Army Report on Creating an Army Installations Test and Demonstration Program Using Commercial Technologies

REPORT TO CONGRESS

HEADQUARTERS, DEPARTMENT OF THE ARMY

March 2020

The estimated cost of this report for the Department of Defense (DoD) is approximately $10,400 for fiscal year 2020. This includes $100 in expenses and $10,300 in DoD labor. Report cost estimate 3-59E3F2F

Army Report on Creating an Army Installations Test and Demonstration Program Using Commercial Technologies

This report is in response to HASC report 116-120 on H.R. 2500 section XXI of the National Defense Authorization Act for Fiscal Year 2020. The report states: "The committee understands that the Army is seeking to integrate innovative technology into the management of installations to promote safety, increase efficiency, lower costs, and improve the quality of life of service members and their families. The committee notes that there are barriers that make it difficult for the Army to test new technologies that could further these goals. Accordingly, the committee directs the Secretary of the Army to provide a report to the House Committee on Armed Services by March 1, 2020, that addresses the feasibility of creating a commercial technologies test and demonstration program." The report further asks that the response include: 1) a process to identify commercially available technologies that improve the performance of infrastructure systems, the provision of base operations services, communications, safety, traffic management, energy use, time management, and related services that are available for testing on military installations, 2) a framework for identifying potential risks associated with remotely monitored systems, and how to mitigate those risks, 3) a methodology for assessing potential cost savings over the life cycle of the technology; and 4) barriers to implementing a solution.

Initial Findings

Technology is pivotal to supporting readiness and modernization, increasing resilience, promoting safety, increasing efficiency, lowering costs, and improving the quality of life for service members and their families. The Army spends over $17B per year to sustain and improve Army installations. Past, incremental approaches to modernizing Army facilities are increasingly inadequate given the pace of technological change and specifically the deployment of "internet of things" (IOT) devices that are integrated into "smart" buildings, resilient micro-grids and connected infrastructure. The Army would benefit from a dedicated, data-driven innovation effort for installation modernization, keeping pace with broader Army modernization efforts, and modeled on similar efforts elsewhere in the Department of Defense. This report outlines the parameters for such a solution.

Based on an assessment of past practices and ongoing initiatives, a program to integrate innovative commercial technologies onto Army installations is feasible. When aligned with Army missions, coupled with modernization, readiness, and reform priorities, innovative technologies can create a wide range of attendant benefits, such as enhanced recruitment and retention of Soldiers which, when factored into a cost-benefit analysis, increase the value of any given technology. While some barriers to deploying technology do exist, the best path to overcoming these barriers involves demonstrating the contributions that any given technology makes to one or more Army priorities in the areas of readiness, modernization, reform, or meeting the needs of Soldiers, families, and Army civilians. There is great promise in leveraging Internet of Things (IoT) technologies to give Army leaders better visibility of installation operations and to support data-driven analytics for enhanced decision-making.

Army Report on Creating an Army Installations Test and Demonstration Program Using Commercial Technologies

"Smart" connected devices supported by artificial intelligence offers the potential to establish proactive responsiveness, thereby increasing the efficiency and the resilience of installations. Unfortunately, these devices, if not properly secured, have potential to create cyber vulnerabilities that would-be adversaries could exploit. Cyber security must be integral to all systems deployed on Army installations. The Army acting alone cannot substitute for actions best performed by other Federal agencies such as the Departments of Energy or Transportation. From the public policy perspective, a broader Federal consortium could drive the uptake of innovative technologies at greater scale.

The Department of Defense has successfully managed technology test and demonstration programs for many years across a range of technologies, reducing costs and enhancing mission effectiveness. Two examples having a direct correlation to the installation management portfolio are the Strategic Environmental Research and Development Program (SERDP) and the Environmental Security Technology Certification Program (ESTCP). These two programs, while successful are narrowly focused on basic and applied research for environmental and energy applications. They do not encompass the full range of technologies needed to advance Army installations at the rate necessary to meet current and future requirements.

The Army has made some initial inroads with "smart" technology exploration for its installations, yet needs more. This past year, the Army used advanced data analytics to develop and test a number of scenarios for Army infrastructure investments. In 2019, the Army executed a partnership with the Marine Corps for an autonomous vehicle (AV) pilot at Joint Base Myer Henderson Hall. Following on that, Fort Carson will host an AV pilot that will test transporting troops on post. On the drawing board is a pilot to create a "smart" child development center with sensor technology to monitor facility usage, improve safety, enhance security, maintain accountability, and explore caregiver behavior interactions.

In May 2019, the Army held an Industry Day that provided a showcase of Army requirements. The event attracted over 350 participants from more than 80 companies, academic institutions, and Federal laboratories, demonstrating the significant interest in synchronizing to meet these evolving issues. These pilot projects and the industry day represent the Army's initial efforts to explore existing technology solutions performed in an installation setting. Together, they demonstrate the potential for partnerships with private industry.

Army Report on Creating an Army Installations Test and Demonstration Program Using Commercial Technologies

Background

The 2018 National Defense Strategy states that the homeland is, "no longer a sanctuary". Installations, as the initial maneuver platforms for the Army, offer targets that an adversary could attack in order to disrupt or delay the Army's ability to mobilize and deploy forces. The Army's war-fighting concept defines a Strategic Support Area, where installations reside, as part of the battlespace, acknowledging that they should anticipate disruption and attack.

The Army has undertaken a multi-year "installations of the future" (IoTF) effort to examine installation performance and develop the insights to shape the strategic direction of the installation management enterprise. The effort started in 2017 using the same twelve global trends that the Army's uses to assess its future operational environment. Those trends included; climate change/resource competition, economic rebalancing, demographics/urbanization, collective intelligence, increase in human performance, human computer interaction, technology/engineering and manufacturing, robotics, cyber/space, artificial intelligence, big data, and power generation and storage. The Army also gained knowledge of the advancements of "smart cities" initiatives across the country through interactions with cities investing in smart technology, the National Institute of Standards and Technology and industry events. This research led to a categorization of three main factors driving the need for change.

The nature of threats faced by installations has evolved and increased. The Army must anticipate and prepare for the disruption of all activities on our installations, particularly those related to mobilization and deployment. Threats include cyberattacks on energy services, information operations targeting soldiers and family members, and unconventional kinetic attacks (drones) on key infrastructure such as ports, airfields, and rail.

The Army has advanced a new operating concept, changing the "battle space" and creating new demands on installations. There are significant new requirements placed on Army installations serving as initial maneuver platforms in the Strategic Support Area of Multi Domain Operations (MDO). This means installations are no longer isolated from the operational theater. In the MDO framework, Army installations are part of the Strategic Support Area. These platforms, located in the homeland, are catalysts for readiness and Army must operationalize them to meet warfighting requirements. The ability to generate, sustain, deploy, and operate the force in a secure environment is essential. The character of conflict is changing and expanding to include many forms of kinetic and non-kinetic threats requiring both material solutions and increasingly, knowledge based or non-material solutions.

Technology has changed. Technology is both a threat and an opportunity. Emerging "smart cities" technologies offer opportunities to modernize installations, promote resilience, and increase cost-effectiveness. The Army's future soldiers are growing up in "smart cities" and will

increasingly expect Army installations to provide similar internet-enabled services. The Army has an opportunity to lead the American homeland advancement of "smart" technology through implementation and integration in its communities.

The Army recognizes the power of IOT technology applications and their role in installation management. To elaborate on the Industry Day event discussed above, Army has developed sixteen IOT (sensor-driven) pilots that are ready for execution with industry, pending availability of funding:

- Perimeter access control, linear sensing – enhances security, reduces manpower and need for physical barriers
- Smart Child Development Centers – provides visibility for safety, security, building operations, and human interactions
- Modernized master planning – allows community planners to digitally predict physical impacts and costs for physical structures
- Digital twin for energy and water – provides for improved operations, resilience and "what if" scenarios
- Optimization of space utilization – analyzes space usage and provides data for stationing decisions
- Building fault analytics – monitors building systems and provides data for maintenance
- Real-time facility control analytics – controls and integrates building systems for enhanced response and planning
- Automated facility assessments – uses technology such as drones to monitor changes in structures and environmental conditions
- Frictionless entry – eliminates individual stops at the front gates for cleared personnel, enhancing security, reducing manpower and improving quality of life.
- Computer-aided dispatch and traffic monitoring – assists emergency dispatch for first responders
- Utility monitoring – connects utility monitoring systems for performance improvement
- Tactical vehicle micro smart grid – integrated installation and tactical energy for increased resilience
- 5G infrastructure utility energy service contract – tests top secret 5G capability in a controlled environment to transmit data
- Integrated sensors – tracks and integrates building environment data; CO2, temperature, occupancy rates, sound anomalies
- Autonomous vehicles – personnel and equipment transportation, environmental sensor collection
- Barracks/building analytics – full building automation and usage integration

Army has developed and prioritized these pilots to test existing technology in an installation setting to create a "smart installation" ecosystem. The prioritization focused on three criteria:

ease of implementation, integration into existing engineering, and return on investment. Upon availability of resources, acquisition vehicles are in place for rapid connection with industry.

Identifying commercially available technologies for installation capabilities

An Army test and demonstration program for smart city technology must align with the functions required to operate within the Strategic Support Area, and must improve the performance of infrastructure and/or enhance the delivery of installation systems and services. Such a program should begin by identifying commercially available technologies, testing them, and if successful, integrating them across the enterprise.

One lesson learned from the Army Industry Day in 2019 was that much of the knowledge needed to create or transform technology for secure and smart installations exists within the commercial market space. The industry day event demonstrated that there was ample interest in private industry to collaborate with the Army and configure their technology to the Army's requirements. When screening technology, Army will assess:

- **Alignment to Mission.** Emphasizing installation's support of specific Army priorities and mission requirements.

- **Support to Personnel and Community.** Provide Soldiers and civilians flexible work and lifestyle options that drive effective execution of the mission while maintaining/improving the overall quality of life that pertains to the all-volunteer Army.

- **Modernize the Infrastructure.** Utilizes prototypes to test smart capabilities, realize transition costs, enhance cost-effective and efficient operations, and inform implementation plans for enterprise adoption, ultimately providing total domain awareness of assets, systems, and services of the SSA portfolio.

- **Enable Information Sharing.** Build connectivity between facilities, systems, and services between installations and echelons of command by creating the foundation of a data-driven organization. This must also encompass partnership and synergy where innovation and intersection with private sector service providers occur.

- **Deliver Return on Investment.** Articulate a business case for installation modernization, providing standards, and cost-benefit analysis of capabilities, that facilitates scaling across the enterprise and provides a means to program existing resources more effectively.

There are multiple avenues for Army to reach out to industry and academia to offer opportunities for collaboration. Using a Request For Information (RFI) is one such avenue that has proven successful when coupled with an Industry Day. Setting the stage, Army released the 2019 RFI with specific use cases and asked industry to respond with interest and proof of supportability.

Upon review and adjudication of industry proposals, Army then invited industry partners to attend the industry day. From this, requirements were further refined to the point that an eventual formal acquisition process could be started.

Another avenue to pursue are partnerships with communities testing smart technologies for their own use. For example, Army installations have local mutual aid agreements with surrounding communities to support each other in the provision of fire, police and other emergency services. Both communities could use the same smart technologies to create a shared region-wide level of situational awareness and by extension, make effective use of constrained assets. Such regional approaches are of increased importance given that 70% of soldiers and their families live off base. This summer, Fort Carson Colorado in concert with the City of Colorado Springs, University of Colorado Boulder, and the non-profit organization US Ignite, will pilot the use of an autonomous shuttle vehicle to evaluate options for addressing community wide transportation issues. With the vehicle operating on the installation, the project will explore the use of data, and data sharing among the different partners with an emphasis on achieving synergies with next-generation transportation platforms like ride-hailing, micro-mobility and last mile connectivity.

The Army is also working with other Services on partnerships that could benefit the Department of Defense. Last year, the Olli autonomous vehicle operated at Joint Base Myer Henderson Hall. Olli was a collaboration between the Army, the Marine Corps, the Federal Department of Transportation, the State of Virginia, the Northern Virginia Regional Commission and Local Motors, which manufactured the vehicle. Of note, the vehicle made extensive use of many dual-use technologies pioneered in military laboratories such as additive manufacturing, robotics and advanced sensors. A second phase, when funded, will extend the initial pilot and run an autonomous shuttle off post and across public roads to and from the Pentagon. A third phase would further allow the shuttle to connect with major transportation hubs across Arlington County to improve transportation options for employees and visitors.

While there are several avenues for external collaboration and partnerships, one critical function expected in all future efforts is dedicated attention to data collection, security and analysis. All future IOT technologies will generate data for aggregation, analytics, and potential use in machine learning and artificial intelligence applications. Army has begun the development of a technology referred to as Virtual Testbed for Installation Mission Effectiveness (VTIME) to perform this critical function. Army intends VTIME to provide the installation commander, an intelligent installation control center of the entire installation to enhance the decision process affecting resilience and readiness based on accurate data. When applied between installations as well as across the enterprise, it simultaneously can optimize resources by improving data standards for delivery allowing multiple vendors to supply synchronized solutions. Part of this effort involves the creation of a “digital twin” for Army installations. A digital twin is the digital replica of a real physical environment that is developed and built using data collected from sensor and IOT devices. Once created, such a twin opens the possibility to a wide range of modeling, simulation and training activities.

Army Report on Creating an Army Installations Test and Demonstration Program Using Commercial Technologies

Considering potential risks

When embarking on a demonstration and pilot program regarding deployment of commercial technologies on Army installations, two broad categories of risk are involved. The first set of risks, which are relatively well known, involve those risks inherent with the development, testing, acquisition and fielding of any new technology. The second category of risk involves those risks associated with enemy attack and/or exploitation of a deployed technology given the new threat environment. Apart from these two categories, there is also the risk of status quo. By doing nothing, installations will fall behind technologically; facilities will not keep pace with Army modernization efforts, resilience will degrade, and readiness will suffer.

Acquisition Risk. The DOD defines risk, in the context of an acquisition program as future uncertainties relating to achieving program technical performance goals within defined cost and schedule constraints. Defined by (1) the probability of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur. For the purposes of this report, discussion will center on technical, cost, schedule, and business risks.

Technical risk focuses on whether a given product or technology will fail to perform as intended or to a given set of requirements. Adjustments and adaptations generally occur in piloting and early deployments of technology. In general, the Army should refrain from being the "first-mover" on technologies that are primarily civilian in nature. Instead, the Army would expect industry to have addressed the technical factors through their own research and development programs, moving a given technology to, or close to full commercialization. For such technologies, the Army's role is to provide the real world test environment to apply industry products in an installation setting. The Army may be willing to accept higher levels of technical risk for technologies that are more military in nature, such as defense systems to protect against drone incursions.

Cost risk relates to the probability of losses due to cost overruns. A given product or technology could prove technically viable but exceeds established cost allowances or is unable to produce the anticipated benefits. Cost risk is best managed through appropriate terms and conditions contained within the formal agreement establishing a given pilot program.

Closely associated with cost risk, is schedule risk, or when a pilot program does not reach its objective before the pilot completion time, leading to cost overruns and/or non-performance. The Department has a number of legal templates that it will apply to any demonstration program with the aim of reducing or eliminating any risks associated with cost overruns and/or schedule extensions.

Business risk considers the overall viability and financial health of commercial entities entering into partnerships with the Army. The intent is avoiding pilot programs sponsored by companies

with a risk of insolvency, forcing them to abandon the program, and in turn creating either upkeep or disposal costs to the Army. To address this risk, Army will incorporate mechanisms that consider entity financial posture and ensure that would be partners have sufficient assets to complete any demonstration program.

Individual technology pilots would also follow the Army's Risk Management Framework principles described in Department of Army Pamphlet 25-2-14, Risk Management Framework for Army Information Technology, April 2019.

Finally, while harder to define, is behavioral/cultural risk that a given technology, even if it performs as intended and within cost parameters, may be found unsuitable due to lack of compatibility with existing Army practices. Anticipating and factoring in resistance to change is a part of any technology demonstration. Indeed, some technologies have the explicit intention of disrupting sub-optimal processes. The key to overcoming any cultural or organizational resistance will be having the support of local garrison and installation leadership. It is clear from past efforts that a top-down approach that does not include the full support of local installation leaders and Army communities is unlikely to achieve intended results. It is critical that Army choose pilot site installations that endorse the technology insertion and fully support testing. Ideally, this support will extend from the senior mission commander through to the front-line installation maintainer. Additionally, successful pilot programs require some degree of community education and engagement in order to increase chances of adoption as well as to get vital feedback necessary for technology improvement and/or fielding.

Adversary Risk. The 2018 National Defense Strategy gives a clear outline that the new era of global competition directly involves Army Installations. Included in this document is the phrase "The Homeland is no longer a sanctuary" which speaks directly to the need to prepare for attacks here in the continental United States. It is a matter of public record that Russia, North Korea and other state actors have conducted cyber intelligence on domestic energy systems and have engaged in influence operations to affect U.S. domestic public opinion. The threat of such actions specifically directed at DOD installations, facilities, and personnel, are a factor in any technology demonstration program and steps must be taken to ensure that a new technology does not create vulnerabilities or in some way provide an advantage to an adversary.

Any technology deployed onto an Army installation could be subject to attack or exploitation by a future adversary. Technologies that may be appealing from a commercial or convenience perspective may be unsuitable for use on an Army installation. For example, many corporations and public entities use smart-building technologies to report in near real-time, energy and water consumption, power generation and/or parking lot occupancy. While such technologies are appealing, an adversary could use such information to gain harmful insights into Army operations and deployments.

Guarding against adversary risk will be difficult. Essentially the Army will need to employ existing IT systems risk management framework to all IOT enabled devices. Additionally, Army will apply standard counter-intelligence practices and reviews of supply chain integrity to any technology that could give a potential adversary control over Army systems.

Finally, while not captured neatly into either category above, an expanding set of natural events pose a threat to installation operations and constitute an additional area of risk. An increase in severe weather events driven by climate change are leading to a range of adverse impacts on the Army. These impacts include destruction of infrastructure through more frequent and intense tornado and rain events, water restrictions due to drought, and the need to curtail training for wildfire prevention. In this context, advanced technology becomes a tool for predicting and preparing for natural disasters. The development of smart micro-grids and on-site energy production will build resilience. The need to adapt to a changing climate will create opportunities through construction techniques for integrated infrastructure, transportation, and utilities with smart sensors.

Return on investment: cost savings and non-monetary benefits

Any test and demonstration program will include a cost-benefit analysis of expected returns to the Army. This analysis will be in accordance with the guidance and approach outlined in the Army's Cost Benefit Analysis Guide, as prepared by the Office of the Deputy Assistant Secretary of the Army (3rd Edition, V3.3, 21 January 2020). Such an analysis must include, but is not limited to, a financial return on investment.

Technology has the potential to reduce sustainment and maintenance costs, as well as associated human capital expenses. Army installations represent an over $440B in property plant replacement value and have an annual operating budget in excess of $21B. Despite this latter amount, Army has underfunded facility maintenance to focus on modernization resulting in a growing backlog of unmet requirements. Technology insertion that provides an efficient, autonomous, and/or real-time assessment of facility and infrastructure performance to identify just-in-time, predictive, and scheduled maintenance for major pieces of equipment has the potential to shrink that gap and allow the Army to target investments for greatest impact.

Readiness is one of the Army's three stated priorities, and an important consideration for return on investment. Technologies in a test and demonstration program must include measures related to supporting a given installation's ability to generate readiness and achieve its stated mission. Specific areas that contribute to readiness include improvements in training, safety, security, warfighting operations, power projection, maintenance and quality of life.

Resilience, in the context of an Army installation, is the ability to quickly recover from a shock and maintain operations. Following the discussion above on risks, resilience is crucial in the current environment of constant attack. A test and demonstration program must clearly include

an element that measures whether the technology enhances the installation's ability to protect and recover from an adverse event, whether manmade or from natural causes.

Looking to the future, the Army must consider the contributions that any tested technology has on the quality of life experienced at an installation, and whether that technology influences the recruitment and retention of current and future soldiers. Communities around the world are developing "smart spaces" that improve the delivery of public goods and services, provide convenience and/or save time. The Army must offer similar environments. Smart installations will be a more appealing environment to work and live for the future Solider.

Barriers/proposed solutions

Deploying IoT technologies on Army installations presents some unique challenges not faced in the past. These technologies represent a merger between information technology and operational technology. Further, the rate of technology evolution in this domain exceeds the rate of culture or behavior evolution. This duality challenges existing governance rules and funding mechanisms designed in an industrial era and set up for one or the other type of technology, but not for both or for their complimentary inclusion. Existing Army acquisition processes exist for delivery of a material solution, not the coherent delivery of both materiel and knowledge solution across the enterprise. In some cases, a proven technology paired with a new or emerging technology complicates the allowable funding source. Data collected from certain IoT devices could have wider applicability and could include an expanded universe of partners. For example, building occupancy data adds value for infrastructure master planners, as well as emergency responders, energy managers and even human resource specialists. This complicates responsibility for covering the costs of testing and deployment. Finally, IoT technologies connect installations to surrounding communities in new ways creating new possibilities for public private partnerships.

Allow for use of operations and maintenance, in lieu of research and development funds. Current authorities provide guidance on the use of funds for specified activities. Operations and maintenance funding may be appropriate to pilot physical technologies and infrastructure, but separate funding streams are required to develop the capability to aggregate data and build integrated AI capabilities upon this data. Currently, research and development funds are required to develop data aggregation tools and analytics capabilities to integrate successful pilot technologies into an effective "smart installation". A solution to this issue would be a narrow statutory exception that allows the use of operations and maintenance funds for integration evaluation in installation technology test and evaluation projects. This would allow more flexibility to test and integrate existing technology for a holistic approach to analytics and improved processes.

Congress has authorized Other Transactional Authority (OTA) for the purpose of research, development, testing, evaluation, piloting/prototyping innovative solutions. One example of such a vehicle is the Consortia for Energy and Environment and Demilitarization that could

accelerate the assessment of selected private sector technologies. Congress could further enhance the OTA capability by clarifying the use of operations and maintenance appropriations for pilots.

Remove barriers for Army Lab Partnerships. The DoD laboratories have a unique ability to accept project order funds to perform work from a multitude of customers. This allows them to accept a variety of work with a variety of funding sources and take up to two years obligating those funds. There is a caveat that the servicing organization, often a laboratory, must retain no less than 51% of the funding "in house" to perform the work. This provision may make sense for early stage or basic research on technologies primarily military in nature. Yet this restriction can impede the rapid advancement of technology, particularly when conducted through a partnership involving large-scale prototype activities. A possible solution would be to require a lesser amount for pilot installation technologies efforts. This would inherently provide the requiring and serving organization more flexibility in development of installation based prototypes and pilot projects with other technical organizations.

Expand Authorities for City partnerships. Congress provides funding for DoD's Office of Economic Adjustment (OEA). The intent is to assist communities negatively affected from base realignments and closures. Congress recently expanded OEA's authorities to include energy resilience projects. Congress could consider a similar approach in regards to smart technology applications that mutually benefit the Army and the supporting communities.

Incentivize private industry to bear more demonstration risk. There are limited resources available for installation technology innovation, and those resources understandably compete with other Army priorities. "Smart city" technologies are a growing business sector for the private industry. Informal discussions with industry leaders indicate there is an interest in using Army facilities to test new technologies in a controlled environment, outside a laboratory. With the appropriate statutory authorities, the Army could establish a limited incentives program with private industry. Such an arrangement would shift risk of investment to the private sector, preserving Army resources for other priorities.

Conclusion

Smart technology is flooding the market both inside and outside the fence, it is cheaper than ever before and it achieves ROIs that matter. Concurrently, current and future soldiers expect to live in a technology-enabled environment. For the Army to succeed in its key priorities of readiness, modernization, reform and improved quality of life, it must have modern, "smart" and resilient installations. Such installations must be able to operate in a contested environment while simultaneously providing enhanced public goods, services and conveniences comparable to, and compatible with "smart cities" initiatives. The creation of a dedicated commercial technologies test and demonstration program, appropriately managed for risk and return, could advance the Army's interests in this regard.