similarly, a June 2017 report by NERC examining the impacts of an August 2016 fire found that "four of these (transmission) fault events resulted in the loss of a significant amount of solar photovoltaic generation. The most significant event related to the solar PV generation loss occurred at 11:45 a.m. Pacific and resulted in the loss of nearly 1,200 MW. There were no solar PV facilities de-energized as a direct consequence of the fault event; rather, the facilities ceased output as a response to the fault on the system."

While these events involve inverters acting as they are designed to do and protecting the grid, they also illustrate the vulnerability – a hacker or other agent gaining access to the inverters could cause similar or much larger fluctuations or losses of power.

The security challenges that exist relative to solar energy and inverters are compounded by three realities:

1. Most inverters are produced by foreign or foreign-owned companies, such as Chinese company Huawei, the world's largest manufacturer of inverters.
2. There are no universal standards assuring the integrity of inverters regardless of where they are manufactured.
3. An increasing number of inverters are monitored to enable better control of the power flow to and from the grid, providing added vulnerability to hackers or a foreign aggressor

An added concern is that the U.S. military is actively engaged in developing electric generation systems that allow it to be independent of the grid, if necessary, so that the armed forces are more resistant to an attack on the electricity supply and more resilient in the event that an attack succeeds. A major part of the military's growing energy independence now comes from solar-powered microgrids, creating a potential vulnerability in the integrity of those systems.

The solar inverter issue is one specific example within a larger concern regarding the global supply chain that provides the hardware, software, and firmware necessary to operate and maintain the grid. For many years, electric utilities have had procurement practices in place to govern the purchase of equipment being integrated into the grid, but increasing threats and the growing challenge of enhancing cyber security have created a heightened focus on the reliability and security of the supply chain.

Recognizing that the integrity of individual components affects the overall integrity of the grid, the Federal Energy Regulatory Commission (FERC) in 2016 ordered the electric utility industry's reliability watchdog – NERC – to develop a mandatory, enforceable standard to govern utility supply chain practices. (FERC, 2016)

Responding to FERC's directive, NERC's board of trustees adopted a series of supply chain reliability standards in August 2017. (NERC, 2017). Compliance efforts on the part of utility industry have begun in earnest, as evidenced in part by a webinar conducted by NERC in March 2018 to engage directly with the utility industry. (NERC, 2018). On October 18, 2018, FERC took an important next step by approving these supply chain risk management reliability standards.

The increasingly distributed nature of the grid also necessitates that parties installing electrical equipment become more rigorous about cyber security. As more and more solar photovoltaic panels are installed at the commercial and residential level, the number of megawatts that can affect the integrity of the local distribution system and affect the larger bulk

power system rises concurrently. For example, the WECC, which promotes Bulk Electric System (BES) reliability in all or most of 14 Western states plus Alberta and British Columbia, Canada, and parts of Mexico, noted in a June 2018 report that due to the significant increase in solar electricity production in the region, and the potential for its intermittent nature to affect reliability, the region needs to have a greater reserve margin available to ensure overall system stability and reliability. (WECC, 2018).

This is an issue where the government and the private sector must work together. Utilities and others involved in our owning and operating the assets that make up our national grid cannot go it alone. Cyber security across an increasingly distributed grid is very complex, and the integrity and security of the country's electric grid ultimately is a matter of national and economic security affecting the health and welfare of all Americans.

iii. Analysis

Cyber threats to inverters can take multiple forms. A threat actor can gain physical or remote access to a photovoltaic inverter by "jumping a fence," conducting a brute force password crack, gaining unauthorized access to mobile/cloud application, or manipulating an unsecured Wi-Fi network. Hacking or destroying a single or small number of inverters at a time will not affect the U.S. electric grid. If a threat actor could, however, control inverters at a sufficiently large scale, the actor would be capable of controlling the flow of power from PV systems, and cause peaks or valleys of several gigawatts which would, in turn, cause massive power balancing issues on the grid and lead to possible large-scale power outages.

The impact a single large-scale blackout can be inferred from the Northeast Blackout of 2003, which cost the national economy approximately $6.4 billion from outages lasting one to three days. (Anderson P. & Geckil I., 2003). In a detailed 2015 report by Lloyd's of London and the University of Cambridge, which posited a cyber-attack on a number of electricity generators in the Northeast, researchers estimated the impact on the U.S. economy from the resulting 15-state blackout at $243 billion, with a potential to exceed $1 trillion. (Maynard, Beecroft, 2015). To be successful in causing a large-scale power outage, a threat actor must have access to a substantial number of inverters. Therefore, according to our research (see section 6.7), the most significant risk to PV inverters are likely from nation-state threats operating illicitly in the inverter supply chain.

A threat actor with access to the inverter supply chain allows the manipulation of massive quantities of inverters, the ability to embed malware into the operating system away from the end-consumer and to operate under the veil of a reputable manufacturer. A threat actor could install malware into the inverter's operating system or firmware, or modify the hardware, to allow reliable remote access to the device.

China is the largest inverter manufacturer in the world controlling 47 percent of the market. (ENF, 2018). The Chinese company, Huawei, has been the world-leading PV inverter

manufacturer for the past several years. (Hill, 2016). The *Investigative Report on the U.S National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* prepared for the U.S. House of Representatives Permanent Select Committee on Intelligence, provided details, gathered through interviews with industry experts and current and former Huawei employees, suggesting that Huawei may be violating United States laws. The allegations describe a company that has not followed United States legal obligations or international standards of business behavior. (Rogers, M. & Ruppersberger C.A., 2012). The Congressional investigative report also states there is a growing recognition of vulnerabilities resulting from foreign-sourced telecommunications supply chains used for U.S. national security applications.

The U.S. National Counterintelligence and Security Center (NCSC) has assessed that supply chain infiltration has already threatened the U.S. critical infrastructure sector and could threaten other sectors as well. Meanwhile, new foreign laws and increased risks posed by foreign technology companies due to their ties to host governments may present U.S. companies with previously unforeseen threats. (NCSC, 2018). Due to the concerns of the U.S. intelligence community raised in the Congressional report, Huawei has been banned from bidding on U.S. government contracts since 2014. Huawei has, however, planned the U.S. launch of its *Fusion Home Smart Energy Solution* at the end of summer 2018. (Benny, 2018). The *Fusion Home* system combines smart photovoltaic hardware, including sophisticated inverters that can switch electric grids automatically, with intelligent monitoring software with connected home technologies.

Based on this research, we provide the following key recommendations:

Recommendation 1: Expand the Committee recommendation in *Investigative Report on the U.S National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* to include the electric utility industry supply chain.

- The United States should closely monitor the products penetrating the U.S. photovoltaic market by foreign-owned manufacturers.
- The U.S. government, particularly DoD, should not include foreign manufacturer equipment, including components, in microgrids or other energy installations designed to ensure grid reliability or grid independence.

Recommendation 2: Federal, State, and private sector entities should work together in creating compliance requirements and best practices based on shared information for large photovoltaic systems to include minimum physical and cybersecurity measures and a supply chain security program.

Recommendation 3: The U.S. photovoltaic industry should adopt a supply chain certification program to protect PV components and inverters from manufacturer to installation. A supply chain certification similar to the ISO 28000 standard helps establish, implement, maintain, and improve a security management system within the supply chain. (ISO, 2018).

Recommendation 4: Experts acknowledge the catastrophic economic impact of a successful attack on the U.S. electric market. Regulators at the state and federal levels should immediately encourage and incent utilities to increase investments in cybersecurity.

Recommendation 5: Implement the recommendation in the 2018 DHS report *Assessment of Electricity Disruption Incident Response Capabilities* that DHS work with cross-sector partners to develop cyber situational awareness across interdependencies that will provide cross-sector visibility, in real time, into cybersecurity incidents that occur in critical U.S. infrastructure to protect against cascading impacts. (DHS, 2017).

(This page intentionally blank)

Contents

1. Objective & Scope

This section presents the reason for writing this research paper and the boundaries of its research.

1.1 Objective

To assess threats, vulnerabilities and risks posed by the power industry's supply chain with particular focus on inverters used in solar operations in order to briefly provide risk mitigation options to reduce risk to U.S. critical infrastructure.

1.2 Scope and Limitation

The scope area of the study is limited to the U.S. electrical grid. The study investigated samplings of published (online) documentation of solar energy, the U.S. electrical grid, and PV inverters. The limitations are to PV technology only, specifically PV inverters. The assumption is that inverters introduce risk to the U.S. electrical grid by providing direct pathways that can be exploited by threat actors worldwide. While all inverter technologies, software, and hardware used to facilitate the transfer of electricity from generation systems to the grid are vulnerable to threats and pose potential risks, this report specifically focuses on photovoltaic inverters because of their widespread current use and the projected growth of solar energy.

2. Methodology

This section presents the approach and methodology used to establish the risk to PV inverters.

2.1 Risk Methodology

To evaluate the overall risk of PV inverter vulnerabilities to perceived threats, a data-centric holistic risk management approach was used to provide a balance between threats and vulnerabilities versus currently implemented security countermeasures. The risk management methodology used is a modified version of the Electricity Subsector Cybersecurity Risk Management Process (RMP) developed by the Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology. (NIST) (DOE, 2012). The five-step assessment process provides a framework for evaluating risk to PV inverters as follows:

- Identify the asset (What are the current capabilities of PV inverters, including capabilities and built-in security measures?)
- Identify the threat (Who has the intent and capabilities to target PV inverters, the U.S. electrical grid, or the U.S. as a whole?)
- Identify the vulnerabilities (What inherent capabilities, or lack thereof, allow identified threats to accomplish their intended task of causing harm or misuse of PV inverters?)
- Assess risks (Calculate risks to PV inverters using a standardized set of metrics)
- Determine countermeasures (Recommend steps that can be taken to reduce or mitigate risks to the grid posed by PV inverters)

4. Photovoltaic Inverters

This section presents a broad understanding of the importance of inverters within a PV system and their importance in integrating solar energy into the US electric grid.

3.1 Importance of PV Technology

The massive expansion of solar generation worldwide to date, and its projected growth trajectory to midcentury, reflects technological, political and regulatory advances and is a logical component of any significant strategy to mitigate climate change. In recent years, solar costs have fallen substantially, and installed capacity has multiplied, but today solar energy still accounts for only a small fraction of U.S. and global electricity generation. (Stauffer, 2015).

Owing to a combination of improved technology and manufacturing processes, and increased competition among suppliers, a decline in the cost of two key PV system components — the photovoltaic module and the power inverter — is contributing to rapid growth in U.S. PV deployment (MIT, 2015). By mid-2014, the price for residential inverters in the United States had dropped by approximately 50 percent from typical prices in 2009. (NREL, 2015).
In an extensive, 365-page study on the future of solar energy, MIT concluded: "Solar electricity generation is one of the very few low-carbon energy technologies with the potential to grow to a very large scale." The study projects the development of current solar technologies out to the year 2050, concluding that solar energy has the potential to generate power on a multi-terawatt scale. By contrast, today's largest solar farm has only a 550-megawatt capacity. This projection is a clear illustration of the growth potential of solar energy. (CleanEnergy Authority, 2017).

3.2 PV Inverter Criticality

The inverter is the gateway between the photovoltaic panels and either the grid or a facility's electrical infrastructure, playing a key role in coverting current and voltage, and improving the overall efficieney of the photovoltaic system. Without an inverter, the electricity generated by the system cannot be converted to the proper current and voltage and put to use. Inverters also minimize losses when energy is transferred from solar panels to the grid, or a business, delivering more power and saving money. (Trinity Solar, 2014).

4. Threats

This section presents an overview of the categories of persons, groups, or nation-states that potentially have the capability and intent to target PV inverters. Specific persons, groups, or nation-states may fall into multiple threat categories.

4.1 Ideology

Ideological threat actors want to carry out eco-terrorism, bioterrorism, or any other form of destruction to satisfy a personal system of beliefs or ideals. Eco-terrorism is practiced by groups engaged in "anti-system" violence, e.g., violence against existing political structures. (Elliott, 2002). Bioterrorism includes threats to contaminate water supplies or to destroy or disable energy utilities. Domestic and international terrorists seek to erode the civilian population's confidence in our critical infrastructure and cause economic harm to the country by creating power outages through cyber attacks.

4.2 Monetary

The most likely threat from a monetary perspective would be an actor using inverter monitoring capabilities to gain insider knowledge on the current performance and efficiency of photovoltaic systems at scale. This information could then be used to trade electricity at optimal prices.

Electricity is a commodity that is commonly traded in the futures markets as a contract and made available for purchase or sale within a given time frame. A threat actor with cyber and financial knowledge could use PV inverter technology to defraud the purchase or sale of electric energy. The threat actor with a capability to monitor inverters and system operation would be enough to allow traders to exploit PV system breakdowns. Knowledge of when inverters are fully functional or not working is a critical piece of data since the price of a megawatt-hour can hover close to zero at 3 a.m., and then shoot to $1,500 by 5 p.m. on a hot summer day. (McSwain, 2013). A similar tactic was conducted by California traders using a secret state database that was allowing traders to see every 15 minutes if a given generator was operating, and exploiting the situation when a power plant stopped producing power. This same tactic could be used by traders to exploit PV system breakdowns. In the California case, regulators responded by shutting down the database and lowering price caps. (McSwain, 2013). Threat actors using this approach would be attempting to circumvent the Federal Energy Regulatory Commission's Anti-Manipulation Rule, 18 C.R.F.1c.2.

4.3 Warfare

The *Worldwide Threat Assessment of the US Intelligence Community* report (Coats, 2018) stated that Russia, China, Iran, and North Korea would pose the most significant cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool

of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face apparent repercussions for their cyber operations. In fact, in a warning issued on March 15, 2018, the U.S. Department of Homeland Security and the Federal Bureau of Investigation said that Russian hackers had infiltrated the U.S. electric grid and may well have had the ability to shut down power plants at will. (DHS, March 2018) Similar warnings preceded this one, including one in June 2017 focused on a narrower set of activities aimed at the U.S. nuclear, energy and manufacturing sectors. (DHS, Oct. 2017). DHS has repeatedly warned that the infiltration campaign is ongoing, and hackers are actively pursuing the long-term objective of being able to access and manipulate computer networks inside the electric industry. (DHS, Oct. 2017).

The use of cyber-attacks as a foreign policy tool outside of military conflict has to date been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber-attacks that pose growing threats to the United States and its partners.

5. Vulnerabilities

This section presents an overview of inherent capabilities, manufacturing processes, shipping, and regulations that may allow a threat to cause harm directly to the grid or use photovoltaic inverters in an unintended manner.

5.1 PV Inverter Targeted Capabilities

Inverters are a required component in a complete PV system. However, inverters introduce two new vectors of vulnerabilities that can be targeted by a threat actor: monitoring and control capabilities.

5.1.2 Targeted Capabilities – Monitoring

A PV inverter can be monitored locally or remotely for multiple different parameters. The most common parameters include:

- Array voltage/current/power;
- Grid voltage/current/power;
- Module temperature;
- Ambient temperature;
- Global irradiance/irradiation; and,
- Wind speed.

Local monitoring generally occurs by looking at a display screen on the inverter or connecting through a USB port or RS-232 serial port. Remote inverter monitoring is achieved by analog modem, integrated services digital network (ISDN), Global System for Mobile (GSM) communications, RS-485, powerline connection, or wirelessly through Wi-Fi or Bluetooth.

The ability to monitor remotely and undetected provides a threat actor the opportunity to carry out ideological, warfare, and monetary gain operations as discussed in sections 4, 5, 6, and 7 of this report.

5.1.3 Targeted Capabilities- Control

Inverter manufacturers offer propriety software and systems that support remote monitoring and power management solutions. For example, inverter manufacturer SMA offers a product called "Sunny Portal." With Sunny Portal, PV system operators and installers can access key system data anytime, anywhere. They can also analyze measured values, and visualize and compare power yields, meaning that even minor deviations can be detected quickly. This capability is designed to allow system operators to remedy problems quickly but could also be used by a threat actor to manipulate or control systems or systems components.

Sunny Portal is the largest PV monitoring portal, with more than 250,000 systems registered worldwide, and more than 14 GW of monitored PV power in more than 160 countries. (Brehaut, 2018).

5.2 Physical

Physical vulnerabilities are any weaknesses, intentional or otherwise, that a threat actor can exploit when achieving direct (hands-on) access to the PV inverter.

5.2.1 Physical- Default Passwords

Many PV inverters from significant manufacturers (SMA, Huawei, Fronius) have default passwords for setting up, configuring, or monitoring the inverter preloaded in the inverter. These default passwords, e.g., 0000, 12312312, 12345678, can be quickly found online on a manufacturer's website. All manufacturers recommend that end-users change the password, but the actual responsibility falls to the end-user to do so. The United States Computer Emergency Readiness Team (US-CERT) states threat actors can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet. It is also possible to identify exposed systems using search engines such as Shodan, and it is feasible to scan the entire IPv4 Internet and find every inverter that has a web interface. Attempting to log in with blank, default, and common passwords is a widely used attack technique (US-CERT, 2016), and could be used to access photovoltaic inverters.

5.2.2 Physical- Lack of Physical Tamper Detection

Physical security countermeasures for a photovoltaic power generating site are readily available, including cameras, lighting, alarms, and intrusion detection systems (IDS). Statistics and insurance claims show, however, that PV system thefts are increasing rapidly, at a rate of approximately 16 percent per year. Because not all thefts result in insurance claims, it is likely that this number understates the actual increase. (Smith 2012; Hren & Mehalic, 2012). With specific regard to the security of PV inverters, currently, no inverter comes with preinstalled or pre-packaged tamper detection hardware, e.g., tamper tape, a conductive strip, or software.

5.3 Cyber

Cyber vulnerabilities are any weaknesses, intentional or otherwise that a threat actor can exploit to remotely gain access to the PV inverter through various communications channels, operations or computer systems. Growing exposure to cyber threats led the U.S. Department of Energy to establish the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) followed a hacking campaign in 2017 that targeted several electricity companies.

CESER's main focus is protecting the nation's power grid and other critical infrastructure against cyber-attacks and natural disasters. (Scott, 2018).

5.3.1 Cyber- Wi-Fi Networks

PV inverters on the market today are Wi-Fi enabled so they can easily be connected to a home or business network wirelessly. Scott Moskowitz, research manager at GTM Research, stated that "cybercriminals could potentially hack a residential inverter and cause an outage, or gain access to your Wi-Fi network, in the same way as they might via your smart TV or Amazon Alexa system." From a grid operators' perspective, the risk is that a hacker or threat actor can access utility-scale or distributed PV systems and use them to sabotage the grid. (Deign, 2018).

5.3.2 Cyber- Chip Vulnerabilities

PV inverter manufacturers have admitted that the well-publicized "Spectre" and "Meltdown" chip vulnerabilities are present in many of the chipsets used in their electronic devices, including PV inverters. (Deign, 2018). These vulnerabilities enable non-privileged applications running locally on a machine to access areas of memory generally reserved only for the operating system. The practical impact is that any application running on a system may be able to access ordinarily off-limits data, such as passwords, security keys or other sensitive information stored in the memory of the local machine. (Hale, 2018).

5.3.3 Cyber- Unrestricted Network Access

PV inverters that connect to other equipment offer additional opportunities for threat actors to gain access to the inverter. A threat actor could use another piece of equipment connected to the network - such as a laptop, workstation or smart TV - as the attack vector to gain control of the inverter. Multiple devices connected to the same network mean more opportunities and pathways for a threat actor.

5.3.4 Cyber- Situational Awareness

The "*Assessment of Electricity Disruption Incident Response Capabilities*" report, prepared by the U.S. Department of Energy in response to Presidential Executive Order 13800, highlighted that existing capabilities for assessing potential consequences and impacts from cyber-related disruptions, and for sharing relevant situational awareness in a timely, coordinated manner across sectors, are often unable to provide the detail needed to better inform government executives, regulators, and utilities of potential risks. (DHS, 2017). The DHS report also noted the following vulnerabilities:

- The electricity subsector's primary existing situational awareness capability, the Cybersecurity Risk Information Sharing Program (CRISP), is limited to business

networks of participating firms and therefore covers many, but not all, electricity customers in the U.S.
- No capabilities exist for entities to correlate cyber incident data in real time across multiple sectors.
- There is no streamlined process for developing cyber incident capabilities. (DHS, 2017)

5.3.5 Cyber- Remote Code Execution

A threat actor can use a remote code execution capability in an inverter to execute arbitrary code on the inverter and remotely command and control the inverter from any available Internet connection. Failed exploit attempts may also result in a "denial of service" (DoS) condition, which occurs when legitimate users are unable to access information systems, devices or other network resources due to the actions of a malicious cyber threat actor. A denial-of-service is accomplished by flooding the targeted host or network with traffic until the target cannot respond or crashes, preventing access for legitimate users. DoS attacks can cost an organization or system significant time and money while their resources and services are inaccessible.

5.3.6- Cyber- Patch Management

Inverters, like all software and hardware, require updates and maintenance to add functionality, improve performance or address vulnerabilities. It may, however, be difficult to provide timely software upgrades or patches for inverters because equipment is located in isolated or hard-to-reach locations. As such, the standard patch, test and deploy lifecycle is fundamentally different in the electrical sector, where it can take a year or more to go through qualification of a patch or upgrade. (Ghansah, 2009).

5.4 Supply Chain

The global supply chain through which the U.S. utility industry purchases photovoltaic inverters is largely unregulated and lacks uniform standards. The current supply chain environment creates a wide variety of opportunities for threat actors to install malware at the point of manufacture, or otherwise compromise the integrity and performance of photovoltaic inverters.

Admiral Michael Rogers (USN Ret.) testified before Congress in 2016 and said: "Foreign cyberactors are probing Americans' critical infrastructure networks and in some cases have gained access to those control systems. Trojan horse malware attributed to Russia was detected in industrial control software for a wide range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure." (NSA Resources, 2016).

5.4.1 Supply Chain- Installing Malicious Circuits or Programming

There are numerous reported cases of foreign-owned companies surreptitiously installing malware, viruses, Trojans, and many other bugs to monitor, manipulate, control, or create a backdoor in software and devices. For example, security researchers at Kryptowire discovered malicious software pre-installed on more than 700 million Android smartphones that enabled the tracking of a user's movements and communications. The encrypted data was sent to a Chinese server through a backdoor (Bing, 2016). Similar surveillance or control mechanisms could be installed in inverters by the manufacturer. Possible operations include:

- Install entirely new circuits to support out-of-band communications (GSM, Wi-Fi mesh, encrypted/VPN based IP communications) that operating system-based (OS) monitoring is incapable of catching;
- Install kernel/root level Trojan horse devices into the OS with preconfigured credentials, symmetric or asymmetric keys;
- Add core functions to the OS system to allow attack operations, e.g., bypass standard authentication systems; and,
- Create a means to allow a threat actor to issue orders or call functions without logging in or reporting, making it difficult to spot or catch a threat's actions, or investigate after an incident

5.4.2 Supply Chain- Government or Local Military Controlled/Influenced

ENF Solar has created a directory of 839 PV inverter manufacturers worldwide (ENF, 2018), that ranks the United States third (six percent) in manufacturer ownership, whereas Chinese and Indian PV inverter manufacturers comprise of 47 percent and 17 percent, respectively, of the total market. In 2016, Chinese Manufacturers Huawei and Sun grow led global PV inverter shipment rankings, ahead of SMA, Sineng, and TMEIC (Hill, 2016).

The directors of the CIA, FBI, NSA, and the Director of National Intelligence told the Senate Intelligence Committee they would not advise Americans to use products or services from Huawei. (Salinas, 2018). The US intelligence community has long been wary of Huawei, which was founded by a former engineer in China's People's Liberation Army and described as "effectively an arm of the Chinese government." (Hill, 2016). Due to the concerns of the U.S. intelligence community, Huawei has been banned from bidding on US government contracts since 2014. The clear concern is that foreign companies, whether government/military owned or not, may be influenced to install malicious hardware or software to fulfill a foreign government's ill intentions.

Companies in China, including foreign firms, are required by law to establish a party organization (Martina, 2017). One senior executive at a Beijing meeting with more than a dozen top European countries stated that some companies were under "political pressure" to revise the terms of their joint ventures with state-owned partners to allow the party final say over business

operations and investment decisions. (Martina, 2017). Among the possible vulnerabilities a manufacturer can introduce are:

- Creating backdoors that are preconfigured for remote access, allowing the manufacturer or a third-party entry into the base operating system or other software of a company. This approach could be used when the manufacturer is not in the same country as the threat actor, or when the operation is deemed too sensitive to expose to the manufacturer.
- A government or military entity compromises a manufacturer in another country, gaining access to their standard remote access or monitoring capability and "piggybacks" the remote access or monitoring capability. This approach could be used when the manufacturer is not in the same country as the threat actor, or when the operation is deemed too sensitive to expose to the manufacturer.
- A manufacturer creates an avenue for regular remote access to a device to conduct normal maintenance, patching, or performance monitoring on the hardware but voluntarily provides the remote access credentials to the local government or military.
- A manufacturer knowingly aids their local military or government organization by creating a backdoor for remote access.

This last example of an attack methodology occurred in 2017 when the Indian government revealed a list of apps on both Android and iOS that its intelligence agencies identified as spyware. A total of 42 apps on both smartphone platforms were reportedly sending the user's data back to servers in China, providing the potential to carry out cyber-attacks against Indians. (D'Mello, 2017).

5.4.3 Supply Chain- Interdiction in Transit

Physical components of inverters, or the entire PV inverter device, can be interdicted while in transit from the manufacturer to their destination. A threat actor opens the shipment, installs a remote access capability, reseals the equipment, and inserts the package back into transit to the original destination. This threat tactic could be used when the manufacturer is not in the same country as the threat actor, or when the threat actor is based in the target country or has extensive access in the target country.

- In 2017, threat researchers at Check Point, a mobile software provider, detected a severe infection in 36 Android devices belonging to a large telecommunications company and a multinational technology company. The malware had not been downloaded to the device through use; the malware had arrived preinstalled in the device. It was determined that the malicious apps were not part of the official ROM supplied by the vendor but were added somewhere along the supply chain. (Check Point, 2017)

6. Risk

This section presents a methodology and quantitative analysis of PV inverter risk resulting from threats against PV inverter inherent vulnerabilities.

6.1 Risk Methodology

Risk Assessment is the process of evaluating a security risk based on an analysis of threats and vulnerabilities present in a critical asset. Several quantitative equations may be used to compute risk. All risk formulas involve both subjective and objective judgments. For this research paper we have chosen to use the following Risk Formula:

Threat x Vulnerability = Risk

6.2 Likelihood

As reported in the *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector Analysis Report (*Glenn et al., 2016), no lasting damage to U.S. utilities due to a cyber-attack has been reported publicly, but known cyber-attacks and campaigns targeting U.S. electric utilities have been highly publicized. (DHS, 2017; DHS 2018). This report concludes using the described risk methodology that the likelihood for an attack to cause damage to the electrical grid through the exploitation of PV inverters is considered very high.

6.3 Threat Rating Scale

The threat groupings presented section 4 are here broken down into more specific threat actors. The point scale ranks threats on a scale of 1-5, with 1 being the lowest ordinal and 5 being the highest.

1=	The entity has the necessary knowledge that can be obtained via open source or is not actively openly targeting the U.S. electrical grid
2=	The entity has some technical or scientific knowledge but is minimally targeting the U.S. electrical grid
3=	The entity has some technical or scientific knowledge and is actively targeting the U.S. electrical grid
4=	The entity has advanced technical/training or insider knowledge required and may target the U.S. electrical grid given the opportunity
5=	The entity has advanced technical/training or insider knowledge required and is openly targeting the U.S. electrical grid

6.4 Threat Rating

Area	Threat Rating	Reasoning
1. Nation States (China, Russia, N. Korea, Iran, or proxies)	5	*Individual countries explained in sections 6.4.1 -6.4.4

2. Terrorists	3	Terrorist groups such as ISIS have ambitious attack aims when it comes to cyber. While attempts to "take down" the U.S. power grid have been ineffective to date, pro-terrorist groups represent a highly visible threat, and ISIS has proven to be one of the most significant drivers of hacktivist activity through 2015. These groups do not, however, currently possess the sophisticated tools or skills necessary to execute a cyber-attack resulting in a widespread or significant impact on the power system. (Glenn et al 2016)
3. Hacktivists	2	Ideologically motivated hackers, such as Anonymous, typically attack corporations and government agencies by exposing classified data or bombarding their systems to cause DDoS attacks. The National Security Agency stated that Anonymous might be able to cause a limited power blackout. (Glenn et al 2016)

*The country threat actors listed are provided in the *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* prepared by the Mission Support Center, Idaho Nation Laboratory.

6.4.1 Threat- China

China has been an extremely active, advanced cyber actor for some time – particularly regarding economic espionage against U.S. companies – though they often use blunt force cyber tools (such as network scanners, viruses, and botnets) to access targets. (Glenn et al., 2016) China's multiple intrusions into U.S. ICS/SCADA and smart grid tools may be aimed more at intellectual property theft and gathering intelligence to bolster their infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the U.S. bulk electric system. For example, one of the People's Liberation Army Unit 61398 military personnel charged with stealing U.S. industrial secrets in May 2014 was linked to UglyGorilla, a hacker pseudonym responsible for cyber intrusions of a Northeastern U.S. utility beginning in 2012. (Schmidt and Sanger, 2014) Like Russia, China is unlikely to execute a cyber-attack resulting in widespread damage to the U.S. power grid due to the political consequences such a hostile act would likely entail. It is, however, highly likley that nation-state threat actors will continue to probe energy sector participants' networks and remotely accessible assets to learn more about U.S. critical infrastructure. (Glenn et al., 2016).

6.4.2 Threat- Russia

Russia possesses a strong and well-resourced central cyber command. Past cyber intrusions of U.S. governmental organizations, including the Department of State, Department of Defense, and the White House were attributed to Russian state-sponsored hackers. (Perlroth and Sanger, 2018). In 2007, Russia conducted cyber-attacks on Estonia's critical technology infrastructure, flooding government, financial and media sectors with Distributed Denial of Service (DDoS) attacks and in 2009, Russia and China were reported to have had both made attempts to penetrate the U.S. power grid, using software programs to map U.S. infrastructure and potentially disrupt the system (Glenn et al., 2016).

In late December 2015, in the most widespread cyber-attack on a power system to date, sophisticated actors suspected of working for the Russian government targeted the Ukrainian energy sector using multiple cyber tools, including the malware BlackEnergy, to gain initial, unauthorized access to power company networks. This malware was discovered on Ukrainian networks as early as May 2014. (Glenn et al., 2016). The U.S. Department of Homeland Security reported that three Ukrainian distribution companies experienced coordinated cyber-attacks that were executed within 30 minutes of each other. The attack blacked out 103 cities, affecting 225,000 customers, and required the distribution companies to move to manual operations in response to the attack. (Lee, 2016).

6.4.3 Threat- Iran

Iran uses its cyber program as a tool against political foes and for collecting intelligence and has proven itself a highly motivated, although somewhat less sophisticated, cyber actor as compared to Russia and China. A 2016 U.S. federal indictment attributed a 2013 incident involving multiple remote intrusions of a control computer of the Bowman Dam in Rye, New York, to private computer security teams operating on behalf of Iran's Islamic Revolutionary Guard. (Glenn et al, 2016) From 2012 to 2013, Iran went after U.S. online banking sites, hitting them with DDoS attacks. Overall, Iran and government-sponsored cyber-organizations throughout the country are continuing to expand their ability to conduct a major cyber-attack (Glenn et al, 2016).

6.4.4 Threat- North Korea

Although less sophisticated, the Democratic People's Republic of Korea (DPRK) has demonstrated its intent to conduct cyber-attacks, although in a somewhat unpredictable manner. The prime example of this activity was the 2014 Sony breach which left the Sony network crippled for days, and valuable insider information including previously unreleased films, posted to the Internet. The DPRK primarily focuses its cyber operations on intelligence collection rather than destruction, and these activities are mainly directed at South Korea. At the very least, the DPRK has a demonstrated interest in cyber warfare as a way to confront South Korean and U.S. capabilities (Glenn et al, 2016).

6.5 Vulnerability Rating Scale

The point scale used for the vulnerability is 1-5, with 1 being the lowest ordinal and 5 being the highest.

1=	Adequate mitigation programs, measures, and plans are in place and used 100% of the time in PV inverter manufacturing, installation, maintenance, or monitoring.
2=	Programs, measures, and plans are available but used or effective less than 75% of the time in PV inverter manufacturing, installation, maintenance, or monitoring.
3=	Programs, measures, and plans are available but used or effective less than 50% of the time in PV inverter manufacturing, installation, maintenance, or monitoring.
4=	Programs, measures, and plans are available but used or effective less than 25% of the time in PV inverter manufacturing, installation, maintenance, or monitoring.
5=	There are no programs, measures, and plans available or cannot implement immediately in PV inverter manufacturing, installation, maintenance, or monitoring.

6.6 Vulnerability Rating

Area	Vulnerability Rating	Reasoning
1. Physical Security	2	Reference Sections 5.1 – 5.1.2
2. Cyber Security	3	Reference Sections 5.2 – 5.2.5
3. Supply Chain	5	Reference Sections 5.3 – 5.3.2

6.7 Risk Chart

The risk rating represents the probability of a threat event occurring due to the vulnerability inherent in PV inverters. Numerical risk scores equate to five risk categories as follows:

1-5: Low	6-10: Low/Medium	11-15: Medium	16-20: Medium/High	21- 25: High

Area	Threat		Vulnerability		Risk	Risk Level
1. Nation States Exploiting Supply Chain	5	X	5	=	25	H
2. Nation States Exploiting Cyber Security	5	X	3	=	15	M
3. Terrorists Exploiting Supply Chain	3	X	5	=	15	M
4. Nation States Exploiting Physical Vulnerabilities	5	X	2	=	10	L/M
5. Hacktivists Exploiting Supply Chain	2	X	5	=	10	L/M
6. Terrorists Exploiting Cyber Security	3	X	3	=	9	L/M
7. Terrorists Exploiting Physical Vulnerabilities	3	X	2	=	6	L/M
8. Hacktivists Exploiting Cyber Security	2	X	3	=	6	L/M

9. Hacktivists Exploiting Physical Vulnerabilities	2	X	2	=	4	L

7. Impact

This section presents likely consequences or effects from a threat successfully exploiting one or more PV inverter vulnerabilities on a large scale. Of note, and as stated by the Department of Homeland Security, identifying potential impact with any degree of certainty is extremely difficult because "analyzing the impacts of a significant cyber incident requires detailed knowledge of hundreds of dynamic variables that include the capabilities of the adversary, the behavior of the grid operators, and the real-time conditions of the electricity system. As a result, a comprehensive understanding of how a cyber attack may impact the grid and its customers remains a significant gap for the intelligence community, industry, and subject matter experts" (DHS, 2017).

The challenge of assessing potential impacts is further complicated by a lack of general preparedness. On Sept. 27, 2018, the U.S Department of Energy's Assistant Secretary for Cybersecurity, Karen Evans, testified before the U.S. House Energy and Commerce that U.S. utilities are not adequately protected from cyber attacks from Russia and North Korea that could create massive blackouts (Inside Cybersecurity, 2018).

7.1 Equipment Damage

Damage or theft caused by a threat actor, either by a physical or cyber-attack, could cause a PV inverter or entire photovoltaic system to require repair or become unusable. The financial impact of installing a single PV system is high, and on a larger scale, the economic impact could be catastrophic. A typical single PV system costs $48,000 for a single-family home, and up to $824,000 for an industrial plant (Dovetail, 2018). At the end of 2017, there were approximately 1.6 million residential PV systems in the United States (NREL, 2018). A successful attack against 25 percent of the 1.6 million residental PV systems (400,000 * $48,000) in the United States could have an overall estimated cost of $19.2 billion.

7.2 Electric Grid- Financial

A shutdown of the electric grid would be devastating to U.S. businesses, consumers and the economy. A study by Information Technology Intelligence Consulting (ITIC) revealed that for large enterprises with more than 1,000 employees, the costs associated with a single hour of downtime averages $100,000. (ITIC, 2017). In verticals such as banking, media, manufacturing, or transportation, that cost rises to $5,000,000 for a one-hour power outage. (ITIC, 2017). The impact a single large-scale blackout can be inferred from the Northeast Blackout of 2003, which cost the national economy approximately $6.4 billion from outages lasting one to three days. (Anderson P. & Geckil I., 2003).

In an analysis entitled *Business Blackout: The insurance implications of cyber attack on the US power grid,* Lloyd's of London and the University of Cambridge Center for Risk Studies estimate that if an attack temporarily destabilizes the regional grid in the northeastern United States and causes a sustained outage, the economic impacts include direct damage to assets and

infrastructure, a decline in sales revenue to electricity supply companies, a loss of sales revenue to business and general disruption to the supply chain. The total impact to the U.S. economy is estimated at $243 billion, rising to more than $1 trillion in the most extreme version of the scenario. The Lloyd's report also notes that while the scenario described in the report involves sophisticated attackers who can penetrate security as a result of detailed planning, technical skill, and imagination, "A relatively small team is able to achieve widespread impact."

7.3 Electric Grid- Warfare

Unlike natural disasters that harm the electric grid, cyber incidents generally occur without warning. The lack of time to prepare or stand-up a response team has cascading effects throughout the United State, including the military. The DHS report *Assessment of Electricity Disruption Incident Response Capabilities* (DHS, 2017) states, "Across the United States, the Department of Defense (DoD) relies on the electric grid to support military operations at home and abroad. As DoD pursues increasingly advanced capabilities, such as remotely piloted aircraft and precision-guided munitions, its ability to execute critical missions increasingly depends upon a vast and complex network of ground-based communications networks, radars, data centers, and command and control nodes that rely on electricity to operate.

Approximately 85 percent of the energy infrastructure that DoD depends upon is commercially owned, and 99 percent of the electricity consumption of DoD installations is drawn from infrastructure outside these installations." The Department of Defense in their 2015 Annual Energy Management Report noted that "DoD recognizes that such events could result in power outages affecting critical DoD missions involving power projection, defense of the homeland, or operations conducted at installations in the U.S. directly supporting warfighting missions overseas." (Department of Defense, 2016)

8. Conclusion and Recommendations

This research was conducted to assess threats, vulnerabilities, and risks posed by photovoltaic technologies, and in particular photovoltaic inverters, to the U.S. electrical grid and briefly provide risk mitigation options to reduce risks to U.S. critical infrastructure.

Identified threats to the grid from PV inverters can be categorized into three groups: ideology, monetary, and warfare.

PV inverters were observed to be vulnerable to physical, cyber, and supply chain attacks. The lack of regulation and standards is a significant contributing factor in exposing PV inverters to additional vulnerabilities, discussed in section 5 of this report.

8.1. Recommendations

Based on this research, this team of researchers provides the following recommendations:

Recommendation 1: Expand the Committee recommendation in *Investigative Report on the U.S National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* to include the electric utility industry supply chain.

- The United States should closely monitor the products penetrating the U.S. photovoltaic market by foreign-owned manufacturers.
- The U.S. government, particularly DoD, should not include foreign manufacturer equipment, including components, in microgrids or other energy installations designed to ensure grid reliability or grid independence.

Recommendation 2: Federal, State, and private sector entities should work together in creating compliance requirements based on shared information for large photovoltaic systems to include minimum physical and cybersecurity measures and a supply chain security program.

Recommendation 3: The U.S. photovoltaic industry should adopt a supply chain certification to protect PV components and inverters from manufacturer to installation. A supply chain certification similar to the ISO 28000 standard helps establish, implement, maintain, and improve a security management system within the supply chain. (ISO, 2018).

Recommendation 4: Experts acknowledge the catastrophic economic impact of a successful attack on the U.S. electric market. Regulators at the state and federal levels should immediately encourage and incent utilities to increase investments in cybersecurity.

Recommendation 5: Implement the recommendation in the 2018 DHS report *Assessment of Electricity Disruption Incident Response Capabilities* that DHS works with cross-sector partners to develop cyber situational awareness across interdependencies that will provide cross-sector

visibility, in real time, into cybersecurity incidents that occur in critical U.S. infrastructure to protect against cascading impacts. (DHS, 2017).

Recommendation 6: US-CERT recommends the following risk mitigation solutions to default passwords located online:

- Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the internet. Use a sufficiently strong and unique password (US-Cert, 2016).
- Vendors can design systems that use unique default passwords. Passwords based on an inherent characteristic of the system, like a MAC address, or physically printing the password on the system (US-Cert, 2016).
- Vendors can design systems to require password changes the first time after entering a default password (US-Cert, 2016).

Recommendation 7: Block external access at the network boundary, unless required. Filter access to the PV inverter at the network boundary using a default deny on the firewall.

Recommendation 8: Install an intrusion detection system (IDS) on networks with PV inverters connected to monitor network traffic for malicious activity.

Recommendation 9: Passively monitor equipment for actor command and control

Recommendation 10: Inverter shipments should be randomly inspected (including x-ray microscope) to detect circuit modification, or new circuits not included on design)

Recommendation 11: Tamper evident protections should be placed on inverters from factory to installation location. Additional tamper evident devices (e.g., tamper tape, software, and hardware) should be used after installation.

Recommendation 12: The DHS report *Assessment of Electricity Disruption Incident Response Capabilities* recommends DOE should develop a national laboratory testing program for examining grid components to assess cybersecurity supply chain posture and analyze cyber malware impacts to components in a simulated environment (DHS, 2017).

9. References

1 Anderson, P. & Gecgkil I. (2003). *Northeast Blackout Likely to Reduce US Earning by $6.4 Billion.* Retrieved from: http://www.andersoneconomicgroup.com/Portals/0/upload/Doc544.pdf

3 Benny, J (2018, August 21). *U.S. tariffs cast a cloud over Huawei's solar electronics launch.* Retrieved from: https://www.reuters.com/article/us-huawei-tech-solar-electronics/u-s-tariffs-cast-a-cloud-over-huaweis-solar-electronics-launch-idUSKCN1L609Y

4 Bing, C. (2016, November 15). *Chinese-authored spyware found on more than 700 million Android phones.* Retrieved from: https://www.cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/

5 Brehaut, Cedric (2014, May). *Global PV Monitoring: Technologies, Markets and Leading Players, 2014–2018*. Retrieved from: https://www.greentechmedia.com/research/report/global-pv-monitoring-technologies-markets-and-leading-players-2014-2018#gs.hXMsIII

6 Check Point (2017, March 13). *Preinstalled Malware Targeting Mobile Users.* Retrieved from: https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

7 CleanEnergy Authority (2017, January 23). The Future of Solar Energy in the US – What to Expect? Retrieved from: https://www.cleanenergyauthority.com/blog/the-future-of-solar-energy-01232017

8 Coats, Daniel R. (2018, February). *Worldwide Threat Assessment of the US Intelligence Community.* Retrieved from: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

9 D'Mello, Gwyn (2017, December 1). *The Government Has Named 42 Apps "Chinese Spyware," Including Big Names Like TrueCaller.* Retrieved from: https://www.indiatimes.com/technology/news/the-government-has-named-42-apps-chinese-spyware-including-big-names-like-truecaller-334785.html

10 Deign, Jason (2018, May 23). *Inspection Firm Hacks Inverters Within Minutes, Casting Doubt on Security.* Retrieved from: https://www.greentechmedia.com/articles/read/tuv-hack-inverter-security#gs.7HuVSvU

11 Department of Defense (2016, June). *Department of Defense Annual Energy Management Report Fiscal Year 2015.* Retrieved from: https://www.acq.osd.mil/eie/downloads/ie/fy%202015%20aemr.pdf

12 Department of Energy (2012, May). *Electricity Subsector Cybersecurity Risk Management Process.* Retrieved from: https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

13 Department of Energy (2015, January). *Energy Sector Cybersecurity Framework Implementation Guidance.* Retrieved from: https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

14 Department of Homeland Security (2017, October) *Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.* Retrieved from: https://www.us-cert.gov/ncas/alerts/2017

15 Department of Homeland Security (2018, March). *Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* Retrieved from: https://www.us-cert.gov/ncas/alerts/2018

16 Department of Homeland Security (2017, August 8). *Section 2(E): Assessment of Electricity Disruption Incident Response Capabilities.* Retrieved from: https://www.dhs.gov/publication/section-2e-assessment-electricity-disruption-incident-response-capabilities

17 Dovetail (2018, August 23). *Pricing for Solar Photovoltaic (PV) Systems.* Retrieved from: http://www.dovetailsolar.com/Solar-Electric/Pricing-for-Solar-Electric-Systems.aspx

18 Edison Electric Institute (2018, February). *Delivering America's Energy Future, Electric Power Industry Outlook, The Edison Electric Institute's 2018 Wall Street Briefing Presentation.* Retrieved from: http://www.eei.org/issuesandpolicy/finance/wsb/Documents/EEI_WSB_Presentation.pdf

19 Edison Electric Institute. (2018, February). *Delivering America's Energy Future, Electric Power Industry Outlook, The Edison Electric Institute's 2018 Wall Street Briefing Remarks.* Retrieved from: http://www.eei.org/issuesandpolicy/finance/wsb/Documents/EEI_WSB_Remarks.pdf

20 Elliott, L. (2002, May 12). *Ecoterrorism.* Retrieved from: https://www.britannica.com/topic/ecoterrorism

21 ENF (2018, August 22). *Solar Inverter Manufacturers*. Retrieved from: https://www.enfsolar.com/directory/component/inverter

22 FBI (2011. June 27). *Intelligence Bulletin, "Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware"*

23 FERC. (2016, July 21). *Revised Critical Infrastructure Protection Reliability Standards.* Retrieved from: https://ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf?csrt=6849784787400089049

24 Ferris, Robert (2017, February 15). *US solar installations nearly doubled in 2016, and broke some records.* Retrieved from: https://www.cnbc.com/2017/02/14/us-solar-installations-nearly-doubled-in-2016-and-broke-some-records.html

25 Geiger, Julianne (2016, August 15*). The Power Grid Is a Mess, and It's Costing Us Billions.* Retrieved from: http://www.thefiscaltimes.com/2016/08/15/US-Power-Grid-Mess-and-Its-Costing-Us-Billions

26 Ghansah, Isaac, (2009). *Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks California Energy Commission, PIER Energy-Related Environmental Research Program.* CEC-500-2012-047. Retrieved from: http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf

27 Glenn, C., Sterbentz, D., Wright, A (2016, December). *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.* Retrieved from: https://www.osti.gov/biblio/1337873-cyber-threat-vulnerability-analysis-electric-sector

28 Hale, Samuel (2018, January 8). *IoT perspective on critical security flaw identified in CPUs.* Retrieved from: https://www.machnation.com/2018/01/04/iot-perspective-critical-security-flaw-identified-intel-cpus/

29 Hill, Joshua S. (2016, December 9). *Top 10 Solar PV Inverter Manufacturers Account for 80% of Global Shipments.* Retrieved from: https://cleantechnica.com/2016/12/09/top-10-solar-pv-inverter-manufacturers-account-80/

30 Hren, R. & Mehalic, B. (2012). Security and Theft Prevention. *SolarPro*, 5.6.

31 Inside Cybersecurity. (2018). *DOE cyber office director Evans says utilities need more protection against cyber attacks.* Retrieved from: https://insidecybersecurity.com/daily-news/doe-cyber-office-director-evans-says-utilities-need-more-protection-against-cyber-attacks

32 International Organization for Standardization (2018, August 23). *ISO 28000: 2007.* Retrieved from: https://www.iso.org/standard/44641.html

33 ITIC (2017, May 18). *Hourly Downtime Tops $300K for 81% of Firms; 33% of Enterprises Say Downtime Costs > $1M.* Retrieved from: http://itic-corp.com/blog/2017/05/hourly-downtime-tops-300k-for-81-of-firms-33-of-enterprises-say-downtime-costs-1m/

34 Jean, J., P.R. Brown, R.L. Jaffe, T. Buonassisi, and V. Bulovic (2015). *Pathways for Solar Photovoltaics.* Retrieved from: http://dx.doi.org/10.1039/C4EE04073B

35 Lee, R, Assante, M, & Conway T. (2016, March 18). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Retrieved from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

36 Lenardic, D. (2015, December) *PVResources*. Retrieved from: http://www.pvresources.com/

37 Martina, Michael. (2017, August 24). *Exclusive: In China, the Party's push for influence inside foreign firms stirs fears.* Retrieved from: https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU

38 Massachusetts Institute of Technology (2015). *The Future of Solar Energy.* Retrieved from: http://energy.mit.edu/wp-content/uploads/2015/05/MITEI-The-Future-of-Solar-Energy.pdf

39 Maynard, Trevor & Beecroft, Nick (2015, May). *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid. Lloyd's of London and University of Cambridge Centre for Risk Studies.* Retrieved from: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

40 McSwain, Dan (2013, August 3). *Record fines expose power market flaws*. Retrieved from: http://www.sandiegouniontribune.com/sdut-record-fines-expose-power-market-flaws-2013aug03-story.html

41 National Renewable Energy Laboratory (2014). *U.S. Residential Photovoltaic (PV) System Prices, Q4 2013 Benchmarks: Cash Purchase, Fair Market Value and Prepaid Lease Transaction Prices, Technical Report NREL/TP-6A20-62671.* Retrieved from: http://www.nrel.gov/docs/fy15osti/62671.pdf

42 National Renewable Energy Laboratory (2018, May). *Q4 2017/Q1 2018 Solar Industry Update*. Retrieved from: https://www.nrel.gov/docs/fy18osti/71493.pdf

43 NCSC. (2018). *Foreign Economic Espionage in Cyberspace.* Retrieved from: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

44 NERC and WECC. (2018, February). *900 MW Fault Induced Solar Photovoltaic Resource Interruption Disturbance Report*. Retrieved from: https://www.nerc.com/pa/rrm/ea/Pages/Major-Event-Reports.aspx

45 NERC. (2017, August 10). *Proposed Additional Resolutions for Agenda Item 9.a: Cyber Security- Supply Chain Risk Management – CIP-005-6, CIP-010-3 and CIP-013-1.* Retrieved from: https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf#search=CIP%20supply%20chain%20standard

46 NERC. (2018, March 18). *Supply Chain Update.* Retrieved from: https://www.nerc.com/pa/comp/Supply%20Chain%20Webinars%20DL/Supply%20Chain%20Webinar.pdf

47 NSA Resources (2016, May). *Hearing of the House (Select) Intelligence Committee Subject: Cybersecurity Threats: The Way Forward.* Retrieved from: https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml

48 Perea, A., et al. (2018, September). *Solar Market Insight Report 2018 Q3.* Retrieved from: https://www.seia.org/research-resources/solar-market-insight-report-2018-q3

49 Perlroth N. & Sanger D. (2018, March 15). *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*. Retrieved from: https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

50 Rogers, M. & Ruppersberger C.A. (2012). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.* Retrieved from: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

51 Salinas, Sara. (2018, February 13). *Six top US intelligence chiefs caution against buying Huawei phones.* Retrieved from: https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html

52 Schmidt M. & Sanger D. (2014, May 19). *5 in China Army Face U.S. Charges of Cyberattacks.* Retrieved from: https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

53 Scott, Michael (2018, March 7). *Energy Firms Are Worried About Cyber Attacks, But Don't Really Know What To Do.* Retrieved from: https://www.forbes.com/sites/mikescott/2018/03/07/energy-industry-worried-about-cyber-attacks-but-doesnt-really-know-what-to-do/#7bac06eb68bb

54 Solar Edge (2018). *SolarEdge Commercial Offering.* Retrieved from: https://www.solaredge.com/sites/default/files/commercial-catalogue-na.pdf

55 SolarMarket (2018). *Top 5 Solar Inverters.* Retrieved from: https://www.solarmarket.com.au/tips/top-5-solar-inverters/

56 St. John, Jeff (2013). Report: US Smart Grid Cybersecurity Spending to Reach $7.25B by 2020. Retrieved from: https://www.greentechmedia.com/articles/read/report-u-s-smart-grid-cybersecurity-spending-to-reach-7-25b-by-2020#gs.F4==2VE

57 Stauffer, N. (2015, December 14). *The Future of Solar Energy: A summary and recommendations for policymakers.* Retrieved from: http://energy.mit.edu/news/the-future-of-solar-energy-a-summary-and-recommendations-for-policymakers/

58 Trinity Solar Team (2014, October 2014). *What is a solar inverter and why is it important?* Retrieved from: https://www.trinity-solar.com/blog/what-is-a-solar-inverter-and-why-is-it-important/

58 US-CERT (2016, October 7). *Alert (TA13-175A) Risks of Default Passwords on the Internet.* Retrieved from: https://www.us-cert.gov/ncas/alerts/TA13-175A

59 Wood, McKenzie. (2018, June). *Western Interconnection Gas- Electric Gas Study.* Retrieved from: https://www.rtoinsider.com/wp-content/uploads/WECC_Gas-Electric_BES_Study_Public-Report-FINAL-11.pdf

60 Yale Environment360 (2018, March 19). *The World Added Nearly 30 Percent More Solar Energy Capacity in 2017.* Retrieved from: https://e360.yale.edu/digest/the-world-added-nearly-30-percent-more-solar-energy-capacity-in-2017