CONSIDERATIONS FOR **RETROFITTING EXISTING SOLAR WITH EMERGING TECHNOLOGIES [RESET]**

DECEMBER 2021

Prepared for

U.S. Department of Defense, Environmental Security Technology Certification Program

Prepared by

Converge Strategies, LLC

CONVERGE STRATEGIES

ABOUT DEPARTMENT OF DEFENSE, ENVIRONMENTAL SECURITY TECHNOLOGY CERTIFICATION PROGRAM

ESTCP is DoD's environmental technology demonstration and validation program. The Program was established in 1995 to promote the transfer of innovative technologies that have successfully established proof of concept to field or production use. ESTCP demonstrations collect cost and performance data to overcome the barriers to employ an innovative technology because of concerns regarding technical or programmatic risk, the so-called "Valley of Death."

To learn more about ESTCP, please visit: www.serdp-estcp.org.

ABOUT CONVERGE STRATEGIES, LLC

Converge Strategies, LLC (CSL) is a consulting company focused on the intersection of clean energy, resilience, and national security. CSL works with civilian and military partners to develop new approaches to energy resilience policy and planning in the face of rapidly evolving threats, vulnerable infrastructure, and determined adversaries.

To learn more about CSL, please visit: www.convergestrategies.com.

ACKNOWLEDGMENTS

The authors of this paper are Alex Pina, Jack Graul, Wilson Rickerson, and Meredith Pringle from Converge Strategies, LLC, Robert Kwartin from KPS LLC, and Taite McDonald from Holland & Knight. The paper benefited from review by Michael Wu (CSL), Justin Welch (Idaho National Laboratory), Kurt Myers (Idaho National Laboratory), and Pouyan Farzanehkari (Stem). The team would like to thank Tim Tetreault and Lucas Tufano from ESTCP, and the entire ESTCP technical committee for their guidance during this project.

The authors would like to thank the following individuals for their insights and expertise:

David Altman, Raytheon Technologies
Matthew Backes, MIT Lincoln Laboratory
Greg Baron, CALIBRE Systems Inc.
Shawn Bennett, U.S. Air Force Office of Energy Assurance
Zoe Berkery, CleanCapital
Mike Chipley, The PMC Group LLC
Graham Coates, Holland & Knight
Bob Collie, Cadence Energy
Tony Colonese, Ameresco

John Conger, Conger Strategies & Solutions
Chris Conroy, PowerSecure, Inc.
Joe Cooley, MIT Lincoln Laboratory
Lynn Costantini, National Association of Regulatory Utility Commissioners
Peter Flynn, Bostonia Partners
Mark Fowler, Ameresco
Douglas Gagne, National Renewable Energy Laboratory
Nathan Getty, Booz Allen Hamilton
Tom Hattery, Oak Ridge National Laboratory
Col. Richard Houghton (ret.), City Light & Power
Robert Johnson, Hannon Armstrong
Greg Kaplan, Ameresco
Bayram Kurbanov, U.S. Air Force
Christopher Lawson, Lawrence Livermore National Laboratory
Matt McCann, AECOM
Richard Morris, U.S. Air Force
Charisa Powell, National Renewable Energy Laboratory
Ted O'Shea, ABM Industries
Mike Osborne, Sussex Rural Electric Cooperative
Jon Powers, CleanCapital
Jim Reilly, National Renewable Energy Laboratory
Tami Reynolds, National Renewable Energy Laboratory
Peter Rood, Glidepath Power Solutions
Chandra Shah, National Renewable Energy Laboratory
Aravind Sri, Stem
Emma Stewart, National Rural Electric Cooperative Association
Steven Vickery, Naval Facilities Engineering Systems Command
Joe Walsh, Centrica
Mark “Dusty” Wheeler, ABM Industries

TABLE OF CONTENTS

INTRODUCTION

The Department of Defense (DoD) maintains a globally networked force responsible for missions around the world. Many of these missions rely on military installations within the United States. U.S. military installations are almost entirely reliant on the commercial electricity grid (GAO, 2020a). Cyber attacks, aging infrastructure, and extreme weather events exacerbated by climate change are causing more frequent and severe power interruptions, which threaten the success of critical military missions (Stockton & Paczkowski, 2019).

DoD has acquired a large fleet of power plants located on, or nearby, its military installations during the past decade. These power plants include more than 2,000 renewable energy projects that generated 3,700 GWh in 2020 in response to Congressional legislation and Executive Orders. DoD has installed more than 1,200 solar photovoltaic (PV) systems across the country, ranging in size from a few kilowatts to over 100 megawatts. Examples of the locations and sizes of some of these systems can be seen in Figure 1. Solar systems account for nearly 40% of DoD's renewable energy generation portfolio (ASD(S), 2021).

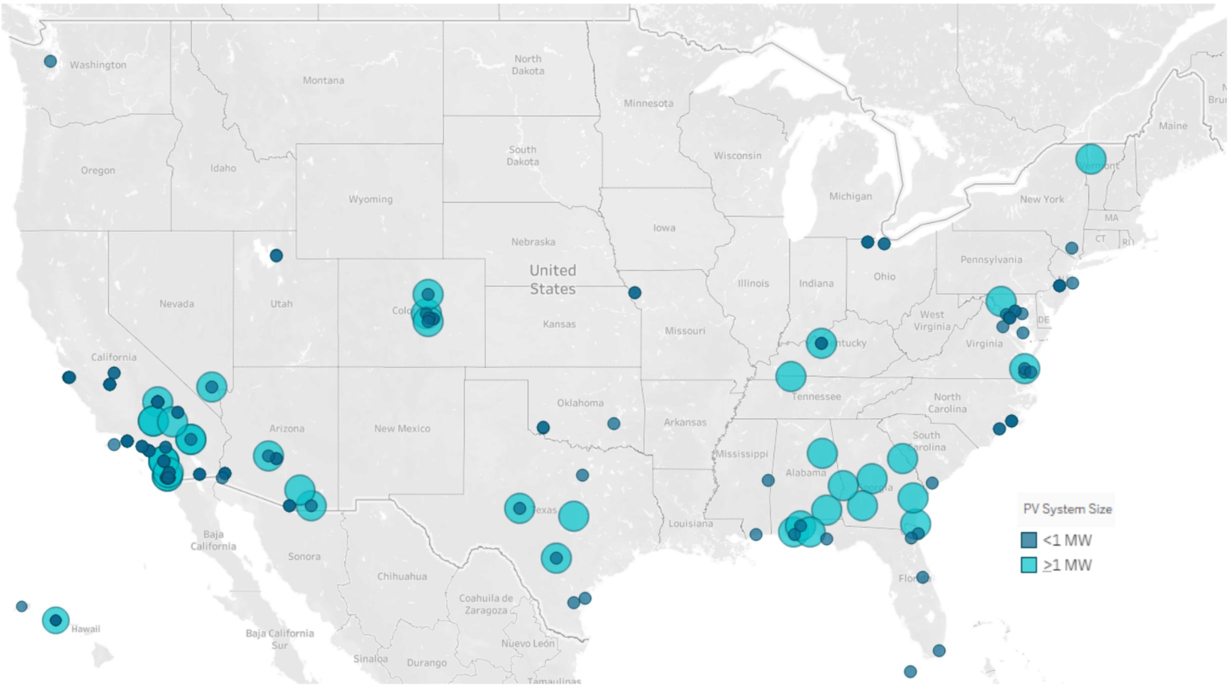

Figure 1: DoD Solar PV Systems Located in the United States, 2009-2021[1]

[1] Converge Strategies research adapted from multiple sources, including Annual Energy Management and Resilience Reports and the DoD Renewable Energy Project Viewer (GAO, 2010; Prehoda et al., 2017; ASD(S), 2020; USACE, 2021).

There are notable examples of solar PV systems that have been configured to provide resilience as part of microgrids. These include, for example, 124 kW of solar PV installed at Kirtland Air Force Base, a 4.5 MW PV system at Naval Construction Battalion Center Gulfport in Mississippi, and a 30 MW PV system at Pacific Missile Range Facility Barking Sands in Hawaii (Crowell, 2020; Rickerson et al., 2018; Rickerson et al., 2021). DoD continues to rely overwhelmingly on backup diesel generators to provide energy resilience, however, and "much of the existing deployed solar PV on DoD installations is installed without islanding capability, preventing use as a true resilience solution" (ASD(S), 2020a). DoD's fleet of existing renewable energy plants represents a significant, but largely untapped, energy resilience resource. DoD - and the federal government more broadly - lacks a process for assessing whether and how energy resilience capability can be added to existing renewable energy projects.

PURPOSE

The Retrofitting Existing Solar with Emerging Technologies (RESET) project explores how DoD can utilize its existing renewable energy assets to support its ambitious energy resilience goals. The project specifically investigates the financial, contractual, engineering, and cyber considerations related to energy resilience retrofits. This report summarizes the key questions that project proponents could ask when evaluating solar PV sites for resilience retrofit feasibility. The questions contained in this report are intended to support initial site screening by energy personnel at installations, as well as by staff within the DoD energy program offices, engineering centers, and acquisition agencies. Similar questions could also be useful to private sector project developers or other energy project proponents. The RESET project team will apply the framework contained within this report to a military installation in order to demonstrate the methodology.

SCOPE

This report focuses on the following opportunities:

- **Retrofit vs. new build.** Military installations may be able to build new projects to accomplish resilience objectives - or repower existing sites - more cost effectively than retrofitting legacy assets with new capabilities. A comparative economic analysis of new build vs. retrofit options should be completed at the outset of a project. This report focuses on retrofitting existing generation assets with resilience capabilities.
- **Generation technologies.** The RESET project focuses primarily on solar PV systems. Solar PV systems are the most prevalent type of renewable energy generation within DoD in terms of the number of systems and geographic distribution. DoD has installed many types of renewable energy on its bases (e.g., biomass, geothermal, landfill gas, and wind

energy), and many of the findings from this report are relevant to other types of renewable energy.

- **Deal structure.** This report focuses primarily on systems that are owned by a third party and financed by private sector capital providers. Systems that are owned, operated, and paid for by DoD may be good candidates for resilience retrofits, but they are typically less complicated and do not face the same range of issues described in this report. Third-party ownership affects not just financial and contracting considerations (Sections 2 and 3), but engineering as well (Section 4).
- **System size.** The report focuses on systems larger than 1 MW. Smaller renewable energy systems can be used to support critical buildings, circuits, and loads, but they tend to be owned and operated by DoD and face fewer of the issues described in this report.
- **Existing assets.** This report is not intended as a design guide for energy resilience projects. There are many existing guides that focus on the technical, economic, and financial considerations of developing new alternative energy projects for military (Craig et al, 2011; OEI, 2014) and civilian applications (IFC, 2015; ACES, 2019). This report acknowledges that new energy generation and storage assets may be required to successfully complete energy resilience retrofits, but does not seek to duplicate existing publications. This report focuses primarily on upgrades to existing assets, while referencing guidance for new project development where appropriate.
- **Resilience capabilities.** Resilience capabilities refer to the ability of energy generation to start up when the power goes out, and to supply electricity to specific loads independent of the electricity grid. Many renewable energy systems cannot perform these functions on their own without additional equipment. As used in this report, "resilience retrofits" include the technologies required to add resilience capabilities to existing renewables. The retrofits may include, for example, upgrades to communications networks, system controls, existing generation, and the distribution system (e.g., network protections and line extensions).

METHODOLOGY

This report is not intended as a generic or comprehensive overview of all considerations related to retrofitting solar PV for resilience. The RESET project focuses specifically on energy resilience retrofits within the DoD context. The project team conducted an extensive literature review on topics related to energy resilience policy and practice within DoD, energy storage and microgrid technologies and market trends, and on financial, contractual, engineering, and cybersecurity considerations related to energy resilience. This report is structured to reflect the direct experience and input of DoD energy resilience practitioners, and of entities that develop and finance DoD energy projects. As a result, this report focuses on project development and business models that have been common within DoD, based on experience from the field, rather than the full range of models identified in the literature. The primary sources for this report include:

- **Direct project experience.** The RESET project team has conducted site assessments, mission thread analyses, tabletop and black start exercises, feasibility analyses, and/or investment due diligence related to energy resilience projects at dozens of military installations across the U.S.
- **Experience from the ESTCP Military Energy Resilience Catalyst (MERC) project.** MERC is a multi-year project to support energy resilience projects across DoD by identifying and disseminating standard, replicable practices. MERC has directly engaged 55 DoD installations to address energy resilience project barriers and opportunities. MERC is managed jointly by RESET project team members: Converge Strategies, LLC and Idaho National Laboratory.
- **Expert interviews.** The RESET project team conducted interviews with more than 40 subject matter experts - ranging from project developers, financiers, and energy service companies to utilities, national laboratories, and DoD officials - in order to inform and validate the structure and focus of the report.

REPORT STRUCTURE

This report provides an overview of the financial, contractual, engineering and cybersecurity considerations related to retrofitting renewable energy systems with resilience capabilities. The report is intended as a guide for screening the resilience retrofit potential of DoD renewable energy projects. Each section begins with questions to help project proponents assess retrofit feasibility. The report is structured as follows:

- **Section 1** provides background information about DoD renewable energy and energy resilience policies, as well as DoD organizational structure that supports installation energy resilience.
- **Section 2** addresses financing considerations that underpin RESET project viability from the perspective of third party project developers and investors where bankability is the bottom line.
- **Section 3** addresses common contracting and legal pathways used throughout the DoD enterprise for energy resilience projects.
- **Section 4** addresses engineering and technical considerations such as interconnection, siting, data collection, and battery technology selection.
- **Section 5** addresses cybersecurity considerations, including the various frameworks that govern connectivity with the DoD network.

1.0 DOD ENERGY POLICY AND ORGANIZATIONAL ROLES

POLICY QUESTIONS	**POLICY** TAKEAWAYS
Does the project align with DoD energy policy?	DoD is directed through federal Executive Orders, policies, and various legislative initiatives to meet renewable energy targets and to ensure energy resilience. Configuring renewable energy systems to provide energy resilience is consistent with, and specifically encouraged by, DoD energy policy.

DoD acquired much of its solar PV fleet in response to goals, policies, and legislative direction requiring federal agencies to buy renewable energy. More recently, energy resilience has emerged as the central tenet of DoD energy policy, even as the renewable energy mandates remain in place. Current DoD energy policy and guidance specifically encourages the increased use of renewable energy for energy resilience. This section explores how DoD renewable energy and energy resilience requirements overlap with and reinforce each other.

1.1 DOD RENEWABLE ENERGY POLICY

A series of laws passed in the mid-2000s encouraged greenhouse gas (GHG) emissions reductions across the Federal government, and set renewable energy requirements for federal agencies and for DoD specifically. These laws include:

- **The Energy Policy Act (EPAct) of 2005 (Section 203)** requires 7.5% of the electricity consumed by all federal facilities to come from renewable energy sources starting in 2013 and each year thereafter.
- **The National Defense Authorization Act (NDAA) of 2007 (Section 2852)** requires that DoD "procure or produce" the equivalent of 25% of the electricity it consumes from renewable energy sources by 2025 and each year thereafter.
- **The NDAA of 2012 (Section 2828)** established an interim target that DoD produce or procure the equivalent of 15% of the electricity it consumes from renewable energy sources by 2018.

Executive Orders within the last ten years have given federal agencies different requirements related to renewable energy, but the underlying statutory requirements have remained in place (McDonald, 2016). Executive Order (EO) 13693 (2015) required federal agencies to consume 30% renewable energy by 2025. EO 13834 (2018) revoked EO 13693, but reaffirmed the requirement that federal agency heads meet statutory renewable energy targets. EO 14008 (2021) tasks agency heads with organizing and deploying a "government-wide approach to combat the climate crisis," including through deployment of clean energy technologies. It also establishes new policy goals to increase renewable energy production on public lands and double offshore wind capacity by 2030 (Section 207).

1.2 DOD ENERGY RESILIENCE POLICY

During the past decade, DoD has established policies that require military installations to sustain their critical missions in case of disruptions to the commercial electricity grid.

- **DoD Directive (DoDD) 4180.01** of 2014 defined DoD's energy policy as the need to improve energy security, including the need to "enhance the power resiliency of installations" (USD(A&S), 2018).
- **DoD Instruction (DoDI) 4170.11** was updated in 2016 to focus installation energy management on "energy resilience" instead of "energy flexibility." DoDI 4170.11 states that DoD components "shall plan and have the capability to ensure available, reliable, and quality power to continuously accomplish DoD missions from military installations and facilities" (USD(AT&L), 2016). DoD subsequently issued more detailed guidance on how energy resilience should be incorporated into planning at the installation level (ASD(EI&E, 2017).

Reinforcing these DoD leadership directives and instructions, Congress, in Section 2831 of the NDAA of 2018, defined "energy resilience" for the first time in statute, and focused DoD energy policy on the need to "ensure the readiness of the armed forces for their military missions by pursuing energy security and energy resilience."[2] (10 USC 2911).

From this headquarters level policy flowed individual Military Departments directives that have established requirements for the minimum number of days that military installations must be able to maintain critical missions independent of the commercial electric grid. The Army and the Navy both require that critical missions be sustained for a minimum of 14 days (DON, 2020; Secretary of the Army, 2020). The Air Force requires that mission essential functions be sustained for at least seven days, unless the mission can be moved to another location (USAF, 2020b).

The Services also have specific guidance related to the deployment of electric systems, power plants, and back-up power generators on base. In some instances, the policies have been at odds with the strategic requirements articulated in DoD-wide policy. The Air Force, for example, issued a policy in 2015 that allowed back-up power systems to only serve individual facilities, rather than multiple facilities (USAF, 2015). The policy also did not list microgrids as

[2] https://www.congress.gov/bill/115th-congress/house-bill/2810/text

eligible back-up power systems. The Air Force policy was misaligned with the energy resilience guidance contained in DoDI 4170.11, and was superseded by a new policy in October, 2020 (USAF, 2020a). The new policy includes microgrids as an eligible back-up power system and allows back-up power systems to serve multiple facilities. The limitations imposed by the 2015 policy, however, caused complications and delays in Air Force energy resilience projects such as the Otis Air National Guard Base microgrid (Altman, 2020).

1.3 RENEWABLE ENERGY FOR RESILIENCE

DoD's Energy Strategic Plan from December, 2020 states that "distributed renewable energy assets are an essential ingredient in a diverse mix of energy supply for resilience with the potential to extend the operation of traditional resources (ASD(S), 2020b)." DoD energy resilience policies allow for and encourage the use of renewable energy for energy resilience. These policies have shaped DoD's current and previous energy project development efforts, and have also provided justification and impetus for DoD to consider its existing renewable energy systems as resilience assets. Examples of policies that have shaped the development of DoD's renewable energy fleet include:

- **The NDAA of 2012.** Section 2822 of the NDAA requires that military renewable energy projects consider energy security during the design and development phase.[3] In cases where military renewable energy projects do not include energy security, the Office of the Secretary of Defense (OSD) requires the Military Department to submit a cost-benefit analysis justifying the decision and to notify congressional defense committees of the decision (USD(AT&L), 2012).
- **1 GW goal.** In 2012, the Obama Administration called on each of the Military Departments (e.g., Army, Air Force, Navy) to deploy 1 GW of renewable energy to increase the energy security of installations by 2025 (White House, 2012). This target was subsequently incorporated into military service strategic energy plans (e.g., DASN(Energy), 2012).
- **REC purchases.** DoD adopted a dual approach to achieving its statutory renewable energy goals that included purchasing renewable energy credits (RECs) from off-site renewable energy projects and generating renewable energy on or near its installations. In 2016, however, DoD stated that RECs not tied to a renewable energy project on a DoD installation (i.e., "unbundled RECs") are not a "desirable substitute for renewable energy production that provides energy resilience for its military installations" (ASD(EI&E), 2016a).[4]
- **DoD Directive 4180.01.** Establishes that DoD's energy policy is to "diversify and expand energy supplies and sources, including renewable energy sources" in order to "enhance

[3] https://www.govinfo.gov/content/pkg/PLAW-112publ81/html/PLAW-112publ81.htm

[4] As of FY 2020, REC purchases account for 5% of renewable energy "produced or procured" by DoD (ASD(S), 2021).

military capability, improve energy security, and mitigate costs in its use and management of energy" (USD(A&S), 2018).

- **DoD Instruction 4170.11.** States that DoD is committed to "creating opportunities to install renewable energy…to enhance resilience." The Instruction requires installations to install primary power and emergency generation to support critical missions, and states that such "energy resilience solutions are not limited to traditional standby or emergency generators. They can include integrated, distributed, or renewable energy sources." The instruction also states that "distributed energy sources shall be used for on-site generation using…renewable technologies…when determined to be life cycle cost effective or to provide resilience" (USD(AT&L), 2016).
- **The NDAA of 2018.** Section 2831 of the NDAA states that "in selecting facility energy projects that will use renewable energy sources, [the Secretary of Defense may] pursue energy security and energy resilience by giving favorable consideration to projects that provide power directly to a military facility."[5]

In addition to requiring that renewable energy projects consider energy security and resilience, Congress has provided additional direction and OSD has issued policies and guidance to prioritize energy resilience within each of the energy acquisition authorities utilized by DoD and the services. (See Section 3 for a more detailed discussion of how energy resilience has been incorporated into various acquisition authorities).

1.4 DOD ENERGY ORGANIZATIONAL ROLES

Retrofit project proponents will need to map and align stakeholders within DoD offices, as well as within DoD installations.

1.4.1. DoD Energy Stakeholders

ORGANIZATION QUESTIONS	**ORGANIZATION** TAKEAWAYS
Are the relevant DoD energy stakeholders aligned in support of the project?	Successful energy resilience retrofits require alignment and coordination at the headquarters level, the energy program office level, and across energy acquisition and contracting entities.

DoD energy policy is designed and executed by a network of senior executives from Pentagon headquarters, energy program offices located within each of the three Military departments (i.e., Army, Air Force, Navy), and hundreds of individual military installations with their own

[5] https://www.congress.gov/bill/115th-congress/house-bill/2810/text

tenants, critical missions, and requirements. Significant coordination between these groups of DoD stakeholders is required in order to achieve DoD's ambitious energy resilience goals.

- **Senior Executives.** The Office of the Deputy Secretary of Defense for Energy (ODASD(Energy)) is responsible for developing "energy-related policy and governance for programs and activities that enable resilient, efficient, and cyber-secure energy for Joint forces, weapon systems and installations."[6] Each military department designates an assistant secretary to serve as a senior executive for installation energy.
- **Energy Program Offices.** Each military service has a dedicated energy program office that assists with energy projects to enhance energy resilience. These offices serve as a conduit between DoD headquarters, individual installations, and the private sector (e.g., renewable energy project developers). The Air Force's Office of Energy Assurance (OEA), the Army's Office of Energy Initiatives (OEI), and the Navy's Energy Security Program Office (ESPO)[7] coordinate project development at their installations and support development and execution of Installation Energy Plans (IEPs).[8]
- **Acquisition and Contracting.** In addition to energy program offices, the military services may work with different offices to support the contracting and acquisition of energy resilience under the authorities discussed in Section 3. Prior to 2010, for example, the Air Force worked with contracting offices at the installation level to enter into energy savings performance contracts (DODIG, 2016). The Air Force subsequently centralized performance contracting program management under the Air Force Civil Engineer Center (AFCEC). AFCEC partners with the U.S. Army Corps of Engineers, the Defense Logistics Agency Energy Office, and the Air Force Installation Contracting Agency, to serve as performance contracting acquisition agents for the Air Force (AFCEC, 2017). These offices manage the procurement and acquisition process for energy savings performance contracts on behalf of individual installations. The offices responsible for energy acquisitions vary by military service and by acquisition type.

1.4.2. Installation Energy Stakeholders

ORGANIZATION QUESTIONS	**ORGANIZATION** TAKEAWAYS
Are there "champions" at the installation level who support the project?	Installation commanders must be supportive of the project, and must be aligned with their energy staff, such as the public works or civil engineering staff responsible for energy

[6] https://www.acq.osd.mil/log/ENR/index.html
[7] The Energy Security Program Office was previously known as the Resilient Energy Program Office, and before that as the Renewable Energy Program Office (Kleim, 2016; Kleim 2017; Kleim, 2019).
[8] An IEP is a "holistic roadmap that enables the installation to work constructively towards its goals in energy efficiency, renewable energy and energy resilience." (ASD(EI&E), 2016c).

	infrastructure, and the installation energy manager.
Are project champions military or civilian personnel?	Some energy leadership positions at military installations are filled by active duty personnel, who rotate to other assignments at other installations. Civilian energy staff, however, do not rotate.

- **Are there champions at the installation level?** Resilience retrofit projects should have advocates, or champions, at the installation level who support and drive the project. Installation-level champions are typically embedded within the installation's energy leadership chain of command and have a working knowledge of the installation's specific energy resilience goals, and the ability to identify and overcome project barriers. Each installation has its own energy leadership (e.g., Public Works Director or Base Civil Engineer) who are responsible for coordinating with overall installation leadership (e.g., Garrison or Wing Commander) in order to execute energy resilience goals from DoD headquarters and the program offices. Each installation may also include dozens of tenants (e.g., other Federal agencies, national laboratories) with their own energy resilience requirements for critical missions. Many installations also have dedicated energy managers who initiate and oversee energy conservation, generation, and resilience projects across the base (USD(I&E), 2005). Resilience retrofit project champions can come from different backgrounds at the installation level, and can include installation energy managers, regional energy managers, engineers, project managers, and community outreach specialists, among others (e.g., Resource Efficiency Managers). Project champions are critical to the success of resilience retrofits because of the complex range of considerations (e.g., engineering, cybersecurity, contracting, and financing considerations) and the diverse mix of stakeholders involved (i.e., installation and headquarters personnel, project developers, and technology providers).
- **Are the champions military or civilian personnel?** Active duty personnel rotate during their careers and do not stay in one location permanently. The personnel filling energy leadership and staff roles at installations may therefore change during the energy resilience project lifecycle. Some energy positions are filled by civilian employees or contractors, who are not required to rotate. If the project champions for the prospective energy resilience retrofit project are scheduled to rotate out, project proponents should work to ensure that a succession plan is in place for new personnel to sustain project momentum

2.0 FUNDING & FINANCING CONSIDERATIONS

The primary consideration for retrofitting existing solar PV for resilience is how to pay for the additional equipment required. Project proponents need to determine whether the project will require additional funding or financing, and where those new sources of capital will come from. Funding refers to an amount of money provided to the project with no requirements to pay it back. For DoD energy resilience retrofits, it is likely that funding would come primarily from appropriated federal budgets and contractual amendments, where available. As discussed in Section 2.2, however, funding may also be provided by state or utility partners. Financing refers to capital provided by, for example, banks or equity investors that must be repaid over time. As discussed in the Introduction, this report focuses primarily on existing projects that are owned by third parties and financed with private sector capital. Securing additional financing therefore typically requires engagement with, and agreement from, existing capital providers – most of which may only be familiar with traditional power purchase agreement structures – not DOD's unique contracting structures and complex regulatory structure and processes (see Section 3 for Contracting & Legal Considerations). Complexities aside, there are multiple ways in which funding and financing may potentially be combined to support retrofits. Examples include:

- **Scenario 1: Funding only.** The cost of the resilience retrofit equipment is paid for by DoD, another Federal agency, state/local governments, and/or electric utilities with dedicated grant programs. Retrofits that do not create significant additional economic benefits, such as new revenue or utility bill savings, require funding.
- **Scenario 2: Financing only.** The cost of the resilience retrofit equipment is paid for by a third-party capital provider, which recoups the investment over time. The capital provider agrees to finance the retrofit based on the new revenue or savings that new equipment is projected to create. A new battery, for example, might be able to earn additional revenue by participating in wholesale and ancillary services markets or might be able to create additional savings by reducing demand charges at the installation (Akhil et al., 2015). While batteries can create multiple streams of economic value, the current policy environment has been insufficient to support batteries configured to do so at scale. Future policy changes, such as federal tax credits for stand alone battery storage systems and FERC orders, may expand opportunities for battery deployment.
- **Scenario 3: Existing project economics.** Some existing projects generate significant economic returns, and there may be opportunities to add resilience retrofit equipment in such a way that the overall project economics remain commercially attractive. However, project owners and capital providers will not agree to add equipment that reduces the overall economic performance of the project without receiving some additional benefit

from the deal. The additional benefit could include, for example, the opportunity to renew or extend a project contract term (which would extend the amount of DoD operating budget funds that the project would receive over time).

- **Scenario 4: A blended approach.** The cost of the new equipment and the retrofit is paid for by some combination of Scenarios 1-3 in which new funding from DoD or other partners, new revenue and savings enabled by the retrofits, and existing project economics are leveraged to install new equipment. As discussed in Section 3, however, contractual limitations may constrain the way that certain funding streams, ownership models, and financing approaches can be combined.

A complicating factor for each of these scenarios is that the resilience retrofit equipment must be optimized to support resilience. Batteries can be configured to maximize economic value from multiple revenue and savings streams, but they will not be useful for resilience if they are fully discharged when a power outage occurs. The contractual structures required to enable batteries to both capture economic value and provide resilience are also not yet widely available or familiar to capital providers. DoD retrofit projects must balance project economics with the ability to meet the resilience requirements of critical missions (Section 1.2).

The rest of this Section focuses on the two questions below:

FUNDING & FINANCING QUESTIONS	**FUNDING & FINANCING** TAKEAWAYS
What sources of funding are available to DoD retrofit projects?	Projects that cannot secure funding may not be able to move forward. DoD budgets, funds from other state agencies, state grant programs, and/or utility investments can pay for resilience retrofits, but each funding source comes with constraints and limitations that require a case-by-case analysis.
What additional risks and returns are created by the retrofit project?	Retrofits that create limited or uncertain financial returns or require complex contracting structures that are not replicable and have additional complexities in comparison to commercial transactions, are less attractive to capital providers.

2.1 FUNDING PROVIDED BY DOD OR OTHER PARTNERS

Energy resilience projects at DoD may use funding from federal agencies (including DoD and civilian agencies like the Department of Energy), state and local governments, and/or electric utilities in order to pay for the upfront costs of retrofits.

2.1.1 Federal Funding

Despite increased focus on energy resilience from DoD headquarters and Service levels (Section 1.2), Congressionally-appropriated funding for DoD resilience remains limited. Historically, DoD has prioritized funding for operational energy rather than installation energy, resulting in DoD budget requests for installation energy resilience projects that may not be fully appropriated (Niemeyer, 2018; Conger, 2018). Examples of appropriated resources that could be systematically used for energy resilience include:

- **Energy Resilience and Conservation Investment Program (ERCIP).** ERCIP is a subset of DoD's Military Construction (MILCON) account, and is the primary source of federal budget funds for developing projects that enhance energy resilience on military installations. In FY 2020, DoD identified 32 energy resilience and conservation projects totaling $232 million.[9] At this current level of funding, it would take an estimated 20+ years to provide an energy resilience project to every installation in the United States.
- **DoD Demonstration Programs.** DoD is able to fund energy resilience demonstration projects through Research, Development, Test, and Evaluation (RDT&E) programs such as the Environmental Security Technology Certification Program (ESTCP). The amount of RDT&E funding available per project, and the amount available for energy resilience each year overall, is limited. ESTCP's total budget in FY 2021, for example, was $61 million, of which $25 million was allocated to energy and water projects (DoD, 2020). Individual ESTCP project awards are typically less than $2 million. RDT&E programs are not intended to drive energy resilience market growth.
- **Facilities Sustainment, Restoration, and Modernization Program (FSRM).** Appropriated funding provided through DoD's FSRM account (part of the Operation & Maintenance appropriation) is another avenue for funding energy resilience. Military installations can request FSRM funds for energy resilience projects, but energy resilience is not prioritized over competing requests for funds in the FSRM scoring model (Narayanan et al., 2019). FSRM funding is also intended for smaller improvements in which project costs generally do not exceed $2 million (Herrera, 2019).
- **Section 2912 funds.** Under 10 USC § 2912, DoD can harvest energy cost savings and place the realized funds in a no-year account without additional Congressional authorization or appropriation. Fifty percent of those funds may be used for "the implementation of additional energy resilience, mission assurance, weather damage repair and prevention, energy conservation, and energy security measures, including energy resilience and energy conservation construction projects, at buildings, facilities, or installations of the Department of Defense…" among other purposes. The Army piloted the Resilient Energy

---

[9] https://www.acq.osd.mil/eie/Downloads/IE/FY2020%20ERCIP%20Congressional%20Notification.pdf

Funding for Readiness and Modernization (REFoRM) Initiative using $35 million of savings under Section 2912 in 2020 (Beehler & Evans, 202), and the Air Force piloted the Resilient Energy Savings Resource Vault (RESERV) using $15 million in savings in 2019 (SAF/IEE, 2020).

- **Other Federal Funds.** DoD organizations can apply for funding under the Department of Energy's (DOE) "Assisting Federal Facilities with Energy Conservation Technologies" (AFFECT) program, but should have reasonable expectations. In 2021, for example, DOE had a budget of $13 million for AFFECT, and planned to award 13-20 projects across the Federal government. No single application could request more than $1 million from the AFFECT program. Federal applicants would need to embed the AFFECT-funded project within a larger ESPC or UESC contract such that the AFFECT funding was leveraged by at least 10:1 by private sector and other funding. Finally, the "Areas of Interest" for the AFFECT program changes from year to year, and energy resilience is not guaranteed to be an Area of Interest every year. DOE Office of Electricity (OE) grant funding has also been awarded to support energy resilience projects at DoD installations. AFFET and OE programs are especially worthwhile to note, as both were appropriated significant amounts of additional funding through the recently passed Infrastructure Investment & Jobs Act (IIJA).

Third-party owned projects may also be eligible for federal tax incentives. New solar PV systems are eligible for a 26% investment tax credit, and a 5-year accelerated depreciation schedule. Project developers may opt to repower some solar sites and replace existing solar PV systems with more efficient panels in order to claim the tax benefits on the new equipment. Energy storage projects that are charged at least 75% from solar energy systems are also eligible for a 26% federal investment tax credit, and a 5-year accelerated depreciation schedule. The rules regarding whether a storage system added to existing solar PV can qualify for solar tax benefit are unclear, but market analysts assume that it is possible, based on previous private letter rulings from the Internal Revenue Service (Elgqvist, 2018; IRS, 2015; IRS, 2017a).

2.1.2 Non-Federal Funding

Some state agencies and electric utilities provide funding support to energy storage and microgrid projects; each program is governed by rules concerning eligible applicants, eligible projects, funding amounts, schedules, etc., all of which are subject to change. There are also no dedicated state or utility funding sources for defense energy resilience projects, and military projects must compete with other project types for non-federal funds. Several recent reports provide case studies of how DoD energy resilience projects have received resources from state agencies and/or from utilities (Klauber et al., 2021; 2021; Rickerson et al., 2021). Most of the projects that have received civilian resources have been new construction, although there are exceptions. Otis Air National Guard Base in Massachusetts, for example, received state funding to retrofit a wind energy project to provide resilience, and Marine Corps Air Station Miramar in California received state funding to add additional resilience capabilities to a landfill gas microgrid (Rickerson et al., 2018). Broadly, the types of funds include:

- **State energy funds and green banks.** A growing number of states have created incentive programs for energy storage and/or microgrids (Cramer & Verclas, 2021; Endemann, 2019). The Database of State Incentives for Renewable and Efficiency (DSIRE)[10] provides a summary of available storage and clean energy programs, but for the most current and complete information, DoD installations should contact their state energy offices to determine if financial support is available and under what conditions.
- **State military advisory bodies.** Close to 35 states have military advisory bodies dedicated to coordinating with DoD, and 13 states have funds to enhance the military value of installations (NCSL, 2016). Although the primary purpose of many of these offices and funds is economic development, some state agencies, such as the Connecticut Office of Military Affairs, have provided funds for energy resilience to DoD installations (CT OMA, 2020).
- **Utility investments.** As described in a report from the National Association of Regulatory Utility Commissioners, some utilities have invested ratepayer funds in renewable energy and/or energy resilience projects at DoD installations (Rickerson et al, 2021). These projects include, for example, multi-megawatt PV projects at military installations served by Southern Company in Alabama, Georgia, and Mississippi, a 50 MW biodiesel power plant at Schofield Barracks in Hawaii, and a 24 MW power plant at Marine Corps Air Station Yuma. These projects require consideration and approval from state regulators, and typically need to demonstrate that they create benefits to ratepayers above and beyond the national security benefits of supporting DoD missions.

2.2 THIRD PARTY FINANCING

DoD policy and guidance emphasizes the use of third-party ownership and private sector capital to acquire renewable energy projects (USD(AT&L), 2016; ASD(EI&E), 2016b). DoDI 4170.11 also encourages installations "to use alternative financing or utility privatization arrangements in the pursuit of energy resilience projects." Each of the Military Services' energy program offices actively support pipelines of renewable and resilient energy projects that leverage private sector capital.

[10] https://www.dsireusa.org/

As a result of these policies and project development efforts, most of DoD's existing large-scale renewable energy projects are third-party owned and financed. As a result, DoD will need to partner with third-party developers, project owners, and financers to retrofit existing solar PV systems with resilience assets. DoD solar PV projects typically utilize a combination of debt and equity to provide financing for the upfront capital costs. To retrofit existing PV arrays for resilience within the context of a third-party financed project, there must be a mechanism for the capital provider to recover their investment plus profit at an acceptable level of risk. Equity investors, for example, seek an unlevered internal rate of return (IRR) in the low-teens (e.g., 13%), whereas debt providers may seek less than 10%, depending on market conditions (Feldman et al., 2020). If retrofitting an existing project has a *significant* negative impact on the current financial structure of the project from the investor perspective, then the project is unlikely to proceed. However, in instances where retrofit costs are minimized by utilizing one of the scenarios outlined above, a retrofit project may be possible.

2.2.1 Investor Risk Considerations

A potential investor in an energy resilience retrofit project will identify sources of risk that could threaten their investment recovery and profit realization (Holmes, 2019; Tine, 2019; Strahl et al., 2015). Two significant risks with resilience retrofits include:

- **Technology performance and obsolescence risks.** Resilient energy systems are newer than many other facility technologies that attract third-party investment (e.g., energy efficient lighting, HVAC controls, PV), so fewer investors are familiar with these technologies and those who have invested in them have less experience. This creates a number of concerns: will a specific technology deliver on its performance claims? Will it need more maintenance than expected? Will its lifetime be shorter than promised? Can it be operated properly by whichever party has operational responsibility? Will newer technologies be introduced that could render the investment obsolete before the contract term is completed? Technology risks may increase the cost of capital to retrofit projects.
- **Revenue risk from new markets.** From the investor's perspective, the ideal revenue stream is contractually guaranteed over the full investment recovery horizon, with the revenue derived from a creditworthy counterparty (Corfee et al., 2010). The United States Government presents little or no counterparty payment risk. The additional revenue streams available to energy resilience projects, however, may not be contractually guaranteed over the long-term. For example, storage and microgrid projects may be eligible to participate in frequency regulation or capacity markets (Oueid, 2019). There are typically no long-term offtake contracts available in these markets, however, and prices

can be volatile (Baxter, 2018). As a result, the developer and the investor are required to assume merchant risk, betting that these markets will generate sufficient revenue to provide an acceptable rate of return over a long term project duration (see Text Box 1). An added element of risk is associated with the fact that various regulatory bodies (e.g., state and federal energy regulators) and wholesale market operators determine the definitions of these products, the structure of their markets and the resources that may or may not participate. There have been several examples of storage value streams becoming impaired due to changes from regulatory and administrative processes (Lacey, 2017). Revenue risk may discourage investors from financing retrofit projects and/or deeply discounting the value of potentially available revenue streams.

- **Market complexity.** The most significant inhibitor to DoD energy resilience market adoption is contracting complexity in combination with an un-replicable market dynamic. DoD projects take significantly longer to develop and deploy, have greater overall uncertainty in comparison to projects in the commercial market, and require a case-by-case solution (ODASD(Energy), 2020). This results in a challenging market dynamic that inhibits developer engagement and typically leads to "deal fatigue" prior to successful project execution.

Text Box 1. Solar and Storage PPA for Fort Detrick

Fort Detrick is the home of the U.S. Army Medical Research and Development Command and its biological research agency, the U.S. Army Medical Research Institute of Infectious Diseases. In 2013, the Army awarded a 25-year PPA to Ameresco for an 18.6 MW solar PV plant at Fort Detrick under 10 U.S.C. 2922a, as well as a 26-year land lease (OEI, 2019). The solar PV project became fully operational in February, 2016. In addition to the solar PV project, the PPA contract also contained a separate contract line item for an energy storage facility. Ameresco began construction of a battery energy storage project under the second contract line item after the solar PV was operational. Ameresco plans to use the battery project to earn revenue through the PJM frequency regulation market, and the company projects that both the solar PV and battery energy storage system will remain economically viable under the contracted PPA rate. Rather than work with external capital providers, Ameresco financed the battery energy storage project itself.

2.2.2 Capital Structure Considerations

The capital structure of the project may also impact retrofit project viability. Existing solar projects may depend on tax equity investors, who utilize models such as "partnership flip" financial structures[11] to allow them to monetize the benefits of the Investment Tax Credit (ITC)

[11] A partnership flip structure enables a project developer to partner with a tax equity investor. The tax equity investor provides a portion of the equity investment in the project (i.e., 30% to 60%) in exchange for an initial claim on federal

and the depreciation of the assets on an accelerated schedule. The ITC is subject to recapture by the federal government if the solar PV project is sold within five years of being in service (Stoel Rives LLP, 2016). As a result, projects that rely on tax equity investors may be reluctant to modify an existing solar project that is within the recapture period in order to avoid disrupting investors' ability to claim these tax benefits. However, if the resilience retrofit occurs after the recapture period, if the retrofit does not impact the project's tax credit status, or if the project is not reliant on tax equity investors and the ITC, project owners may be more inclined to amend the original deal because they only need to consider the debt portion of the project.

2.2.3 Contract Term Considerations

DoD's ability to utilize long-term contracting authority for power projects is crucial to attracting investors. Investors in resilience retrofit projects will likely seek a *minimum* 10-year investment horizon and prefer timeframes closer to 20+ years. However, a challenge to financing energy resilience retrofits is the lack of standardized contractual terms and conditions. Model contracts have been developed to support and streamline deals in the solar, wind, and energy performance contracting industries (Baxter, 2019). Model contracts and standard project documents that address off-take agreements, operating risks, and liability in the event of losses for technologies such as energy storage and microgrids have not been developed and widely adopted (Baxter, 2018). As a result, energy resilience retrofit projects currently require the development of one-off contracts that slow the pace of project development and raise transaction costs.

incentives like the ITC and modified accelerated cost recovery system (MACRS). The tax equity investor agrees on a pre-negotiated IRR for a set period; once the period ends, the agreement "flips" and the project developer receives most of the tax benefits and income associated with the project (Mendelsohn & Kreycik, 2012; Keightley et al., 2019).

3.0 CONTRACTING & LEGAL CONSIDERATIONS

DoD has acquired renewable energy projects using a range of contracting and procurement authorities during the past few decades. In some instances, military installations have purchased renewable energy systems outright. As discussed in previous sections, retrofits of existing energy systems that DoD owns and operates may not raise significant contracting or legal considerations. A large proportion of DoD's renewable energy fleet, however, has been developed in partnership with private sector capital providers and system owners. DoD has used multiple acquisition authorities to contract for renewable projects, rather than a single model (SEAB, 2016). This Section compares and contrasts the authorities used by DoD to acquire renewable energy: energy savings performance contracts and utility energy service contracts, power purchase agreements, enhanced use leases and easements, and utility privatization contracts. Other mechanisms, such as the Military Housing Privatization Initiative, intergovernmental services agreements (IGSAs), and cooperative research and development agreements (CRADAs), have been used to support renewable energy development at military installations. Their use, however, has been limited and is beyond the scope of this report. For each of the authorities in scope, this Section summarizes the statutory basis, energy resilience requirements, and key considerations for energy retrofit projects.

CONTRACTING QUESTIONS	**CONTRACTING** TAKEAWAYS
Which federal acquisition authority was used to procure the solar PV?	DoD uses several different acquisition authorities to procure solar, each of which enables and constrains resilience retrofits in different ways.
What is the contractual pathway for retrofitting existing solar PV systems?	Each of the acquisition pathways results in a government contract. Adding resilience capabilities to existing contracts requires a contract modification, and government contracting officers have the authority to modify existing contracts (USD(A&S), 2021a). Since adding resilience capabilities changes the project, a bilateral contract amendment or new contractual agreement signed by both the government and the contractor is required.
How much time is remaining in the contract?	Each of the acquisition pathways has a contract term limit (e.g., 5-25 years). Retrofits made toward the end of the contract life may be challenging since they may not be able to generate sufficiently attractive economic returns for the project owners over a short time period.
Are the project stakeholders aligned in favor of the proposed contractual	Since a change in scope may alter the economic performance of an existing project, the interests of multiple

changes?	stakeholders need to be carefully balanced. The proposed retrofits must adequately create and align value not only for DoD and for the project owners, but for other stakeholders such as the project investors as well.
How does the underlying land lease compare to the energy contract term?	The duration of the land lease may differ from the energy contract in a way that may enable or constrain adding additional equipment. The land lease may also specify that only certain types of equipment may be installed on the land, which may hinder efforts to add resilience capabilities.
What types of updates are possible without triggering a new competition?	The addition of new energy technologies to an existing PV system may be possible under the existing contract. Depending on the acquisition authority and the scale of the proposed changes, however, the addition of new technologies may require the project to be competitively bid out.

3.1 ENERGY SAVINGS PERFORMANCE CONTRACT & UTILITY ENERGY SERVICE CONTRACT

Under energy savings performance contracts (ESPCs), an energy services company (ESCO) pays the upfront cost to install energy upgrades at federal property. The ESCO's investment - plus profit - is then repaid from the savings generated by the upgrades over time. ESCOs guarantee the technical and economic performance of the energy upgrades. Under utility energy service contracts (UESC), the utility servicing the federal facility pays the upfront costs to install the upgrades, rather than ESCOs. ESPCs and UESCs can each be up to 25 years in length. To date, performance contracts have been one of – if not the most - broadly used contracting vehicles successfully utilized to deploy energy resilience solutions across military installations.

- **ESPC Energy Sales Agreement (ESA).** ESCOs are also allowed to own onsite energy generation within an ESPC and sell the output under an ESA for a period of 20 years. ESCOs are able to claim the federal tax incentives (e.g., the investment tax credit for solar PV) under ESPC ESAs (Logan, 2012; IRS, 2017b). ESAs are not allowed under UESCs.
- **Authority.** The Energy Policy Act of 1992 created ESPC and UESC authority for federal agencies, and specific ESPC and UESC authorities were created for DoD in the FY 2007 National Defense Authorization Act (NDAA) (10 U.S.C § 2913). DoD has issued a policy encouraging the use of ESPCs and UESCs (USD(AT&L), 2008).
- **Resilience Requirements.** DoD issued policy guidance requiring ESPCs and UESCs be used to enhance energy resilience in 2018 (ASD(S), 2018). The guidance states that both

authorities should be executed "in a manner consistent with the energy resilience guidance contained in DoD Instruction 4170.11."

3.1.1 ESPC & UESC Retrofit Considerations

- **Blending.** Energy conservation measures can be blended within ESPCs and UESCs such that the savings from quicker payback measures (e.g., lighting retrofits) can be used to subsidize the economic performance of measures that might not otherwise payback on their own within the contract term. Energy resilience equipment, such as storage or microgrid controls, can be blended into existing performance contracts - but earlier inclusion with the contract will increase the likelihood that the project will perform economically within the maximum 25-year term. Storage and controls can also help ESCOs guarantee additional savings streams, such as demand charge reductions, within performance contracts (Baxter, 2016).
- **Scoping.** Performance contract scopes can be fairly broad and flexible. New capabilities and technologies can be added to performance contracts without needing to recompete the contract, as long as the technologies were not specifically scoped and bid out at the beginning of the project. Since energy resilience is a relatively new field of practice and investment, it has not been scoped in a definitive manner into most existing performance contracts.
- **Additional funding.** ESPCs and UESCs can integrate grant funding from other sources (e.g., state energy funds, AFFECT, DOE OE grants) into the contracts to enhance their economic performance. Until recently, however, federal military construction (MILCON) appropriations were not allowed to be integrated into performance contracts. The Energy Resilience and Conservation Investment Program (ERCIP) can be used to fund military energy resilience projects, but ERCIP funds are a subset of MILCON. As a result, ERCIP has been ineligible for broad use within ESPCs and UESCs. The FY 2021 NDAA (§ 2823(b)), however, updated federal policy to allow ERCIP use within performance contracts (Kidd, 2021).

3.2 POWER PURCHASE AGREEMENT

The DoD is unique among federal agencies in that it can enter into power purchase agreements (PPA) with third-party owners of electricity generation for up to 30 years. DoD PPAs projects can be located either within or outside of military installations, and can generate electricity from either renewable or non-renewable sources. The projects are subject to approval by the Secretary of each military Department.

- **30-Year PPA Authority.** The 30-year PPA is authorized under 10 U.S.C. 2922a, and was created under the Military Construction and Codification Act of 1982. The 2922a PPA authority was not used to support energy project development until after 2012, when interest in the authority increased with the creation of the Army's Multiple Award Task Order Contract (MATOC) (McDonald, 2014; Koch, 2014).

- **Other PPA Authorities.** DoD can also enter into PPAs via other authorities. Federal agencies can also enter into 10-year PPA contracts under FAR Part 41, but this requires delegation of GSA's authority (Acquisition of Utility Services) (GSA, 2015). In certain cases, agencies can include an additional 10-year option at the end of the original 10-year term.[12] DoD has specific authority to enter into 10-year PPAs for renewable energy (10 USC 2410q), and can also enter into PPAs of indefinite length, but with a 1-year termination notice (DFARS PGI 241.2).[13]
- **Resilience Requirements.** 10 U.S.C. 2922a Section (d) requires that the Secretary approving the PPA "ensure energy security and energy resilience are included as critical factors in the provision and operation of energy production facilities."

3.2.1 PPA Retrofit Considerations

- **Energy resilience integration.** The terms of the PPA contract may not permit the solar PV generator to be included as part of a larger energy resilience solution, such as a microgrid. In such a case, the terms of the PPA would need to be renegotiated (Kurnik & Voss, 2020). The addition of new equipment (e.g. battery storage) under a PPA may also require the PPA to be competitively bid out to the market if there is not a contract line item that allows for it in the original contract (see Text Box 1).
- **Pricing.** The purchase price for electricity under the PPA is typically contracted as a cents per kilowatt-hour (¢/kWh) amount at a fixed rate or with an escalator. The 25-year contract for the 16.4 MW solar PV system at Davis-Monthan AFB, for example, has a price of $0.045/kWh with 1.5% annual escalator (Elliott, 2014). Retrofits that would push the comparable $/kWh rate above the contracted amount - or at least above the cost that power would otherwise be purchased from the utility - may be less likely to be accepted and approved.
- **Islanding.** PPAs generally do not include provisions to allow the system to island. The contract would likely need to be modified to specify that islanding is permitted and also to clarify terms such as who would own the risk that the resilient system would function as required during islanded operations.

[12] The option can either be a "true" option, which means that the federal government cannot be penalized if they do not opt to extend the PPA (Shah, 2011). The federal government also entered into solar PPAs with conventional 10-year options that require penalty payments if the option is not exercised (SEAB, 2016).
[13] A 14 MW solar PV system at Nellis AFB was acquired under the DFARS PGI. *See* Andrews (2011)

3.3 UTILITIES PRIVATIZATION

Under utilities privatization (UP) contracts, DoD can convey the utility systems (e.g., electricity, natural gas and/or water) that it owns to other entities for a period of 10 to 50 years. The new system owner must invest funds to acquire, renovate, replace, maintain, operate, upgrade, and expand the utility systems conveyed by the installation. Historically, UP contracts were utilized to support on-base electricity needs and wastewater. Since approximately 2014, there is a precedent of amending UP contracts to support a broader suite of energy contracting needs, including energy resilience and demand response through amendments to existing contracting vehicles.

- **Authority.** UP authority, which was created through the FY 1998 NDAA, is found under 10 U.S.C. § 2688. DoD issued a Defense Reform Initiative Directive in 1998 mandating that the military departments devise plans for privatizing all utilities.
- **Resilience Requirements.** The FY 2018 NDAA added language to the UP authority requiring that the "conveyee manage and operate the utility system in a manner consistent with energy resilience and cybersecurity requirements and associated metrics provided to the conveyee to ensure that the reliability of the utility system meets mission requirements." DoD has implemented this requirement through supplemental UP guidance (USD(A&S), 2019).

3.3.1 UP Retrofit Considerations

UP contracts can be modified to incorporate additional measures in a more straightforward and seamless manner than others. Long-term UP contracts, however, may not include appropriate incentives for utility operators and incumbent UP contractors to make additional investments. DoD acknowledges that UP contracts can "present a near-term challenge to improve the reliability of existing energy infrastructure since energy resilience was not negotiated into the existing contract" (ASD(EI&E), 2017). DoD contracting officers may also not be willing to approve the additional costs, and budget impacts, associated with financing resilience retrofits through UPs. In the past, the Military Services have frequently taken a "strategic pause" in order to "determine if privatization is the best option for recapitalizing their deteriorating utility systems" (GAO, 2020b). UPs are a replicable contracting structure that can broadly facilitate the deployment of commercially-viable energy resilience solutions across DoD installations.

3.4 ENHANCED USE LEASE

The DoD enhanced use lease (EUL) or "leaseback" authority allows the Services to lease non-excess real property under their control to commercial persons or entities if the lease will promote national defense. It is distinct from the other authorities in that it enables real estate transaction authorities, and is not specifically for energy projects. The EUL authority allows the government to receive "in-kind consideration" (IKC) in lieu of rent payments. Each of the Military Services has used EUL authority to lease land for the development of energy projects. The project developers then configure the projects to provide energy resilience to the military installation during power interruptions as the IKC. EUL's must typically be paired with energy procurement contracts to ultimately be of value to project developers and third-party financiers, since this vehicle only serves as a land lease and not the energy procurement contract for energy solutions. EULs are also utilized for commercial building development, which potentially could provide resilience benefits to the installation as well.

- **Authority.** EULs are authorized under 10 U.S.C. 2667. The contracts are authorized for up to five years, unless the departmental Secretary determines that longer periods will promote national defense. EULs used for renewable energy projects are typically multiple decades in length. A review of Navy energy EULs, for example, found that the contract lengths ranged from 25-37 years (DODIG, 2017).
- **Resilience Requirements.** The NDAA of 2018 amended the EUL authority to state that energy projects "shall prioritize energy resilience in the event of commercial grid outages." DoD policy also requires that renewable energy projects procured by EUL be actively used by DoD in order to count toward DoD renewable energy requirements. One of the approved avenues for demonstrating active use is "to provide energy security for the installation by, e.g., retaining the right to divert to the installation the energy produced by the project in times of emergency" (USD(AT&L), 2012).

3.4.1. EUL Retrofit Considerations

- **Lease size.** The value of an in-kind contribution within EULs is calculated based on the fair market value of the land that is leased. In order for additional equipment to be added to an EUL, additional land must be leased, and the calculated fair market value of that land must be sufficient to support the purchase of the new equipment as an IKC.
- **Lease term.** Leases are limited to the useful life of energy production facilities, and cannot extend beyond that period to allow "follow-on or upgraded facilities" to be added to the project site (ASD(EI&E), 2016b).
- **Complexity.** Similar to the contracting structures and analysis above, it is important to note that there are no legal limitations to deploying additional resilience through EULs. EULs, however, are a complicated contracting framework that has been deployed on a case-by-case basis.

3.5 EASEMENTS

The Secretaries of the military departments can grant easements for "rights-of-way over, in, and upon" land controlled by DoD, provided that it does not interfere with DoD activities. The easements are explicitly allowed for a wide range of civil infrastructure, such as railroads, canals, tunnels, and reservoirs. Electric substations, transmission and distribution poles, and power lines are also explicitly eligible for easements. Easements can also be granted for "any other purpose that the Secretary considers advisable," which has opened the door for easements to also be used to site electricity generating projects. As with EUL's, in-kind contributions may be provided to the federal government in consideration for providing the right-of-way.

- **Authority.** Easements are authorized under 10 U.S.C. 2668. There is no limit on the duration of the easement, although easements cannot "include more land than is necessary for the easement."
- **Resilience Requirements.** DoD has issued guidance that easements used for energy and electrical infrastructure projects "should ensure that these projects appropriately take into consideration energy resilience requirements, as specified under title 10 and DoDI 4170.11." The guidance states that the cost effectiveness of adding technologies such as generation, batteries, microgrids, transfer switches, and inverters should be assessed when existing easements are modified or when replacement easements are sought. If easement projects receive in-kind consideration, then this in-kind consideration "shall ensure, when possible, that the installation has the necessary priority in the event of commercial grid outages."

3.5.1 Easement Retrofit Considerations

- **Technology inclusion.** Easements require specific language regarding the types of technologies that are being granted a right-of-way. Easements for existing solar PV systems may only specify an easement for the solar systems, and may not allow specifically for other equipment such as battery energy storage or switchgear. Easements may need to be modified to incorporate the additional technologies that would be required to add resilience capabilities.
- **Use of existing easements.** Although easements may need to be modified to accommodate additional technologies, DoD encourages the use of existing easements. DoD's energy resilience guidance for easements states that project proponents "should consider issuing a modification of an existing easement if such an easement can accommodate an additional use," rather than requesting the issuance of a new easement.

4.0 ENGINEERING CONSIDERATIONS

Energy resilience retrofit projects will encounter a broad range of engineering considerations. These considerations are governed by power systems engineering principles, with less room for interpretation than some of the considerations raised in other report sections. This section provides an introduction to some of the common engineering decision points related to selecting locations where energy resilience retrofits may be feasible, but does not attempt to provide a comprehensive summary of all the considerations a retrofit project may face (e.g., detailed design, integration, and commissioning). As described in Section 4.1, this overview is structured to reflect project architectures that present the best opportunities for resilience retrofits, as identified by subject matter experts with direct experience working with DoD. A key differentiator for this overview is that it focuses on existing solar PV that are interconnected upstream of the transmission substation, since this configuration enables more flexible, cost-effective, and technically feasible energy resilience retrofits (Section 4.3). This overview also focuses primarily on retrofitting existing systems, rather than the design considerations for installing new energy technologies (e.g., diesel generators or battery storage) that may be required.

Each subsubsection below starts with questions that project champions and/or project developers will need to understand, provides background information on the consideration, summarizes the most common options found in the field, discusses the implications for project design, and recommends preferred directions as appropriate.

4.1 ENERGY RESILIENCE SCOPING

ENERGY RESILIENCE SCOPING QUESTIONS	**ENERGY RESILIENCE SCOPING** TAKEAWAYS
Are mission requirements clear?	The proposed retrofit should support specific energy requirements identified by mission owners.
Have critical loads been identified and prioritized?	The project should be designed to provide resilience for specific critical loads upon which priority missions depend.
How does the project complement existing assets?	The project should be designed to intentionally strengthen, integrate, or replace existing energy assets in a way that addresses resilience gaps.

Project champions and project developers must answer a few basic scoping questions before moving on to more detailed engineering considerations. The following questions can help project developers understand the needs and capabilities of military installations, and help ensure that proposed retrofits are designed to meet DoD energy resilience targets and policies.

- **Are mission requirements clear?** DoDI 4170.11 requires that DoD develop energy resilience requirements that "align to critical mission operations in collaboration with tenants, mission owners, and operators of critical facilities on military installations" (USD(AT&L), 2016). Project developers must understand the mission requirements before beginning a project. The requirements should serve as the foundation for system design; poor alignment with requirements can lead to retrofit project failure. The mission owner provides mission requirements that support the warfighter. Typically, these requirements are not publicly available and conversations with mission owners are necessary. At the facility level, energy requirements are translated into the technical terms, such as quantity (i.e., the number of items in the facility needing power), response time (i.e., time until the mission will fail without power), duration (i.e., the length of time until the mission will need to move to another location), and quality (i.e., sensitivity of equipment to power interruptions). Identifying mission requirements is a critical first step to project design since having accurate requirements will help determine whether existing solar PV systems can meet mission needs or whether additional (or alternative) technologies are more appropriate. The proposed retrofit should support specific requirements identified by mission owners.
- **Have critical loads been identified and prioritized?** Prioritizing loads is important for determining the facilities or areas of the military installation that have the highest need for resilience. These priorities are determined by the installation commander based on the mission requirements and they are not published due to their sensitive nature. Individual loads are ranked on an ordinal scale or grouped into tiers. Even though the priorities change depending on the scenario (e.g. troop deployment versus cyberattack), there is typically only one version of the prioritized list. Understanding the priority loads will help the project developers determine which mission requirements need to be investigated first since they will provide the largest impact for resilience. Focusing on the priority loads will also increase support for an eventual project from higher levels within the DoD. The project should be designed to provide resilience for specific critical loads upon which priority missions depend.
- **How does the project complement existing assets?** Project developers must consider current energy assets when evaluating whether another asset is needed to meet the mission requirements for priority loads. These assets are any system that provides power or energy to the priority loads in addition to, or instead of, the electrical distribution system on the installation. Building- or grid-scale assets are normally tracked by the

installation engineers or public works staff, while equipment or partial-building scale assets are tracked by the mission owners. Installation engineers may therefore not have complete knowledge of currently installed energy systems at the building level. The lists of existing assets will commonly include uninterruptible power supply (UPS) systems, generators, and solar PV, with other generation and energy storage assets appearing occasionally. Project developers should compare current assets against the mission requirements and priority loads to determine gaps where a solar PV retrofit project can increase resilience for missions that are important to the installation. The project should be designed to intentionally strengthen, integrate, or replace existing energy assets in a way that addresses resilience gaps.

4.2 DATA ACCESS AND AVAILABILITY

DATA ACCESS AND AVAILABILITY QUESTIONS	**DATA ACCESS AND AVAILABILITY** TAKEAWAYS
Can the project developer access the data?	Many DoD installations do not have readily available energy system information, as a result of a lack of metering equipment or data access. Projects should identify the level and quality of available data at the outset.
What is the minimum amount of data necessary for a project?	At a minimum, electric utility bills must be shared with the project developers in order for them to verify the load requirements for the installation.

The following questions can help project developers understand data access and availability requirements in order to help ensure that proposed retrofits are designed to meet DoD energy resilience targets and policies:

- **Can the project developer access the data?** The level of installation data available will affect the fidelity of the economic and resilience analysis of any solar PV retrofit project. Many DoD installations do not have access to the necessary data as a result of not having meters, meters that do not capture the necessary data, and/or the inability of personnel to access the data collected. Data analyses are a required component of project design and the results are used to determine whether a project should move forward in the design process. Limited data will cause the engineers to use assumptions that could lead to incorrect project decisions. The designation of energy data as controlled unclassified information (CUI) will also require developers to comply with those standards before accessing the data, which may limit the developers that are able to work with the DoD. As the DoD continues using third parties to build and fund resilience projects, the importance of data availability and how it is controlled will continue to grow. Locations without sufficient data challenge the technical and financial feasibility of energy resilience retrofits.

- **What is the minimum amount of data necessary for a project?** The installation should share a comprehensive data set that enables the project developers to characterize the installation's energy consumption. For example, total energy demand and time of demand (i.e., interval consumption data) are critical to appropriately size an energy resilience retrofit. Installations should also consider sharing installation energy plans (IEPs), utility outage data, structural/electrical diagrams, and any other information that may be useful to the project developers. Table 1 shows common data types that should be requested to evaluate retrofit project opportunities. Table 1 categorizes the data type as mandatory, preferred, or optional. If the selected site is unable or unwilling to share the mandatory or preferred data, the project is unlikely to succeed. At a minimum, electric utility bills must be shared with the project developers in order for them to verify the load requirements for the installation.

Data Type	Importance
12-36 Months of Electricity Bills	Mandatory
12-36 Months of Electricity Outage Data	Mandatory
Substation and Circuit Electrical Single Line Diagrams	Mandatory
Stakeholder Resilience Requirements	Mandatory
Contracts Governing Existing Solar Assets	Mandatory
12 Months of Building Level Electricity Meter Data	Preferred
List of Important Facilities	Preferred
List of Backup Power Resources	Preferred
On-site Fuel Storage Locations and Amounts	Preferred
Accessible Communication Infrastructure Diagram	Preferred
Map of the Installation with Electrical Infrastructure Overlay	Optional
Stakeholder List and POCs	Optional
Previous Energy Assessments, Plans, and/or Studies	Optional
Incentives or Funding Mechanisms for Projects	Optional

Table 1: Data Type Categorization by Importance

4.3 SOLAR PV INTERCONNECTION

SOLAR PV INTERCONNECTION QUESTIONS	**SOLAR PV INTERCONNECTION** TAKEAWAYS
Does the interconnection agreement allow for adding resilience?	Existing interconnection agreements with solar PV systems may not allow resilience capabilities to be added.
Is the resilience project connected upstream or downstream of the substation?	Projects that are interconnected upstream of the substation are preferable since they require fewer network protections, and can be more readily configured to flexibly provide resilience to downstream critical loads

The following questions can help project developers understand how solar PV interconnection impacts project development:

- **Does the interconnection agreement allow for adding resilience?** An interconnection agreement governs the technical parameters of how a generation asset may connect to and operate with the utility electrical system. Interconnection agreements are mandatory, and the utility will not allow an asset to function until they have approved and verified the system implementation. These agreements were previously unique due to the limited instances of large-scale solar assets. Utilities are increasingly standardizing solar PV interconnection, as they become more common. Existing solar PV projects may be governed by agreements that did not contemplate future resilience applications, limiting what may be done without completing a new interconnection agreement and risking project delays.
- **Is the resilience project connected on the utility side of the substation transformer ("upstream") or downstream of the substation?** The primary interconnection decision that impacts the engineering design is whether the asset is tied to the bulk electric system on the utility side of the substation in an "upstream" configuration or tied to the distribution system on the DoD side of the substation in a "downstream" configuration. Figure 2 provides several example locations of solar PV interconnection points.[14]

[14] It is possible for large-scale PV systems to connect directly to the transmission system, but these systems are rare and beyond the scope of this report.

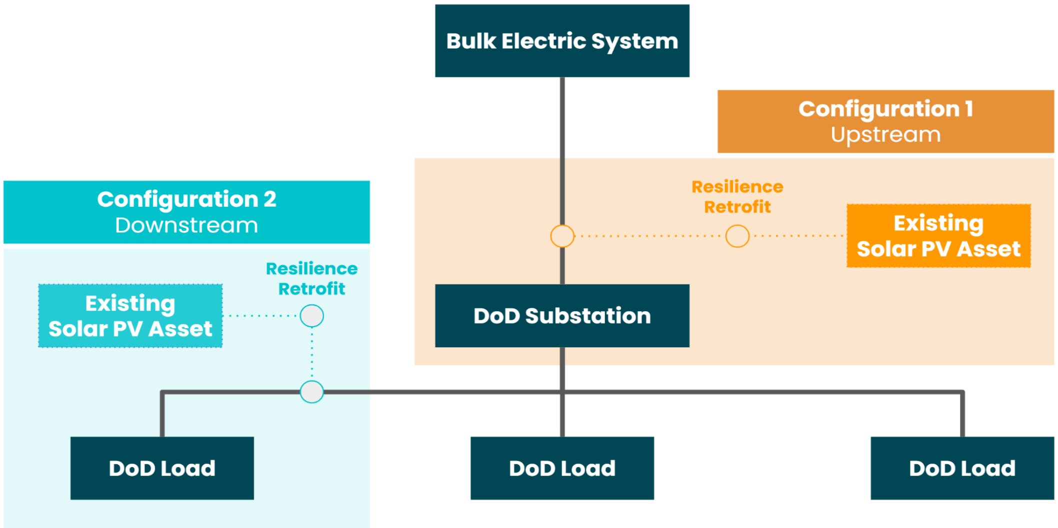

Figure 2: Upstream and Downstream Interconnection Points

There are several considerations related to the point of solar PV interconnection:

- The "upstream" option (i.e., Configuration 1) is used by many of the multi-megawatt, privately-owned solar PV systems located on military installations. The upstream configuration is preferable for energy resilience retrofits. Upstream interconnections require simpler and less expensive protection upgrades, whereas downstream systems (Configuration 2) require additional protection hardware to ensure the system doesn't backfeed the utility connection during an outage event and risk injuring utility repair personnel. Upstream interconnections also enable greater flexibility to serve critical loads at the military installation over time.
- The needs of an installation are dynamic since missions can come and go, change buildings, and/or change mission requirements. These changes may require corresponding changes to energy resilience hardware and controls. The specific feeders and loads served by upstream PV systems can be programmed and controlled at the substation level. Downstream PV systems, by contrast, must be controlled and programmed at system level, which provides less flexibility to address other feeders and loads as DoD missions expand or move. Upstream interconnections may also be more straightforward from a cybersecurity perspective (Section 5). Although downstream systems may be more costly to protect and program, the equipment required for them to connect to lower voltage feeders is less expensive than upstream connections.
- Energy resilience retrofits at sites with upstream connections are preferable to sites with downstream feeder connections - but both are technically feasible. Solar PV systems connected at the building level cannot typically be integrated into energy resilience projects - unless the resilience project is designed to serve only the building load. Instead,

building-level solar PV systems are treated as uncontrollable fluctuations in load from the perspective of an upstream energy resilience retrofit (Text Box 2).

Text Box 2. Existing PV at Marine Corps Air Station (MCAS) Miramar

MCAS Miramar has built two separate microgrids: a multi-megawatt microgrid that serves the entire installation and a smaller-scale microgrid that serves a single office building. In both cases, the base has worked to integrate existing solar PV systems into the microgrids. The installation-wide microgrid is powered by landfill gas, natural gas, and diesel generators. There are also 1.2 MW of distributed solar PV systems that are located within the islandable area and interconnected behind-the-meter at specific buildings. Although these systems are within the area served by the microgrid, they are not connected to the microgrid controller and cannot be directed to serve other loads during power outages. Instead, the 1.2 MW of PV systems are treated as variable loads within the microgrid service area. The building level microgrid is powered by a 230 kW solar PV carport system and battery energy storage (Faries, 2017). There is also a 30 kW PV system on the building's rooftop. MCAS Miramar is evaluating whether and how the existing 30 kW system can be retrofitted with additional controls and communications and integrated into the building-level microgrid (Klauber et al., 2021).

4.4 EXISTING DISTRIBUTION SYSTEM ARCHITECTURE

DISTRIBUTION SYSTEM ARCHITECTURE QUESTIONS	**DISTRIBUTION SYSTEM ARCHITECTURE** TAKEAWAYS
Does the substation have the capability to move power from one transformer to another?	Project developers should target locations where the solar is electrically connected to all substation loads.
How much control is needed to serve the priority load?	Project developers should target locations where the entire substation already has controls installed.
Is there communication infrastructure at the substation?	Project developers should target locations with communication infrastructure at the substation.
Can the existing electrical distribution system configuration accommodate the proposed retrofit?	Extending or reconfiguring an installation's existing distribution grid can add significant cost to retrofit projects. Retrofit projects that require little or no upgrades are more likely to succeed.
How much of the distribution system equipment must be configured for islanded operation?	Project developers should target locations with multiple, smaller substations to limit the devices needing configuration.

The following questions can help project developers understand how the existing distribution system architecture impacts project development:

- **Does the substation have the capability to move power from one transformer to another?** Some substations have multiple transformers. In some cases, the equipment necessary (e.g., switches and relays) to control the movement of power from one transformer to another may not be present in the substation. This may be a design decision to control costs, or to partition the substation capacity and reserve it for future use (e.g., additional load growth). If the solar PV system is connected to the transformer that is associated with priority loads, no additional equipment may be necessary. If the PV system is not connected to the transformer with priority loads, additional equipment may be required to enable power flow between the transformers and from the PV system to the loads.
- **How much control is needed within the substation to serve the priority load(s)?** Solar PV assets used for resilience will need to provide power to priority loads shortly after a power outage. The ideal situation is for any switching from grid power to the solar PV asset with storage to happen automatically through programmed logic controllers that can be remotely operated. This allows system operators to remain in a control center monitoring, and controlling if needed, the entire distribution grid in real time. Otherwise, system operators would need to travel to each location to conduct switching actions, causing a delay in backup power delivery to the priority loads. The need for control increases as the resilient power is directed toward a narrower portion of the installation distribution system. For example, deciding to serve one of ten feeders with the resilience retrofit would result in all ten feeders needing automated control hardware to ensure the load is directed to the right feeder. Alternatively, a solar PV asset and resilience retrofit solution large enough to power the entire substation will eliminate that requirement and reduce the control hardware investment required. Project developers should target locations where the entire substation already has controls installed.
- **Is there a communication network at the substation for the required controls?** Remote or automated controls are typically included in new substations because they increase safety and functionality. Including this functionality requires a communication network that increases project costs compared to a manually controlled substation. Manually controlled substations are more common since much of DoD's distribution infrastructure is decades old and control hardware is relatively new. Upgrading a manually controlled substation is costly and running new communication networks to a geographically isolated location is even more expensive. Not including these capabilities will reduce the ability of the system to provide power to other loads if the asset isn't large enough to power the entire substation. It is worth noting that adding communication capabilities to

substation equipment increases the potential for cyber attacks if the network doesn't include appropriate cybersecurity protocols (Section 5). Project developers should target locations with communication infrastructure at the substation.

- **Can the existing electrical distribution system configuration accommodate the proposed retrofit?** In addition to the point of interconnection (Section 4.3), the costs of integrating an energy resilience retrofit into an installation's distribution system will be driven by the size, electrical characteristics, and location of the proposed hardware. Changes to distribution systems take a long time to complete due to reviews by utility providers, regulatory agencies, and/or DoD technical stakeholders. Unless the project developer sees a clear financial benefit for making a change, or can find additional resources to support grid upgrades (Text Box 3), the configuration of the existing distribution system will dictate the type of energy resilience solutions that are feasible. Energy resilience retrofits are more likely to succeed in locations where little to no change to the distribution system configuration is necessary.

Text Box 3. Distribution Grid Upgrades for Existing Renewable Energy Generators

Existing renewable energy assets may not be situated optimally in relation to the substations they need to connect to or the critical loads they need to serve. Military installations may need to make significant investments in their distribution systems in order to include their existing renewable energy assets as part of an energy resilience solution. Otis Air National Guard Base, for example, is seeking to integrate an existing 1.5 MW wind turbine into a microgrid with a battery storage system and a diesel generator (Altman, 2020). The project required 3.5 miles of new electric distribution cable in order to connect the wind turbine to the microgrid. Otis ANGB worked with the 249th Engineering Battalion, Delta Company (Reserves) to install the distribution line as part of its training exercises. Together with labor contributed by other units, the in-kind labor saved $3 million in construction costs (Klauber et al., 2021). At Marine Corps Air Station Miramar, the installation received $5 million in DoD funding to build a 6.5 mile distribution line to connect the base to an existing landfill gas plant (Purtee, 2014).

- **How much of the equipment within the distribution system must be configured for islanded operation?** The protection and control devices in the distribution system (e.g., circuit breakers and relays) are configured to operate with the stable and consistent power provided by the grid. Solar PV and BESS inverters provide a wider voltage and frequency range during islanded operation than when connected to the bulk electric grid. This wider range can violate the protection device set points, causing those pieces of equipment to trip offline. As a result, the settings on any protection devices used for islanded operation will need adjustment to allow power to flow as intended. Depending on which parts of the distribution system are served by the assets, this may be a significant financial investment and will drive decisions about whether to power the entire distribution system or only specific parts. Similarly, each device may need to be controlled to ensure power is directed to the priority load safely. All of these controls may require communication networks as well, further increasing project costs if the communication infrastructure is not already in place. Retrofit projects that target locations with missions served by multiple, smaller substations will reduce the number of devices needing configuration and limit project cost.

4.5 EXISTING SOLAR & PROJECT SITING

EXISTING SOLAR AND PROJECT SITING QUESTIONS	**EXISTING SOLAR AND PROJECT SITING** TAKEAWAYS
How much land is available around the existing PV and the substation?	Project developers should target locations with sufficient land area for siting a BESS in close proximity to the substation and PV asset.
What inverters are used by the solar PV asset?	Project developers should target locations with AC inverters on the solar PV to increase flexibility in project siting.
What is the weight capacity of transit to the site?	Project developers should target locations with maintained road and bridge infrastructure suitable for truck load traffic.
Is water available for cooling or fire suppression at the site?	Project developers should target locations where water infrastructure or connections are available for projects that include certain types of battery storage.

The following questions can help project developers understand how existing solar and project siting impacts project development:

- **How is the existing PV sited in relationship to the substation?** The physical relationship between the PV system, the substation, and a battery storage system has implications for system efficiency and cost. The most efficient and least cost configuration is to install the battery in close proximity to the PV system and the substation. This would allow the PV system to provide direct current (DC) power directly to the battery for charging. An alternating current (AC) inverter would then be placed in between the battery and the substation to complete the connection. Many legacy solar PV assets are installed near, or in some cases surrounding, the substation, and there might not be sufficient space to site a battery nearby. If the battery is sited further away from the PV system and the substation, longer lines will be required, and the system may need an AC inverter between the solar PV and the battery. This configuration is less efficient because of multiple power inversions, and the additional equipment required is more expensive

- **What is the weight capacity of transit to the site?** An often-overlooked constraint during the planning process is the weight capacity of roadways, bridges, and other transit modes to the site. Some roads and bridges can be limited to very low capacities (e.g., 10,000 lbs) and in some cases maintained roads are not available for transporting the equipment to the ideal location. This reduces the size, and sometimes the amount, of systems available for the project developers to use in meeting the mission requirements. Heavier storage systems are often cheaper due to economies of scale and eliminating these options reduces the financial margins for developers. For example, lithium-ion BESS companies are starting to coalesce around 20- and 40-foot shipping container designs that may be too heavy for infrastructure in remote locations. Project developers should assess whether the proposed retrofit sites have roads and bridges suitable for truck load traffic.
- **Is water available for cooling or fire suppression at the site?** Some resilience retrofit solutions (e.g. lithium-ion batteries systems) require temperature control to maintain optimal performance and avoid fires or system damage. These systems typically use water for cooling and fire suppression. A site without water will require additional cooling and fire suppression equipment that will increase the cost, increase the land area required, and reduce the system efficiency due to parasitic energy loss. The installation could bring water infrastructure to the site, but that is typically expensive due to the geographically isolated locations of many DoD solar PV assets. Project developers should target locations where water infrastructure or connections are available.

4.6 INTEGRATING EXISTING GENERATION

INTEGRATING EXISTING GENERATION QUESTIONS	**INTEGRATING EXISTING GENERATION** TAKEAWAYS
How large is the solar PV asset compared to the load?	The size of the PV system compared to the priority loads will dictate system configuration. Smaller-scale PV systems will limit the size of load that can be served, and the duration of associated energy storage.
Can additional existing energy generation and storage systems complement solar PV?	Existing assets can provide stability for the islanded system and ensure long duration operational requirements are met.

The following questions can help project developers understand how integrating existing generation may impact project development:

- **How large is the solar PV asset compared to the load?** The size of the solar asset, the load that needs resilience, and the energy storage system must be aligned. A smaller solar asset (<5 MW) will limit which loads are serviceable by the PV, and limit the degree that the PV system can serve the load and charge a battery simultaneously. A solar PV asset that is significantly larger than the loads and storage solution creates an opportunity to use additional renewable energy for additional critical loads or to accommodate changes to load in the future. Even large-scale PV systems, however, will likely need to be integrated with other generation and storage assets in order to achieve the longer duration power outage targets established by the military services (Section 1.2).
- **Can additional existing energy generation and storage systems complement solar PV?** Two primary considerations related to other existing assets are their potential contributions to energy resilience, and their system interconnection.
    - *Diesel Generators.* DoD has historically relied on diesel generators to provide back-up power for critical missions. Military installations may have dozens to hundreds of existing emergency diesel generators on-site. Installations may also have existing power generation (e.g., CHP, power plants, fuel cells) and/or battery storage systems. Existing generation and storage can complement solar PV in several ways. They can provide additional capacity and flexibility to serve priority loads, extend the duration that the resilience system can perform, help ensure power quality for critical loads, balance the variable output of solar electricity, and support the voltage levels required to enable microgrid islanding (i.e., grid forming). These benefits must be balanced against the need for additional controls, communications, and costs required for each additional asset integrated with the solar PV system.
    - *Point of Interconnection.* As described in Section 4.3, the ability to integrate existing assets may also be constrained by their point of interconnection. Assets connected at the building level can operate in parallel with microgrids that are connected upstream (e.g., at the feeder level). The building-level assets, however, cannot be incorporated into the feeder-level microgrid to serve loads in other buildings without expensive voltage regulation equipment at each generator. Substation-level microgrids are similarly limited in the ability to use assets connected on one feeder to serve loads on another feeder. Micorgrids may use downstream assets for targeted load management, but this requires connecting the downstream assets to a network that is controllable from a central point (i.e. microgrid controller), which also adds additional expense and potential cyber vulnerability (Section 5).

5.0 CYBERSECURITY CONSIDERATIONS

Cybersecurity is a continually evolving field, where the threats mutate daily and the solutions race to keep pace. This constant state of change makes it difficult for organizations to create standards that are not outdated by the time they reach practitioners. Cybersecurity experts are deft at their craft, but they need clear direction on which threats are a concern and the level of protection needed before they can architect an appropriate defensive system. Nearly every cybersecurity solution is unique since the vulnerable equipment and systems are varied. Even so, there are several consistent considerations that will guide the cybersecurity provider toward a set of options that meet the priority load mission requirements. Similar to the engineering considerations, each section below starts with a question the project developer will need to understand, provides background information on the consideration, summarizes the most common options a project developer will find in the field, discusses their impact to the project design, and recommends a preferred direction if technically feasible.

5.1 BASELINE SECURITY POSTURE

BASELINE SECURITY POSTURE QUESTIONS	**BASELINE SECURITY POSTURE** TAKEAWAYS
What is the risk?	Determine the risks to mitigate before starting the project to avoid schedule delays and cost overruns.
What are the protection requirements?	Determine the appropriate level of protection for confidentiality, integrity, and availability to avoid bringing the OT system to a halt.
What are the vulnerable components?	Identify the equipment that is connected to a network or is accessed by equipment previously connected to a network.

The project developers must know the answer to several questions about the current status of cybersecurity for the existing solar PV, and on the installation, before architecting a solution. The following questions will help project developers understand the threats to the system and the mission requirements. Misunderstanding these basic questions will result in a project that may be vulnerable to cyber attacks, may cost more than necessary, or both.

- **What is the risk?** Cyber hackers range in their motives (ransom to system damage) and skill levels (novice-in-a-basement to a state-sponsored organization). Understanding the potential risks from these bad actors and determining which ones need mitigation is an important step for narrowing the cybersecurity solution space. Some of these risks are publicly reported, while others are more specific to the military and closely guarded. The risks range from phishing emails soliciting sensitive data to vulnerabilities in operating software granting the hacker access to control the system. Choosing to mitigate all risks is a never-ending endeavor that is likely more expensive than necessary. Selecting an acceptable risk threshold for an energy retrofit will help scope the effort required to add an appropriate level of cybersecurity. Making this determination after the project starts will lead to cost overruns and create unnecessary risks to the project's financial viability.

- **What are the protection requirements?** There are requirements for the amount of cybersecurity protection needed for the system components and for the entire system. Each component within the system may treat information differently and understanding those requirements will help the project developers select the right solution. The basic principles of requirements deal with determining the confidentiality (i.e., sensitivity of viewing information), integrity (i.e., guarding information against modification), and availability (i.e., ensuring access when needed) of information. Overdesigning a cybersecurity system for any one aspect may bring the system operation and maintainability to a halt, one of the possible goals desired by the cyberhackers.
- **What are the vulnerable components?** Identifying which components are vulnerable is another important step in narrowing the design scope of the cybersecurity solution. The most vulnerable components are typically those with a connection to the outside world (e.g., internet, cellular, radio frequencies) since they are accessible to anyone in the local area, or even the world. Components that are connected to these networked components are also vulnerable since an attacker uses those connections to reach further into the network. Even though a component is not connected to a network, it may still be vulnerable, especially when considering insider threat possibilities. Maintenance systems are often connected to the internet, allowing those systems to act as a bridge for cyber attackers looking for access to non-networked components. There's no predicting which component an attacker will target and project developers must review each component in the system for potential vulnerabilities.

5.2 NETWORK EQUIPMENT

NETWORK EQUIPMENT QUESTIONS	**NETWORK EQUIPMENT** TAKEAWAYS
How old is the equipment?	Older systems drive up project costs since more complex cybersecurity solutions are needed.
What ports and connection types are available on the existing equipment?	Equipment with multiple standard ports and connection types will be easier to protect due to the flexibility they

	afford.
Is the equipment and operating software proprietary?	Proprietary software and equipment may need to be replaced to enable proper protection.

The type of solar PV and substation equipment used in the retrofit are primary determinants for the type of cybersecurity features required to protect the system. While almost any system can be isolated from an external network and protected from cyberthreats, highly integrated components requiring complex cybersecurity solutions will lead to high implementation costs. The following questions can help project developers understand how network equipment impacts project development:

- **How old is the equipment?** Complex cybersecurity solutions and network integrations are common when using older equipment that was not originally designed with cybersecurity practices in mind. Those systems will typically support a flat network architecture where access to one system provides access to most, if not all, systems in the network. When coupled with a remote connection, it becomes increasingly difficult to isolate the systems and still provide the functionality required for operation. This would lead to changing the system equipment to support appropriate cybersecurity practices and increase project costs.
- **What ports and connection types are available on the existing equipment?** Cybersecurity systems require a variety of connections to monitor the equipment for suspicious activity and create separate, isolated communication networks while maintaining the equipment connections to conduct their function. Some pieces of equipment are not designed with cybersecurity in mind and may only have the necessary connections to conduct their functions. This lack of connections may hinder the project developer's ability to implement cybersecurity and may necessitate new equipment, increasing the project cost. An ideal piece of equipment would have multiple serial channels and ethernet ports available for the cybersecurity team to use. However, proper network architecture will be required to ensure these increased connections do not increase the system's vulnerability. Section 5.3 will discuss considerations regarding the risk of connections.
- **Is the equipment and operating software proprietary?** Equipment tied to energy systems is often company-specific and designed to perform a single function (e.g., control a switch to move when a condition is met). Most of the operational technology (OT) pieces of equipment are not designed with cybersecurity in mind since they were previously protected by physical and network isolation. The increase of connected devices increases the need for cybersecurity on those OT systems, including frequent software updates and patches. Project developers attempting to add cybersecurity to these systems will likely

encounter proprietary equipment connections and operating software that may require individual vendors to connect to the OT systems. Vendors connecting their own hardware introduces a potential vulnerability and needs to be mitigated by a customized cyber security architecture. If proper mitigation isn't feasible for the proprietary devices, then they may need to be replaced. In some cases, alternative equipment may not be available and the team would need to decide whether the risk of using the device is acceptable or if system functionality should be decreased by installing a more secure piece of equipment. These additional steps increase the cost of the project and reduce the financial viability.

5.3 CONNECTED DEVICES

CONNECTED DEVICES QUESTIONS	**CONNECTED DEVICES** TAKEAWAYS
What are the connection options for the device?	A device with more connections to the internet and other networks will have a greater cybersecurity risk.
Who wants to connect to the device and what does the connection allow?	Every user connection increases the risk and high levels of device control require intricate cybersecurity solutions.

The following questions can help project developers understand how connected devices impact project development:

- **What are the connection options for the device?** Many of the emerging technologies available for retrofitting existing solar PV for resilience have the option for remote connectivity and/or centralized control. These options can enable greater functionality for the system (e.g., demand response participation) and increase the system benefit for the end user (e.g., load/generation monitoring and management). These options can also increase the potential for cyberattacks since the previously isolated systems are now connected to a network with other systems. The cybersecurity risk is correlated with the level of network connectivity. An isolated network of system components without remote access will generally be more difficult to attack than assets accessible via the internet. For instance, many energy management and control systems (EMCS) use the cloud for storing and accessing data. Depending on the network architecture, these systems are more accessible to an attacker. Each level of network connection has different policies, or lack thereof, which impact the schedule and cost to integrate the emerging technology.
- **Who wants to connect to the device and what does the connection allow?** The cybersecurity considerations for device connections are not limited to just local control and monitoring. Project developers, maintenance personnel, manufacturers, integrators,

and a host of third parties will want to connect to the systems for their own purposes. Most of those connections will provide a web interface for personnel to view the data from anywhere (i.e., at work, at home, on a cell phone). Each of these connections requires careful consideration of what data is available and what control is granted to the user. As control and data availability for the internet connected user increases, the cybersecurity team will need to increase the complexity of the solution to protect the equipment. For example, allowing the user to review data about system cost savings will require a lower level of security than allowing the user to control how the assets function.

5.4 NETWORK CONNECTIONS

NETWORK CONNECTIONS QUESTIONS	**NETWORK CONNECTIONS** TAKEAWAYS
Is the system located inside or outside the DoD installation?	Systems located inside the DoD fence line can connect to the DoD network, which can reduce project capital costs.
Is the system connected to DoD networks?	Connecting to DoD networks may reduce infrastructure costs, but will lead to unpredictable costs and timelines associated with receiving approval through the RMF process.

The following question can help the project team determine how the network connectivity will impact the approval process necessary for the system to operate:

- **Is the system located inside or outside the DoD installation?** In general, resilience retrofits that are located within the DoD installation fence line can use the DoD networks to communicate between system components. Systems connected to a DoD network will reduce how much infrastructure the project team needs to develop as part of the project and minimize capital costs. Resilience retrofits located outside the DoD installation fenceline will need to provide their own networks and associated infrastructure to communicate between system components. Building a standalone network is costly if the resilience retrofit is geographically isolated from commercial networks or the terrain is difficult for construction equipment.
- **Is the system connected to a DoD network?** The network connections for the resilience retrofit and associated components will govern whether the project will need to comply with the risk management framework (RMF) or the cybersecurity maturity model certification (CMMC). Each of these processes are described in more detail in Appendix A and Appendix B, respectively. Systems that are connected to DoD networks are required to use the RMF process to ensure the resilience retrofit includes an appropriate level of risk mitigation when dealing with cyber threats. This process is long and must be completed for each resilience retrofit, with the potential exception for off-the-shelf equipment that is

already certified by the DoD as cyber compliant. Systems that are not connected to DoD networks and handle DoD information are required to use the CMMC process to ensure the entities involved operate their networks in a manner consistent with DoD cybersecurity standards. Since this requirement is at the network or company level, each resilience retrofit does not require a separate approval process as long as the existing certification is valid. This reduces the approval timeline and associated costs. Systems that are not connected to DoD networks and do not carry DoD information are not required to comply with the RMF or CMMC processes. Still, these resilience retrofits should consider the DoD requirements and follow some basic level of proper cybersecurity protections and hygiene as described in NIST Special Publication 800-171 (Ross et al., 2016). Given the nature of resilience, it is unlikely a system will not carry DoD information or impact the operations of a DoD system.

5.5 PERSONNEL KNOWLEDGE

PERSONNEL KNOWLEDGE QUESTIONS	**PERSONNEL KNOWLEDGE** TAKEAWAYS
Do the DoD stakeholders understand cybersecurity?	DoD stakeholders without cybersecurity knowledge will require additional guidance that increases the project cost without improving the system performance.
Are there relevant examples of cybersecurity projects to guide personnel?	Each cybersecurity system is uniquely complex and new simpler approaches that can be applied more broadly are gaining traction.
Who will maintain the cybersecurity system?	Failure to include life cycle management in the project budget will result in a system that doesn't function or costs significantly more than expected.

The following questions can help project developers understand how personnel knowledge impacts project development:

- **Do the DoD stakeholders understand cybersecurity?** Cybersecurity is a relatively new concept for the broader energy community as it shifts from focusing on clean energy to increasing the resilience of energy systems against man-made threats. The dynamic nature of cybersecurity has limited the number of DoD energy professionals with knowledge of industry standard cybersecurity practices, let alone cutting-edge approaches to protecting systems. As a result, many of the DoD personnel pursuing retrofit projects will rely on third-party firms or project developers for cybersecurity guidance on the right approach to meet mission requirements. Developing this guidance is time consuming and expensive, leading to increasing project costs that do not always improve the underlying system's performance. However, the process of implementing cybersecurity for a resilience retrofit will increase DoD personnel knowledge of the system and may increase their ability to maintain an appropriate security posture over time.

- **Are there relevant examples of cybersecurity projects to guide personnel?** The lack of technical depth in cybersecurity among most DoD stakeholders and scarcity of successful case studies decreases the potential of adding cybersecurity to existing networks. Entities who consider adding cybersecurity protocols to existing equipment may stop pursuing the concept due to the unknown path of implementation. The sheer number of different pieces of equipment (e.g., programmable logic controllers) without a standard protocol makes it difficult to find a "one size fits all" solution. The uncertainty surrounding the cost and schedule of this project approach can create financial risks that reduce project viability. There are approaches to simplify and standardize the cybersecurity solution (e.g. monitoring network traffic via packet capture, securing network entrance and exit points, and using data diodes and firewalls), but those approaches have not been documented in a complete case study users could follow for a resilience retrofit.
- **Who will maintain the cybersecurity system?** Most of the project will focus on designing a cybersecurity solution compatible with the equipment on the installation and the requirements for operating. The project developers will have in-house experts or they will bring on third-party experts to build the systems. The sustainment of the systems typically falls on DoD stakeholders who are not experts on cybersecurity, let alone have a working knowledge of the custom solutions needed to meet security requirements. DoD personnel in this situation need training from the project developers on how to maintain the system along with continuing support to prevent the system degrading over time. This solution relies heavily on DoD personnel learning on the fly. Alternatively, the project developer can provide support, or hire a third-party to do it, for the life of the project. This solution is expensive, but it will ensure the cybersecurity requirements are met.

NEXT STEPS

This report supports ESTCP Project # EW20-5330, *Retrofitting Existing Solar with Emerging Technologies [RESET]*. This report will support two additional lines of effort under the RESET project:

- **EAFB Feasibility Studies.** The EAFB Feasibility Studies are a series of resilience retrofit feasibility studies for a solar PV system at Edwards Air Force Base (EAFB). They focus on the areas of funding/financing, legal/contracting, engineering, and cybersecurity. They examine the feasibility of a RESET approach at EAFB in Kern County, California. EAFB is investigating whether and how to retrofit three 1 MW solar PV systems with resilience solutions under an existing PPA. The study also includes analysis of a go/no-go decision to pursue the resilience retrofit based on results from the feasibility studies.
- **DOD Policy and Program Recommendations.** The recommendations for DoD will be based on findings from the EAFB Feasibility Studies and interviews conducted during the formation of this report. The recommendations will use the guiding questions contained in this report as a framework. The recommendations will explore the steps that DoD policymakers and energy leadership could take to scale resilience retrofits.

APPENDIX

APPENDIX A: RISK MANAGEMENT FRAMEWORK

RMF QUESTIONS	**RMF** TAKEAWAYS
Is there a repeatable RMF process for solar and storage retrofit projects?	A tailored RMF process does not yet exist, but there are examples of other equipment approvals for reference.
How can RMF approvals impact the project timeline?	RMF packages require multiple, detailed and time intensive reviews before they proceed to the next step and any major error can result in needing to re-do a step.

The DoD uses the RMF to mitigate the cybersecurity risk of systems that are either owned by the DoD and/or connected to the DoD Information Networks (DODIN) (DoD CIO, 2014). The systems connected to DoD networks are typically similar to the "downstream" configuration shown in Figure 2 and are required to complete the process. The RMF is thorough, taking a considerable amount of time and effort before the retrofit system receives an authority to operate (ATO). Without an ATO, the system often cannot connect to a DoD network. It may be possible for certain systems to connect to the DODIN without an ATO, but those situations are extremely rare and the accepted process for unique systems is to pursue an ATO.

The following questions focus on gathering the latest information on the RMF process to determine how it may impact on the project development. The answers to these questions won't prevent the project from moving forward, but may increase the cost and timeline to complete it.

- **Is there a repeatable RMF process for solar and storage retrofit projects?** Many types of connected systems have gone through the RMF process, providing case studies for connecting computers and networking equipment to DoD's network. These case studies generically detail the steps necessary to receive an ATO, and can point the way to a repeatable process for equipment approval (see Figure 3). Retrofitting solar PV assets for resilience is a new concept, however, and case studies of resilience retrofits that have received an ATO through the RMF process do not yet exist. Energy project developers may be able to create RMF application packages for resilience retrofits by drawing on portions of the RMF process used for other equipment approvals. The lack of case studies will increase the amount of work required to complete the process, but it does not mean it is infeasible.
- **How can RMF approvals impact the project timeline?** The RMF process previously had six primary steps, each with multiple substeps (see Figure 3). Recently, NIST added a seventh

step, called “Prepare”, that sets the stage for the original six steps in the process and can reduce the difficulty of the other steps if thoroughly completed. Each of the seven steps in the RMF process has decision points with multiple Action Officers (AOs). The AO for each step reviews the data packages in their respective jurisdiction and decides whether the risk management approach is sufficient to move the package forward. If the package doesn’t properly mitigate the identified risks, then the project team will need to return to a prior step to address the issues. This rework is time consuming and may result in significant project delays. As the number of network connected devices increases, the queue of packages needing approval for each of the AOs also increases and leads to longer, unpredictable timelines for receiving approval. This uncertainty in the process timeline requires the project team to budget longer timelines and higher costs.

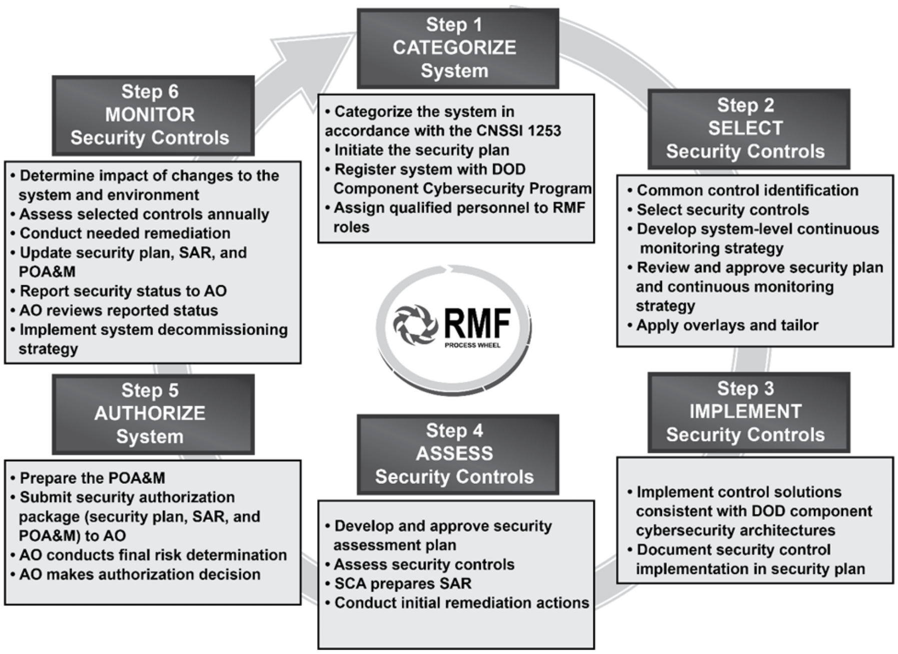

Figure 3: Risk Management Framework Six-Step Process[15]

[15] *Risk Management Framework for Army Information Technology*, Department of the Army (2019).

APPENDIX B: CYBERSECURITY MATURITY MODEL CERTIFICATION

CMMC QUESTIONS	**CMMC** TAKEAWAYS
How does the CMMC affect energy resilience project developers?	CMMC may be required for companies that handle DoD information and the process is applied once every three years for the company instead of per system.
Is there standardization to the CMMC process?	The process is new and still developing, but it is standardized and there is documentation on how to comply with the program.
Can the CMMC process be used for solar PV and resilience retrofit projects?	Solar and resilience retrofit projects, amongst many others, are allowed under the CMMC process assuming the information travels on a non-DoD network.
Who is held liable for cybersecurity breaches?	Liability for a cybersecurity breach is not yet tested due to the program newness and could pose a potential risk to project costs.

The following questions focus on gathering the latest information on the Cybersecurity Maturity Model Certification (CMMC) to determine how it may impact on the project development. The answers to these questions won't prevent the project from moving forward, but may increase the cost and timeline to complete it.

- **How does the CMMC affect energy retrofit project developers?** The CMMC is a new process based heavily on previous cybersecurity standards (e.g. NIST 800-171 and DFARS 252.204-7012). Defense contractors used the previous standards to mitigate the cybersecurity risk of systems owned by third parties that contain DoD information but are not connected to DoD networks. The solar PV systems connected to non-DoD networks are similar to the "upstream" configuration shown in Figure 2, but it is unclear whether energy companies will be required to comply with CMMC requirements. Companies considered part of the defense industrial base have to comply with the new process by 2025, or earlier if a government contract requires compliance. These companies are then accredited for three years to use DoD information before needing another accreditation review. This process differs from the RMF approach that requires approval for individual systems instead of company-wide approval. The CMMC process does not allow for the accredited companies to operate on DoD networks, which still require RMF approval.
- **Is there standardization to the CMMC process?** The CMMC process is in the early stages of implementation, but the goal is for it to become a standard and repeatable process where a company can predict the cost and schedule for becoming compliant. Unlike the RMF process that customizes cybersecurity to the product, companies must conform their

practices to over 100 controls to achieve CMMC compliance and achieve a basic level of cybersecurity. The process is intended to be simple and clear enough that one person can start the process and another can finish it without needing to start the process over. These goals are largely hypothetical, though, since only a handful of companies have completed the CMMC process due to the newness of the program. Still, the number of companies achieving compliance over the next four years will increase exponentially as the compliance deadline looms.

- **Can the CMMC process be used for solar PV and resilience retrofit projects?** According to preliminary CMMC materials, a CMMC-accredited company would be authorized to connect a solar PV asset and energy storage system to a non-DoD network without other approvals (USD(A&S), 2021b). This quicker approval timeline is feasible since the DoD and non-DoD networks are physically separated (i.e., air gap) and the project developer is only accessing the non-DoD network. This approach comes with some risk since the burden or protecting DoD information against cyberattacks shifts onto the project developer. Previously, the burden belonged to DoD since they approved each system and the operating protocols. The project developer needs to consider whether the significant decrease in timeline to operate the system, and thereby reduced project costs, is worth the potential drawbacks of protecting DoD information.
- **Who is held liable for cybersecurity breaches?** The CMMC approach is not yet implemented across DoD. This delay is due in part to the relatively recent revision of the process requirements and the time necessary to implement the controls for achieving accreditation. Because of the untested nature of the approach to a large number of real-world scenarios, project developers will likely identify several barriers to providing cybersecurity for solar PV and resilience retrofit projects. One of the uncertainties is how liability for a cybersecurity breach is treated. There could be fines or loss of accreditation and project developers must account for this risk when determining the feasibility of a project. This liability barrier, and other ambiguities, will bring the costs and timeline closer to those typically expected for the RMF process. Still, the repeatability of the process provides more benefits for non-DoD operations than one-off approvals currently available.

REFERENCES

Advancing Contracting in Energy Storage (ACES) Working Group. (2019). Energy Storage Best Practice Guide: Guidance for Project Developers, Investors, Energy Companies and Financial and Legal Professionals. Washington, DC: Energy Storage Association.

Akhil, A.A., Huff, G, Currier, A.B., Kaun, B.C., Rastler, D.M., Chen, S.B., Cotter, A.L., Bradshaw, D.T., & Gauntlett, W.D. (2015). DOE/EPRI Electricity Storage Handbook in Collaboration with NRECA. (SAND2015-1002). Albuquerque, NM and Livermore, CA: Sandia National Laboratories.

Altman, D.H. (2020). Hybrid Micro-grid with High Penetration Wind for Islanding and High Value Grid Services. (EW-201606). Alexandria, VA: U.S. Department of Defense Environmental Security Technology Certification Program (ESTCP).

Andrews, A. (2011). Federal Agency Authority to Contract for Electric Power and Renewable Energy Supply. (R41960) Washington, DC: Congressional Research Service.

Baxter, R. (2016). Energy Storage Financing: A Roadmap for Accelerating Market Growth. (SAND2016-8109). Albuquerque, NM: Sandia National Laboratories.

Baxter, R. (2018). Energy Storage Financing: Performance Impacts on Project Financing. (SAND2018-10110). Albuquerque, NM and Livermore, CA: Sandia National Laboratories.

Baxter, R. (2019). Energy Storage Financing: Advancing Contracting in Energy Storage. (SAND2019-12793). Albuquerque, NM and Livermore, CA: Sandia National Laboratories.

Beehler, A.A. & Evans, J.T. (2020). New Army REFoRM Initiative Will Help Army Installations Retain 50% of Energy Cost Savings. Army.mil.

Conger, J. (2018). An Overview of the DOD Installations Enterprise. Washington, DC. The Heritage Foundation.

Corfee, K., Karcher, M., Cleijne, H., Burgers, J., Faasen, C., Tong, N., Rickerson, W., Grace, R., and Gifford, J. (2010). Feed-in Tariff Designs for California: Implications for Project Finance, Competitive Renewable Energy Zones, and Data Requirements. Sacramento, CA: California Energy Commission.

Craig, B. D., Lane, R.A., Knoeller, S.L., Conniff, O.R., Fink, C.W., and Ingold, B.J. (2011.) Department of Defense Energy Handbook: Alternative and Renewable Energy Options for DoD Facilities and Bases. Rome, NY: Advanced Materials, Manufacturing and Testing Information Analysis Center (AMMTIAC).

Cramer, S., & Verclas, K. (2021). Private, State, and Federal Funding and Financing Options to Enable Resilient, Affordable, and Clean Microgrids. Washington, DC: National Association of Regulatory Utility Commissioners and National Association of State Energy Officials.

Crowell, C. (2020, June 29). Inside BlockEnergy's Military-Tested Microgrid and the Future of Distributed Renewable Energy. *Solar Builder.*

Defense Federal Acquisition Regulation Supplement (DFARS) Procedures, Guidance, and Information (PGI) 241.2 Acquiring Utility Services.

Elgvist, E., Anderson, K, & Settle, E. (2018). Federal Tax Incentives for Energy Storage Systems. (NREL/FS-7A40-70384). Golden, CO: National Renewable Energy Laboratory.

Elliott, K. (2014). AF's Largest Solar Array Celebrates First Anniversary. Lackland, TX: Air Force Civil Engineer Center Public Affairs

Endemann, B. (2019). Project Development Chapter 5: Incentives. In *Energy Storage Best Practice Guide: Guidance for Project Developers, Investors, Energy Companies and Financial and Legal Professionals*, 75–80. Washington, DC: Energy Storage Association.

Executive Order No. 13693, 80 Fed. Reg. 15869 (March 19, 2015)

Executive Order No. 13834, 83 Fed. Reg. 23771 (May 17, 2018)

Executive Order No. 14008, 86 Fed. Reg. 7619 (January 27, 2021)

Faries, R. (2016). Zinc Bromide Flow Battery Installation for Islanding and Backup Power. (EW-201242). Alexandria, VA: U.S. Department of Defense Environmental Security Technology Certification Program (ESTCP).

Feldman, D., Bolinger, M. & Schwabe, P. (2020). Current and Future Costs of Renewable Energy Project Finance Across Technologies. (NREL/TP-6A20-76881). Golden, CO: National Renewable Energy Laboratory.

Government Accountability Office (GAO). (2010). Defense Infrastructure: Department of Defense Renewable Energy Initiatives. (GAO-10-681R). Washington, DC.

Herrera, G. (2019). Military Construction: Authorities, Process, and Frequently Asked Questions. (R44710, Version 9). Washington, DC: Congressional Research Service (CRS).

Holmes, B. (2019. Project Development - Chapter 6: Offtake Agreements. In *Energy Storage Best Practice Guide: Guidance for Project Developers, Investors, Energy Companies and Financial and Legal Professionals*, 81–90. Washington, DC: Energy Storage Association.

International Finance Corporation (IFC). (2015). Utility-Scale Solar Photovoltaic Power Plants: A Project Developer's Guide. Washington, DC.

Internal Revenue Service (IRS). (2015). Private Letter Ruling 201543001. Washington, DC.

Internal Revenue Service (IRS). (2017a). Private Letter Ruling 201809003 - In Re: Request for Rulings under IRC § 25D. Washington, DC.

Internal Revenue Service (IRS). (2017b). Internal Revenue Bulletin No. 2017-7, Rev. Proc. 2017-19. Washington, DC.

Keightley, M. P., Marples, D.J., & Sherlock, M.F. (2012). Tax Equity Financing: An Introduction and Policy Considerations. (R45693). Washington, DC: Congressional Research Service.

Klauber, A., Cathcart, J., Shwisberg, L., Toussie, I., Adib N., Kelsey, F., Mitchell, S., Pecenak, Z., Stadle, M,. Rickerson, W., Pringle, M., Barrett, S., & Crites, J., (2021). Airport Microgrid Implementation Toolkit. Washington, DC: National Academies of Sciences.

Kleim, J. (2016, May 18-19). Renewable Energy Program Office. Presented at the Federal Utility Partnership Working Group (FUPWG) 2016 Spring Seminar, Cincinnati, OH.

Kleim, J. (2017, April 12). Resilient Energy Program Office: The Department of the Navy's Energy Resiliency Progress. Presented at the Federal Utility Partnership Working Group (FUPWG) 2017 Spring Seminar, Savannah, GA.

Kleim, J. (2019, December 10). Energy Security Programs Office (ESPO). Presented at the Association of Defense Communities (ADC) Energy & Water Forum, Washington, DC.

Koch, A.T. (2014). Rethinking State Regulatory Issues. In *Renewable Energy for Military Installations: 2014 Industry Review*, 6-10. Washington, DC: American Council on Renewable Energy (ACORE).

Kurnik, C. & Voss, P. (2020). Financing Microgrids in the Federal Sector. (DOE/GO-102020-8450). Washington, DC: Federal Energy Management Program.

Lacey, S. (2017, June 21). New Market Rules Destroyed the Economics of Storage in PJM. What Happened? GreentechMedia.com.

Logan, T. (2012). ESPC PPA Overview. Federal Utility Partnership Working Group Spring Workshop, Jekyll Island, GA.

McDonald, T. (2014). Procurement Landscape and Opportunities. In *Renewable Energy for Military Installations: 2014 Industry Review*, 15–18. Washington, DC: American Council on Renewable Energy (ACORE).

McDonald, T. (2016, December 2). Trump Transition and Sustainable Energy: Department of Defense Programs Provide Strong Foundation for Energy Independence. *Holland & Knight Government Energy Finance Blog.*

Mendelsohn, M. & Kreycik, C. (2012). Federal and State Structures to Support Financing Utility-Scale Solar Projects and the Business Models Designed to Utilize Them. (NREL/TP-6A20-48685). Golden, CO: National Renewable Energy Laboratory.

Narayanan, A., Knopman, D., Van Abel, K., Miller, B. M., Burger, N., Merrill, M. V., Rothenberg, A. D., Muggy, L., & Mills, P. (2019). *Valuing Air Force Electric Power Resilience: A Framework for Mission-Level Investment Prioritization*. Santa Monica, CA: Rand Corporation.

National Conference of State Legislatures (NCSL). (2016). Preparing for Duty, State Policy Options to Sustain Military Operations. Washington DC.

Niemeyer, L. (2018). Statement of Honorable Lucian Niemeyer, Assistant Secretary of Defense (Energy, Installations and Environment). Washington, DC: House Committee on Armed Services Subcommittee on Readiness.

Oueid, R.K. (2019). Microgrid Finance, Revenue, and Regulation Considerations. *The Electricity Journal 32*(5): 2–9.

Prehoda, E., Schelly C. & Pearce, J. (2017). U.S. strategic solar photovoltaic-powered microgrid deployment for enhanced national security. *Renewable and Sustainable Energy Reviews, Elsevier*, 78: 167-175.

Purtee, R. (2014). Miramar Landfill Gas Utilization Enabling the First Green Marine Corps Facility. Landfill Methane Outreach Program 17th Annual Conference and Project Expo, Baltimore, MD.

Rickerson, W., Wu, M. & Pringle, M. (2018). Beyond the Fence Line: Strengthening Military Capabilities Through Energy Resilience Partnerships. Washington, DC: Association of Defense Communities.

Rickerson, W., Brousseau, E., Pringle, M., Monken, J., Calvert-Rosenberger, T., Graul, J., & Barker, J. (2021). Regulatory Considerations for Utility Investments in Defense Energy Resilience. Washington, DC: National Association of Regulatory Utility Commissioners.

Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, Mark. (2016). NIST Special Publication 800-171 (Rev. 1): Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Washington, DC: National Institute of Standards and Technology.

Secretary of Energy Advisory Board (SEAB). (2016). Report of the Task Force on Federal Energy Management. Washington, DC.

Shah, C. (2011). Power Purchase Agreements. Federal Energy Management Program Alternative Finance Options Webinar.

State of Connecticut Office of Military Affairs (CT OMA). (2020). Annual Report Fiscal Year 2019-2020. Rocky Hill, CT.

Stockton, P.N. & Paczkowski, J.P. (2019). Strengthening Mission Assurance Against Emerging Threats: Critical Gaps and Opportunities for Progress. *Joint Forces Quarterly,* 95, 22-31.

Stoel Rives LLP. (2017). The Law of Solar: A Guide to Business and Legal Issues. (5th Ed.). Washington, DC.

Strahl, J., Paris, E., & Vogel, L. (2015, December 8-10) The Bankable Microgrid: Strategies for Financing On-Site Power Generation. POWER-GEN International, Las Vegas.

Tine, D. (2019). Risk Management - Chapter Two: Project Risk Insurance. In *Energy Storage Best Practice Guide: Guidance for Project Developers, Investors, Energy Companies and Financial and Legal Professionals*, 263-272. Washington, DC: Energy Storage Association.

U.S. Army Corps (USACE). (2021). DoD Renewable Energy Project Viewer. Washington, DC.

U.S. Department of the Air Force (USAF). (2015). Air Force Instruction 32-1062 - Electrical Systems, Power Plants and Generators. Washington, DC.

U.S. Department of the Air Force (USAF). Air Force Manual 32-1062 - Electrical Systems, Power Plants and Generators (2020a). Washington, DC.

U.S. Department of the Air Force (USAF). (2020). Air Force Policy Directive 90-17 - Energy and Water Management. Washington, DC.

U.S. Department of the Air Force Civil Engineering Center (AFCEC). Air Force Civil Engineer Energy Savings Performance Contracts (ESPC) Playbook. Lackland, TX.

U.S. Department of the Air Force Office of the Deputy Assistant Secretary for Environment, Safety, and Infrastructure (SAF/IEE). (2020). Resilient Energy Savings Resource Vault. Washington, DC.

U.S. Department of the Army. (2019). Risk Management Framework for Army Information Technology. (Department of the Army Pamphlet 25–2–14). Washington, DC.

U.S. Department of the Army. (2020). Army Directive 2020-03 - Installation Energy and Water Resilience Policy). Washington, DC.

U.S. Department of the Army Office of Energy Initiatives (OEI). (2014). Army Guide: Developing Renewable Energy Projects by Leveraging the Private Sector. Washington, DC.

U.S. Department of the Army Office of Energy Initiatives (OEI). (2019). Fort Detrick, Maryland Solar Energy Project Provides On-Site Generation, Supply Diversity and is Microgrid Capable. Washington, DC.

U.S. Department of Defense (DoD). (2020). Department of Defense Fiscal Year (FY) 2021 Budget Estimates: Office of the Secretary of Defense Research, Development, Test & Evaluation, Defense-Wide. (Defense-Wide Justification Book Volume 3 of 5). Washington, DC.

U.S. Department of Defense Chief Information Officer (CIO). (2014). Department of Defense Instruction 8510.01 - Risk Management Framework (RMF) for DoD Information Technology (IT). Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Sustainment (ASD(S)). (2018). Policy on Energy Savings Performance Contracts and Utility Energy Service Contracts. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Sustainment (ASD(S)), (2020a). Annual Energy Management and Resilience Report (AEMRR) Fiscal Year 2019. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Sustainment (ASD(S)). (2020b). Department of Defense Energy Strategic Plan. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Sustainment (ASD(S)), (2021). Annual Energy Management and Resilience Report (AEMRR) Fiscal Year 2020. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Environment and Energy Resilience (ASD(EI&E)). (2016a). Department of Defense Annual Energy Management Report (AEMR) Fiscal Year 2015. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Energy, Installations, and Environment (ASD(EI&E).(2016b). Guidance on Development of Energy Projects. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Energy, Installations, and Environment (ASD(EI&E)). (2016c). Installation Energy Plans. Washington, DC.

U.S. Department of Defense Office of the Assistant Secretary of Defense for Environment and Energy Resilience (ASD(EI&E)). (2017). Energy Resilience: Operations, Maintenance, & Testing (OM&T) Strategy and Implementation Guidance. Washington, DC.

U.S. Department of Defense Office of the Deputy Assistant Secretary of Defense, Energy (ODASD(Energy)). (2020). Alternative Financing for Energy Resilience Projects – Establishment of a Defense Energy Resilience Bank (DERB) for National Security. Washington, DC.

U.S. Department of Defense Office of the Inspector General (DODIG). (2016). Air Force Civil Engineer Center Management of Energy Savings Performance Contracts Needs Improvement. (DODIG-2016-087). Washington, DC.

U.S. Department of Defense Office of the Inspector General (DODIG). (2017). Navy Leases for Energy Production Projects. (DODIG-2017-109). Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)). (2018). Department of Defense Directive 4180.01 - DoD Energy Policy. Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition and Sustainment. (USD(A&S). (2019). Supplemental Guidance for the Utilities Privatization Program. Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition and Sustainment. (USD(A&S). (2021a). Department of Defense Contracting Officer's Representatives Guidebook. Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)). (2021b). Securing the Defense Industrial Base - CMMC 2.0. Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). (2012). Financing of Renewable Energy Projects Policy. Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). (2016). Department of Defense Instruction 4170.11 - Installation Energy Management. Washington, DC.

U.S. Department of Defense Office of the Under Secretary of Defense for Installations and Environment (USD(I&E)). (2005). Department of Defense Energy Manager's Handbook. Washington, DC.

U.S. Department of the Navy (DON). (2020). Installation Energy Resilience Strategy. Washington, DC.

U.S. Department of the Navy (DON) Navy Deputy Assistant Secretary of the Navy Energy Office 1 GW Task Force (DASN(Energy). (2012). Department of the Navy Strategy for Renewable Energy. Washington, DC.

U.S. Government Accountability Office (GAO). (2020a). Climate Resilience: DOD Coordinates with Communities, but Needs to Assess the Performance of Related Grant Programs. (GAO-21-46). Washington, DC.

U.S. Government Accountability Office (GAO). (2020b). DoD Utilities Privatization: Improved Data Collection and Lessons Learned Archive Could Help Reduce Time to Award Contracts. (GAO-20-104). Washington, DC.

U.S. General Services Administration. (2015). Procurement Guide for Public Utility Services: A Practical Guide to Procuring Utility Services for Federal Agencies. Washington, DC.

White House Office of the Press Secretary. (2012). Fact Sheet: Obama Administration Announces Additional Steps to Increase Energy Security. Washington, DC.