**EW22-7299 Energy Management and Information Systems (EMIS) Technology Transfer**

**Guidance for Implementing Smart Building Data Analytics**

Building Technology and Urban Systems Division

Lawrence Berkeley National Laboratory

and

Construction Engineering Research Laboratory (CERL)

U.S. Army Corps of Engineers

Acknowledgements

This work is supported by the Assistant Secretary for Energy Efficiency and Renewable Energy, Building Technologies Program, of the U.S. Department of Energy under Contract no. DE-AC02- 05CH11231. The authors wish to acknowledge Brian Clark, Jason Rodriguez and Robert Renz for their guidance and support of the research, as well as the suggestions from Xiaohui Zhou and Scott Hackel at Slipstream. We are also grateful to the team at Fort Cavazos, Texas, for their support in the planning, review, and outreach phases of the development, and Michael Chipley of the PMC Group LLC for help with the development of the cybersecurity section.

Disclaimer

This document was prepared as an account of work sponsored by the United States Government. While this document is believed to contain correct information, neither the United States Government nor any agency thereof, nor The Regents of the University of California, nor any of their employees, makes any warranty, express or implied, or assumes any legal responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by its trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or The Regents of the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof or The Regents of the University of California.

Table of Contents

[**1. Introduction** 9](#_Toc180673578)

[Background 9](#_Toc180673579)

[Purpose 11](#_Toc180673580)

[Applicability 11](#_Toc180673581)

[Relationship to existing policies and guidance 12](#_Toc180673582)

[Audience 13](#_Toc180673583)

[**2. EMIS Architecture Options** 14](#_Toc180673584)

[Option 1: EMIS lite 17](#_Toc180673585)

[Option 2: EMIS as a UMCS add-on 18](#_Toc180673586)

[Option 3: Cloud EMIS with configuration changes only 19](#_Toc180673587)

[Option 4: Cloud EMIS with software changes 20](#_Toc180673588)

[Option 5: Cloud EMIS with hardware changes only 21](#_Toc180673589)

[**3.** **Assessing EMIS Readiness** 23](#_Toc180673590)

[Factors to evaluate EMIS readiness 23](#_Toc180673591)

[Case study: Assessing EMIS readiness at the Army 25](#_Toc180673592)

[**4.** **Developing the EMIS Business Case**  28](#_Toc180673593)

[Business case development 28](#_Toc180673594)

[Life-cycle cost assessment 30](#_Toc180673595)

[Funding mechanisms 30](#_Toc180673596)

[**5. Case studies of successful EMIS deployment** 33](#_Toc180673597)

[5.1: Case Study: EMIS at Marine Corps Air Station Beaufort and Hanscom Air Force Base 33](#_Toc180673598)

[5.2: Case Study: EMIS at Fort Leavenworth 34](#_Toc180673599)

[5.3: Case Study: EMIS at CERL Champaign 35](#_Toc180673600)

[5.4: Case Study: EMIS across large real-estate portfolio 35](#_Toc180673601)

[5.5: Case Study: EMIS CERL FDD Pilot 36](#_Toc180673602)

[**6. Cybersecurity Considerations** 37](#_Toc180673603)

[Risk Management Framework 38](#_Toc180673604)

[Applying cybersecurity during design 39](#_Toc180673605)

[Security controls and requirements 39](#_Toc180673606)

[Inherited controls and cybersecurity services integration plan 40](#_Toc180673607)

[Construction and delivery phases 41](#_Toc180673608)

[**References** 44](#_Toc180673609)

List of Figures

[Figure 1:EMIS Framework- Data inputs and EMIS Capabilities 11](#_heading=h.2s8eyo1)

[Figure 2:UMCS Architecture 16](#_heading=h.z337ya)

[Figure 3:Five-Level Reference Architecture from UFC 4-010-6 17](#_heading=h.3j2qqm3)

[Figure 4:EMIS lite 19](#_heading=h.4bvk7pj)

[Figure 5:EMIS as a UMCS add-on 20](#_heading=h.1664s55)

[Figure 6: Cloud EMIS with configuration changes only 21](#_heading=h.2bn6wsx)

[Figure 7:Cloud EMIS with software changes 22](#_heading=h.3as4poj)

[Figure 8:Cloud EMIS with hardware changes 23](#_heading=h.49x2ik5)

[Figure 9:Rules-based decision tree process 25](#_heading=h.ihv636)

[Figure 10:Rules-based decision tree 27](#_heading=h.32hioqz)

[Figure 11:Sample business case outline 28](#_heading=h.41mghml)

[Figure 12:Energy Savings Performance Contract Life Cycle 31](#_heading=h.4h042r0)

[Figure 13:Typical DoD Army technology implementation process 32](#_heading=h.2w5ecyt)

[Figure 14:Installation diagram at CERL 36](#_heading=h.48pi1tg)

[Figure 15:Installation diagram at DoDEA 37](#_heading=h.1302m92)

[Figure 16:Platform Information Technology Life Cycle 42](#_heading=h.3l18frh)

List of Tables

[Table 1: EMIS architecture options summary 21](#_heading=h.2p2csry)

[Table 2: Important factors for a business case 26](#_heading=h.2grqrue)

List of Acronyms

|  |  |  |
| --- | --- | --- |
| AHU | Air Handling Unit | |
| API | Application Programming Interface | |
| ASO | Automated System Optimization | |
| ATO | Authorities to Operate | |
| BAS | Building Automation Systems | |
| BOS | Base Operations and Support | |
| CCB | Criteria Change Board | |
| CEWWE | Comprehensive Energy, Water, and Waste Evaluation | |
| CIO | Command Information Officer | |
| CUI | Controlled Unclassified Information | |
| DDC | Direct Digital Control | |
| DoD | Department of Defense | |
| DODIN | DoD Information Network | |
| DPW | Department of Public Works | |
| EACA | Energy Awareness and Conservation Assessment | |
| EAPP | Energy Engineering Analysis Program | |
| EIS | Energy Information System | |
| EM | Energy Manager | |
| EMIS | Energy Management and Information System | |
| ERCIP | Energy Resilience and Conservation Investment Program | |
| ESCO | Energy Service Company | |
| ESPC | Energy Savings Performance Contracts | |
| ESTCP | Environmental Security Technology Certification Program | |
| FCS | Field Control Systems | |
| FDD | Fault Detection and Diagnostics | |
| FPOC | Field Point of Connection | |
| FRCS | Facility-Related Control System | |
| HBSS | Host Based Security System | |
| HNC | Huntsville Center, Army Corps of Engineers |
| HQ | Headquarters |
| HVAC | Heating, Ventilation and Air Conditioning |
| ICAN | Installation Area Campus Network |
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISSE | Information System Security Engineer |
| ISSO | Information System Security Officer |
| LCCA | Life-cycle Cost Assessment |
| LHC | Land Holding Command |
| MICC | Mission and Installation Contracting Command |
| MILCON | Military Construction |
| NEC | Network Enterprise Center |
| O&M | Operations and Maintenance |
| OS | Operating System |
| PLC | Programmable Logic Controller |
| QA | Quality Assurance |
| REM | Resource Efficiency Manager |
| RMF | Risk Management Framework |
| SRM | Sustainment, Restoration, and Modernization |
| UESC | Utility Energy Services Contracts |
| UFC | Unified Facilities Criteria |
| UFGS | Unified Facilities Guide Specifications |
| UMCS | Utility Monitoring Control System |
| UP | Utilities Privatization |
| USACE | United States Army Corps of Engineers |
| VLAN | Virtual Local Area Network |

# **Introduction**

## Background

Energy management and information systems (EMIS) are a broad and rapidly evolving family of software tools that continuously and automatically monitor, analyze, display, and optimize building energy use and system performance. The information generated from EMIS tools enables building engineers, facility managers, and energy managers to operate and maintain their buildings more efficiently and with improved occupant comfort by providing quicker visibility into, and analysis of, the operations of lighting, space conditioning and ventilation, and other end uses. EMIS is a tool a building operator can use to unlock improvement opportunities that are not typically apparent without continuous and automated analysis. EMIS includes energy information systems, fault detection and diagnostic tools, and automated system optimization software:

* **Energy information systems (EIS):** EIS analytics focus on meter-level monitoring, analysis, and charting, and may incorporate automated opportunity analysis.
* **Fault detection and diagnostics (FDD):** FDD analytics automate the process of detecting faults and suboptimal performance of building systems and help to diagnose potential causes. FDD focuses on system-level monitoring, analysis, and charting. FDD can provide root cause issues and recommended fixes, compared to generalized high level alarms that front end utility monitoring and control systems currently provide. Additionally, FDD can be used for commissioning or functional performance tests after a construction project is ready to be tested by the Government, to perform a more rigid review than is currently performed.
* **Automated system optimization (ASO):** ASO analytics continuously analyze and modify building automation system (BAS) control settings to optimize heating, ventilation and air conditioning (HVAC) system energy use while maintaining occupant comfort. Some ASO technologies have the capability to implement demand flexibility control strategies that can adjust a building’s load profile across different timescales for electrical grid benefits.

Figure 1 illustrates the possible data inputs for EMIS and their capabilities. The left side of Figure 1 shows that building operations data are available from many sources, and with the proliferation of new technologies (e.g., Internet of Things (IoT) devices, distributed energy resources) the volume of data has increased exponentially in recent years. EMIS has emerged to enable building owners to extract accurate and actionable insights from large amounts of data. For example, modern building automation systems (BAS) monitor hundreds of points per building, and an owner may have a building portfolio generating many thousands of data points at 15-minute or higher intervals. The typical BAS can provide alarms for operational readings that are out of range (e.g., temperature setpoint), but the analytical capabilities fall well short of helping to identify root causes of the problems and provide solutions to achieve an optimized system. For instance, a BAS will provide information of a leaking hot water valve, since the air temperature setpoint will be met, but not have details on the amount of wasted energy. EMIS provides the needed analytical horsepower to help building owners find meaning from data. These systems support the identification and implementation of operational improvements in commercial buildings. A recent major study showed median whole building energy savings of 3% for EIS and 9% for FDD analytics (Kramer et al., 2020). Another study found that using EMIS with ASO provided between 5% and 11% whole building energy savings (General Services Administration, 2023). However, despite their potential and a fast-growing range of options, EMIS continue to be under-adopted technologies throughout the federal building stock. The barriers to adoption include complexity of systems integration, complicated user interfaces, data availability challenges, and making the business case for implementation and maintenance.

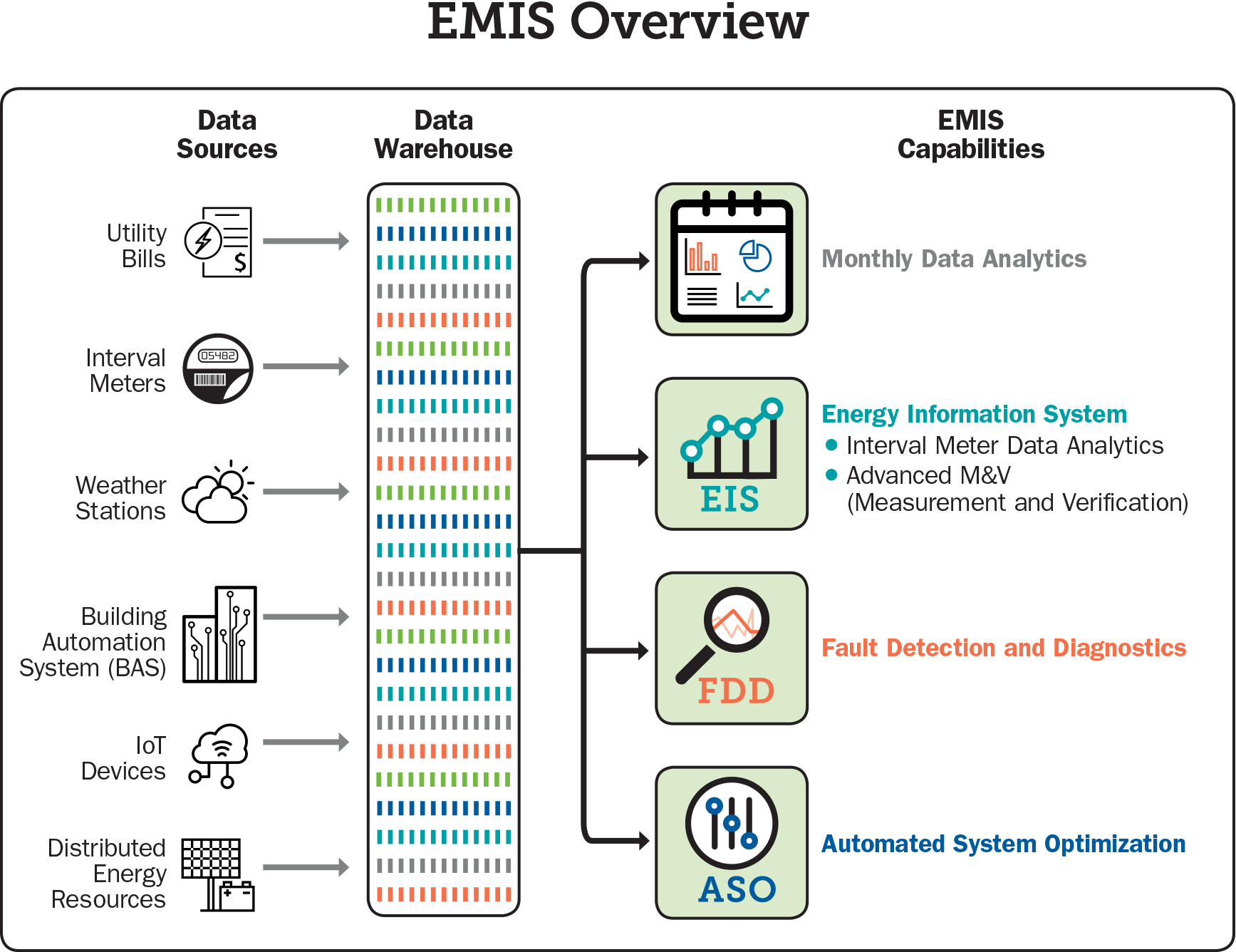


Figure 1: EMIS Framework - Data inputs and EMIS capabilities

## Purpose

The objective of the Department of Defense (DoD) *‘EMIS Guidance for implementing smart building analytics’* further referred to as “Playbook” in this document, is to provide guidance for implementing an EMIS which can be a key tool for meeting DoD sustainability goals. The Playbook is intended to help DoD building operators and facility managers overcome the most critical process and technical barriers that are impeding scaled adoption of EMIS within DoD installations.

The rest of the Playbook is organized into sections that aim to address specific questions as follows:

* **How do I select an EMIS configuration to suit my building?** Section 2 provides different EMIS architecture options, each with different installation, cybersecurity, and sustainment implications.
* **How can I assess whether my building is ready for an EMIS?** Section 3 presents factors that can be used to assess when a site is ready for EMIS procurement and installation.
* **How can I navigate the funding and procurement of an EMIS?** Section 4 provides the context and resources to prepare a business case to secure funding for the procurement of an EMIS.
* **What are the cybersecurity issues I need to be aware of when installing an EMIS?** Section 6 presents cybersecurity considerations.

The Playbook establishes options to implement different types of EMIS more rapidly, that are tailored to individual circumstances. It also includes options for how to secure funding and navigate network security requirements.

## Applicability

The Playbook is applicable to all DoD building energy projects. The Defense Logistics Agency Energy Office and the Services Energy Offices are the starting point for most energy projects. The DoD depends on the private sector to provide the vast majority of energy projects and has special legislative and Executive Order authorization for the acquisition of energy projects. These include Energy Savings Performance Contracts (ESPCs), Utility Energy Services Contracts (UESCs), Utilities Privatization (UP), Energy Resilience and Conservation Investment Program (ERCIP), and other contract or program vehicles.

## Relationship to existing policies and guidance

The DoD has seen the potential of EMIS, as evidenced by its selection for ongoing Environmental Security Technology Certification Program (ESTCP[[1]](#footnote-1)) demonstration projects over recent years (Bush et al., 2022). However, these projects also have revealed the ways in which DoD’s internal processes are not yet aligned to take advantage of high value EMIS opportunities at scale. With energy costs accounting for approximately 2% of DoD’s annual budget, and with DoD managing over 560,000 buildings, the savings potential is significant (Greenley, 2019). Further, EMIS are an ideal complement to other high-potential technologies such as distributed energy resources, advanced building controls, and advanced energy security strategies. FDD technologies can also prevent energy performance degradation over time, support various commissioning processes, improve operational efficiencies and facilitate predictive maintenance, which contributes to increased equipment life, improved reliability and lower labor cost.

The Energy Independence and Security Act of 2007 (Baker, 2008) requires Comprehensive Energy and Water Evaluations (CEWEs) to be performed at each covered federal facility every four years to identify potential energy and water efficiency and conservation measures (with covered facilities representing a total of at least 75% of total facility energy use). The Energy Act of 2020 (Degette, 2020) builds upon these requirements to include ongoing commissioning requirements within the scope of facility assessment (which, by definition, imply the use of EMIS) and also created more granular tracking requirements for energy audit activities.

The Army Installation Energy and Water Strategic Plan (Army Installation Energy and Water Strategic Plan, 2020) included objectives and targets that are complementary to increased EMIS adoption, including a target that 95% of installations have full-time energy managers by 2023, that installation-wide building automation systems are in place by 2028, and that an Army-wide energy and water data analytics capability is established by 2024. Similarly, other service branches such as the Navy and Air Force have their own strategies for improving efficiency at installations; an EMIS adoption would support achievement of their goals (Air Force Installation Energy Vision, 2021; Department of the Navy Installation Energy Resiliency Strategy, 2020).

## Audience

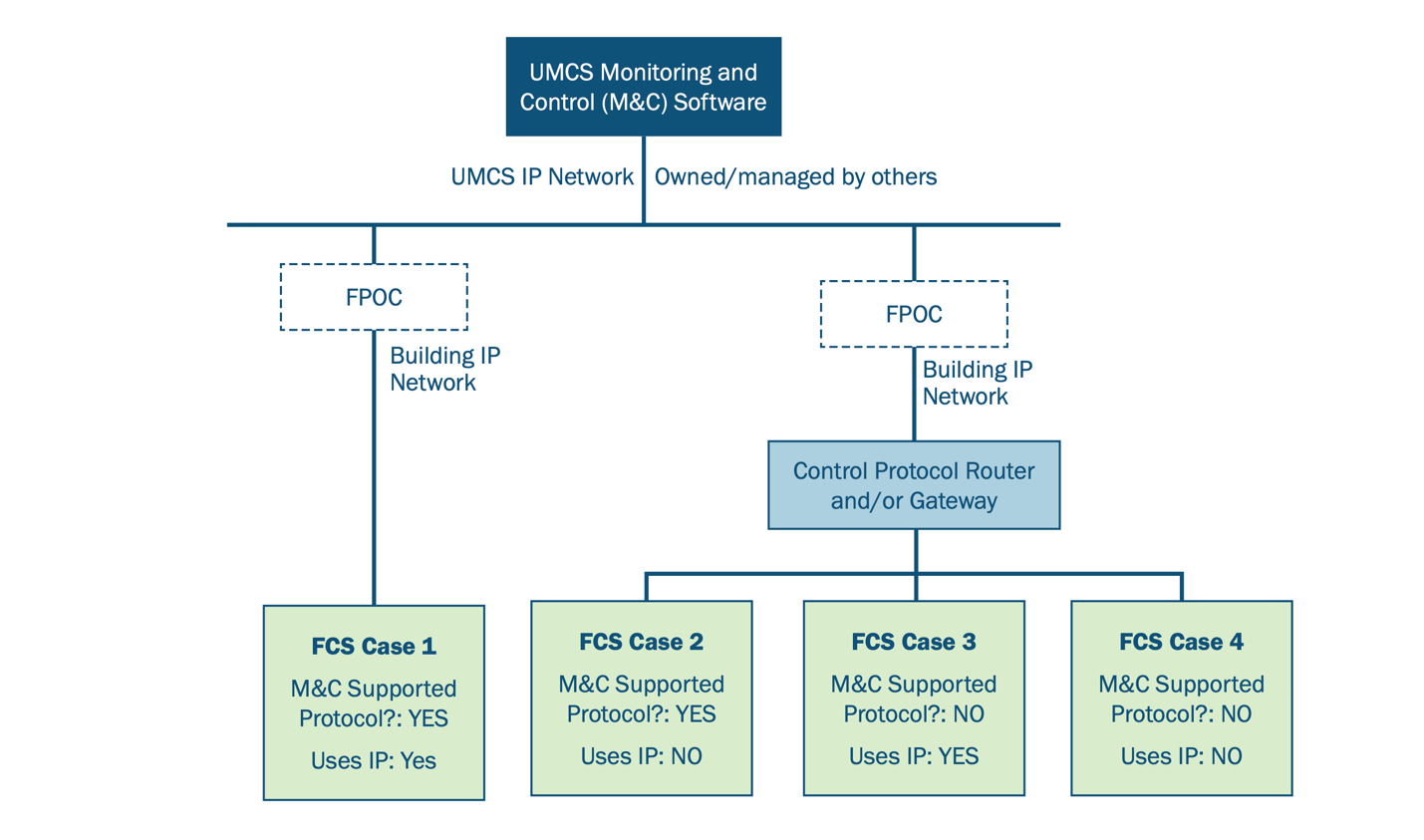
This document provides support mainly to installation and operational level staff such as the base energy manager, facility manager, contractor, energy service company (ESCO), and EMIS technology developers. The resources can be used to communicate the value of EMIS to other staff involved in processes such as project prioritization, solicitation, and award. This document provides implementation guidance and is not meant to supersede any existing statute or regulation.

# **2. EMIS Architecture Options**

EMIS can be installed and configured in different ways, each with their own configurations and benefits, each of which are called an ‘architecture option’ in this document. The installation and integration of an EMIS within DoD requires the selection of an appropriate architecture option that aligns with the existing Field Control System (FCS) and its Utility Monitoring and Control System (UMCS) front-end integration options, outlined in Unified Facilities Criteria (UFC) 3-470-01 (Utility Monitoring and Control System Front End and Integration, 2018), and the five-level Control System Architecture, outlined in UFC 4-010-06 (Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems, 2023).

The UMCS is a base-wide system, but it may initially consist of very few field control systems, or even only one. The UMCS may later be expanded to include additional field control systems. A single UMCS is expected to connect to many field control systems from several or many different vendors; the field control systems may be procured separately and then integrated into the UMCS front end. A base-wide UMCS consists of a UMCS front end (specified by Unified Facilities Guide Specifications (UFGS) 25 10 10 Utility Monitoring and Control System Front End and Integration) connected to one or more FCS. These FCS may be building control systems (BCS) (which are generally direct digital control (DDC) systems for the control of HVAC, lighting, and other building systems) or utility control systems (which vary in composition from “smart relays” to DDC controls to programmable logic controllers (PLCs) for control of power distribution or other “industrial” systems).

As illustrated in Figure 2, the UMCS network architecture supports four fundamental FCS cases, and consists of a base-wide internet protocol (IP) network connected to one or more field control systems through a field point of connection (FPOC) device, which provides an interface between the UMCS IP network and the field control network (FCN). The field control network (FCN) is the network used by a FCS, which only covers networks related to level 1 and level 2 as shown in the five-level architecture (Figure 3). Monitoring and control supported protocol refers to protocols that the UMCS Monitoring and Control Software (M&C) software uses. Typical protocols include BACnet/IP, LonWorks/IP, and Niagara Fox. In general, FCNs themselves may use a wide variety of media and protocols, but building control networks for systems based on LonWorks should be a combination of IP, TP/FT-10, and possibly TP/XF-1250. Building control networks for systems based on BACnet should be IP and/or MS/TP. It is worth mentioning that FCS Case 2-4 and their UMCS front-end integration options should be only for legacy field control systems; all other systems should use the option for FCS Case 1.



Notes: 1) All FCS may have a non-IP network in addition to any IP network. 2) All buildings installed under UFC 3-410-02/UFGS 23 are Case 1. Cases 2-4 should only be for legacy. 3) M&C protocols include those selected via tailoring options in UFGS 25 10 10 and others that may be supported by that vendor’s M&C software. 4) Note that in Cases 2-4, the UMCS integrator may need to install Control Protocol Router and/or Gateway and also install/extend the building IP and/or non-IP networks.

Figure 2: UMCS Architecture

On the other hand, in the five-level control system architecture, each level represents a collection of field control system components that are logically grouped together by function, and which generally share a cybersecurity approach (note, the FCS shown in Figure 2 is broken out into Levels 0, 1, and 2 in the five-level control system architecture). This architecture is defined as a general architecture suitable for a wide range of field control systems, and there are some key considerations when integrating EMIS at different field control system levels, because it is rare that EMIS exert control capabilities. In addition, not every implementation of a control system will make use of every level, or every type of component shown at a level. Figure 3 depicts the five-level architecture.

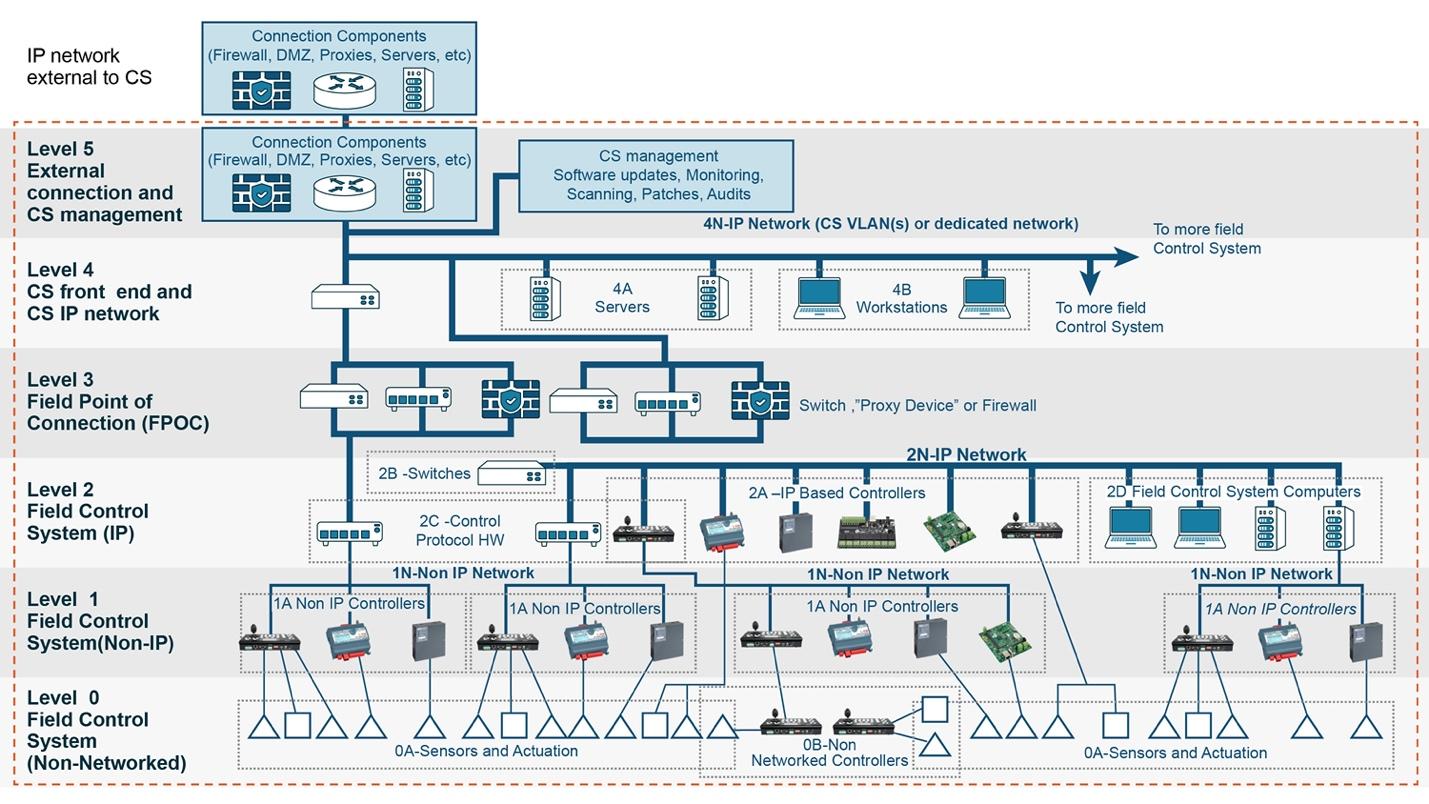


Figure 3: Five-Level Reference Architecture from UFC 4-010-6

A brief description of each level (from simple to complex devices) is:

* Level 0. Non-networked devices that communicate using analog and binary signals. These include sensors and actuators as well as non-networked controllers (including their dedicated sensors and actuators). These communicate with Level 1 via hardware I/O (analog and binary signals). EMIS implementation does not affect this level and will not be included in the subsequent figures.
* Level 1. Networked controllers not on an IP network (such as BACnet MS/TP, RS485 (DNP, Modbus), LonWorks TP/FT-10).
* Level 2. Networked controllers on an IP network.
* Level 3. The FPOC, which is a connection between the field control system IP network at Level 2 and the Level 4 IP network.
* Level 4. The site-wide IP network used for the control system, along with front-end servers and workstations (desktops and laptops).
* Level 5. Interfaces to “external” networks (IP networks other than the control system network).

There are a variety of ways that EMIS capabilities can be installed within this generic UMCS architecture framework, which we call an “EMIS architecture option” here. Each architecture option has different installation, cybersecurity, and sustainment implications. Some vendors offer multiple architecture options based on control protocols in use, hardware requirements, and connectivity limitations. Any early discussion on EMIS deployment should identify what existing system changes are needed based on the architecture options and include teams affected by differing levels of functionality and IT security. Depending on where in the UFC and UMCS architecture changes are needed for the EMIS implementation, there are five suggested configuration options:

* Option 1: EMIS lite
* Option 2: EMIS as a UMCS add-on
* Option 3: Cloud EMIS with configuration changes only
* Option 4: Cloud EMIS with software changes
* Option 5: Cloud EMIS with hardware changes only

Annotations for where the UFC and UMCS architecture need configuration changes, software changes, or hardware changes are shown in the corresponding figures below. Selecting a suitable EMIS architecture is based on multiple objectives, such as initial investment cost, recurring cost, and robustness with respect to the existing UFC architecture and UMCS front end. This architecture allows distinctions to be made between portions of the control system that resemble a standard IT infrastructure and portions that do not . This is important, as many security controls can be applied in the normal fashion to the portion of the control system that looks like a standard IT system but cannot be applied without modification (or sometimes cannot be applied at all) to the portion that does not look like a standard IT system.

## Option 1: EMIS lite

In this architecture, the existing UMCS is configured for basic fault detection and enhanced graphics/alarm. This is a low-cost option with low-to-moderate benefits. It applies to any UMCS make/model, and the configuration changes occur at the front end (Level 4) (see figure 4). Configuration changes consist of changing settings, purchasing licensing, point tagging and naming, and setting up the FDD interface (licensing may be needed depending on vendor). This is the lowest risk option from an IT standpoint, and also has the benefit that users will already be familiar with the UMCS interface. However, it would require some effort to configure fault detection rules and design graphics, and would not be expected to have the range and depth of fault detection capabilities that is typical of commercially available FDD software tools.

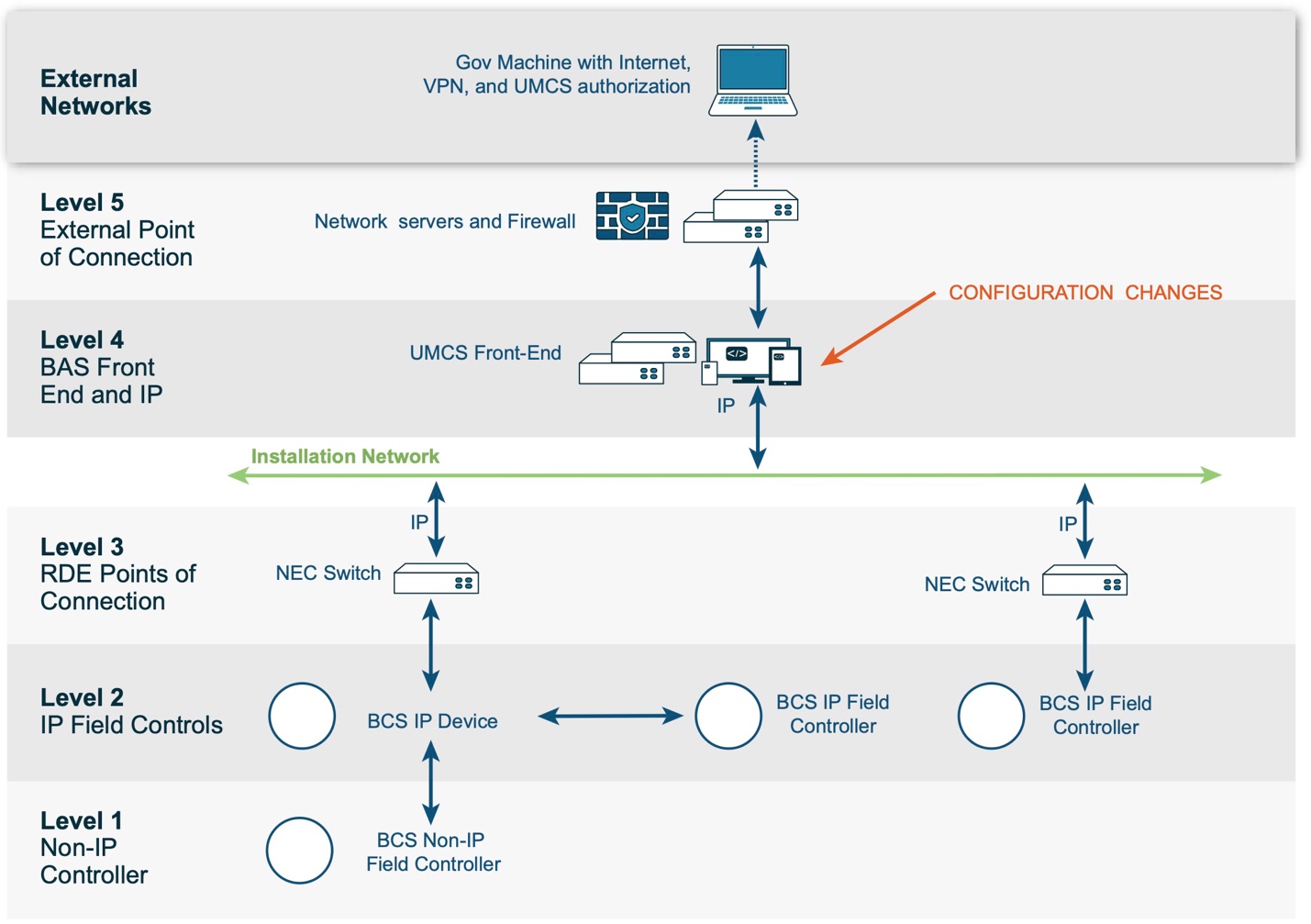


Figure 4: EMIS lite

## Option 2: EMIS as a UMCS add-on

UMCS add-ons or on-premise EMIS instances are installed without cloud services. This applies to UMCS with EMIS add-on options offered by the UMCS software vendor or a third-party on-premise EMIS solution provider. Configuration changes occur at levels 1, 2, and 4 (see figure 5). In this architecture, significant level 1 and level 2 configuration changes are likely. Hardware changes may be necessary at the building supervisory controller (Level 2) for the installation of the analytics.

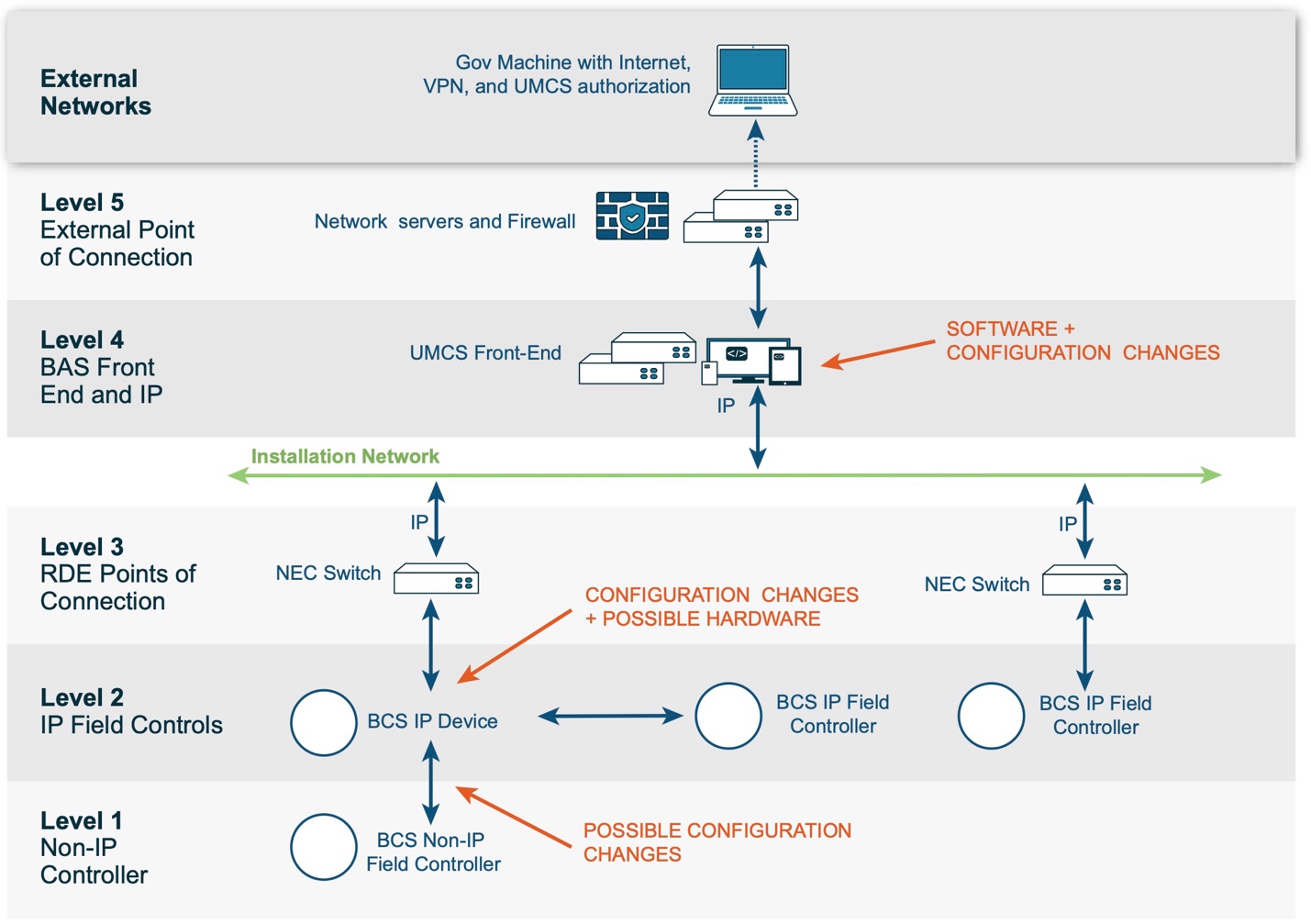


Figure 5: EMIS as a UMCS add-on

## Option 3: Cloud EMIS with configuration changes only

This is the simplest cloud option with no hardware or software update, and configuration changes (similar to option 1) occur at levels 2 and 5 (see figure 6). When a DoD entity is connecting to the cloud, additional cybersecurity considerations (outlined in Section 5) will be required, such as monitoring to connect to the third-party analytics provider or even to a GovCloud platform. The advantages of this architecture are that it is offered via a standard cloud option with real time EMIS software updates with less effort required onsite. The disadvantage is that it raises the IT approvals process, cost and timeline.

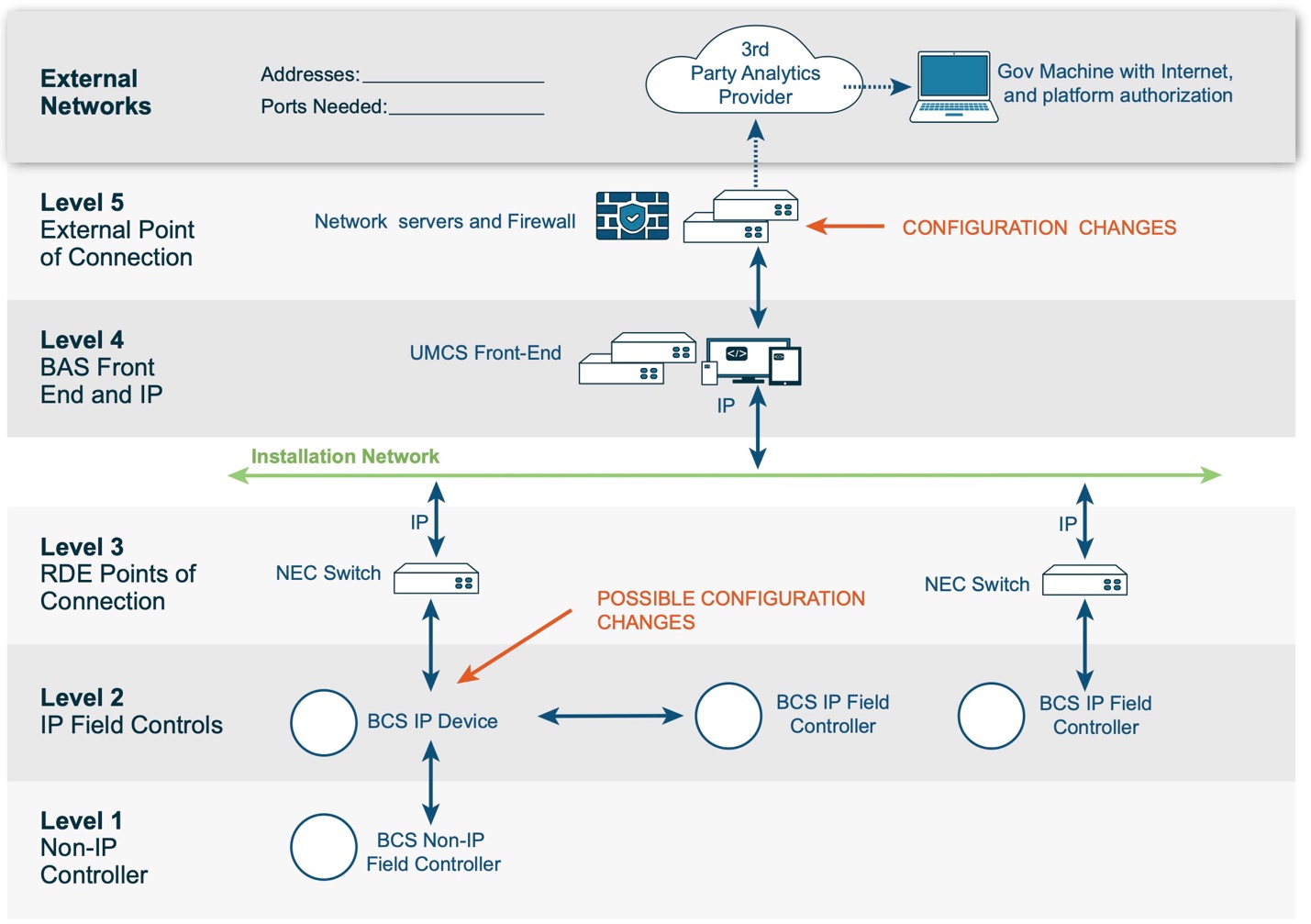


Figure 6: Cloud EMIS with configuration changes only

## Option 4: Cloud EMIS with software changes

In this architecture the EMIS provider will require that some service continuously run at the UMCS server level to push data to their cloud location. The communication to the cloud location will be required, typically with non-specialized ports/protocols. The EMIS software can be integrated with cloud platforms using an Application Programming Interface (API) and the software changes involve enabling data exchange between the monitoring system and cloud service. Depending on the cybersecurity posture, other hardware may be added. In the case of the Army, it may require ‘assessment only,’ in coordination with the local Criteria Change Board (CCB), as opposed to a more comprehensive approval process. Configuration changes occur at levels 2, 4 and 5 (see figure 7).

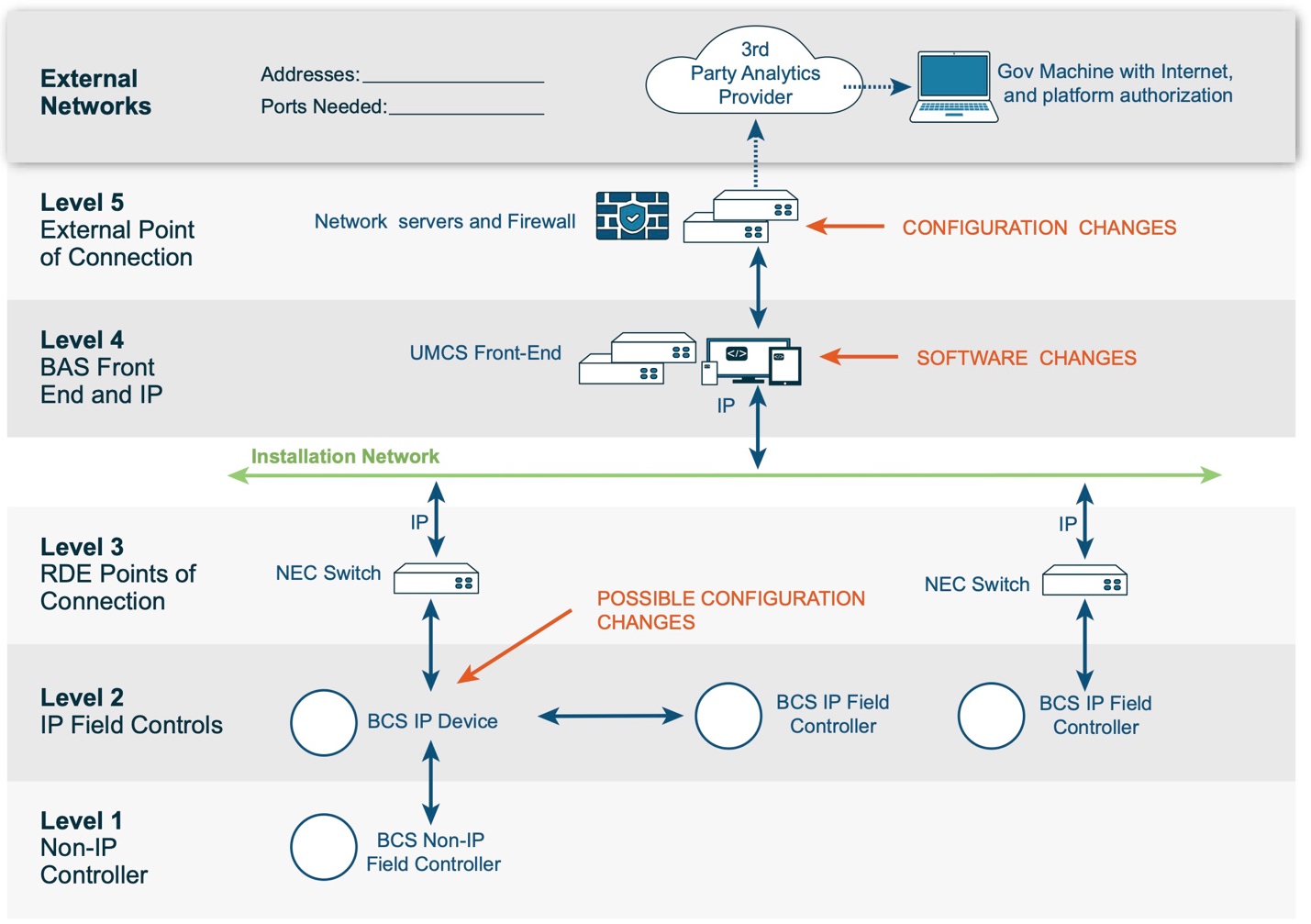


Figure 7: Cloud EMIS with software changes

## Option 5: Cloud EMIS with hardware changes only

This is the same architecture as the previous option, providing another method to connect to the cloud, but it runs in a box with an IP connection on the Installation Network (ICAN) or depicted in the figure as Installation Network. The hardware device installed could be a “cache poller,” “bridge,” router, or cellular modem, depending on the existing infrastructure and communication requirements. Configuration changes occur at levels 2 and 5, with installation of new hardware at level 4 (see figure 8).

This option requires extra IT coordination for activities such as IP assignment, MAC address whitelisting, install, initial configuration, patching, and has more of an impact expected to existing processes such as authority to operate (ATO). The ATO process is aimed to minimize and manage risk responsibly. It is an official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

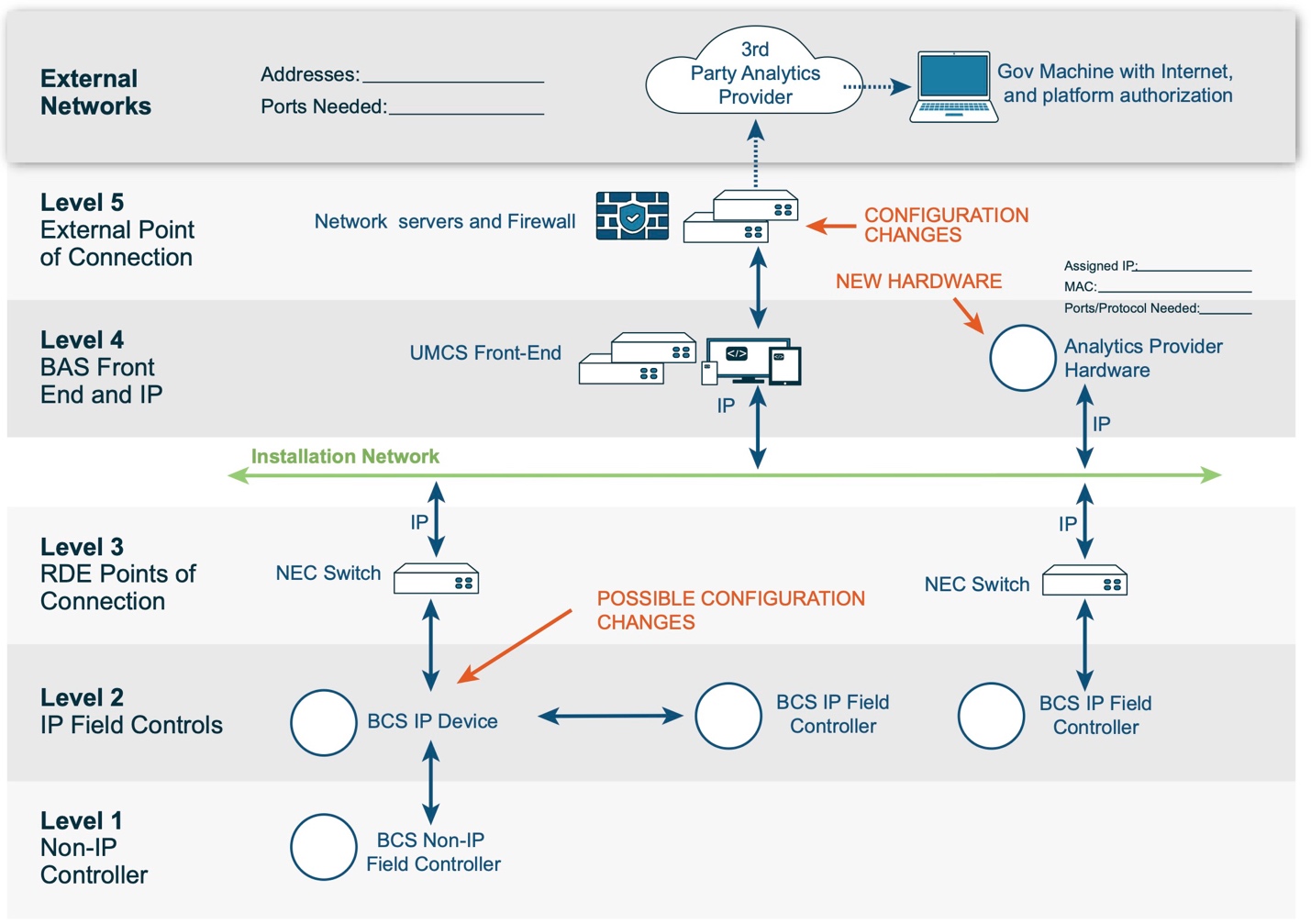


Figure 8: Cloud EMIS with hardware changes

A summary of the various EMIS architecture options is shown in Table 1.

*Table 1: EMIS architecture options summary*

|  |  |  |  |
| --- | --- | --- | --- |
| **Architecture Option** | **Description** | **UMCS Front End changes required?** | **Architecture Level?** |
| EMIS-lite | Basic function on existing UMCS | Yes | 4 |
| EMIS as UMCS add-on | UMCS add-ons or on-premise EMIS without cloud services | Yes | 1, 2, and 4 |
| Cloud EMIS with configuration changes only | Simplest cloud option | No | 2 and 5 |
| Cloud EMIS with software changes | Cloud option with some EMIS continuously running at the front end | Yes | 2, 4 and 5 |
| Cloud EMIS with hardware changes only | Cloud option with some EMIS continuously running on an added EMIS hardware | No | 2 and 5 |

# **Assessing EMIS Readiness**

## Factors to evaluate EMIS readiness

When evaluating EMIS potential across a large installation with hundreds of buildings, it is beneficial to prioritize the buildings where the suitability and benefits of implementing EMIS are greatest. Several factors are likely to influence how prepared a facility is for procuring and installing EMIS. The characteristic features of the existing building stock and control systems can be used to establish a department-wide assessment of the potential for EMIS implementation or readiness level, and select a priority list of buildings that are "EMIS-ready." Some crucial factors to consider for determining EMIS readiness include:

1. **Physical Characteristics:** Large buildings (over 50,000 square feet), buildings with high HVAC condition index (CI) (HVAC CI measures the asset’s condition at a specific point in time on a score between 1-100), energy-intensive buildings (IT/simulation, central plant), or buildings with complex central HVAC configurations will see maximum benefits from EMIS. Complex central HVAC configurations include multiple central hydronic systems, chilled water and steam/hot water, and complex distribution systems (hot water variable air volume). A high relative pump count, as indicated in system-of-record datasets such as “BUILDER”, may be considered as a proxy for this complexity. Where utility or government-owned meter data are available, buildings above peer-group energy use intensity (EUI) benchmarks may have higher likelihood of savings opportunities.
2. **Connected and Secured Digital Controls:** Building Control System data (specifically HVAC and energy meter equipment data) serve as the core data source for EMIS functionality. These control systems must have ATO to qualify for EMIS readiness status. Exceptions include EMIS systems that can be included in new or reauthorized UMCS ATO packages or EMIS systems that are targeted for stand-alone building-level implementation.
3. **IT Coordination Staffing:** Even with an ATO and FedRAMP[[2]](#footnote-2) certification, dedicated IT coordination will still be required to plan, secure, and maintain any cloud-based connections. UMCS IT staff such as an Information Security Officer may be best suited to coordinate changes with installation network management staff. Tasks will likely include: conveying ATO architecture changes, submitting CCB requests, sponsoring FedRAMP certification, coordinating non-inherited security controls from FedRAMP certification, determining EMIS port/protocol requirements, configuring security of new hardware/software, updating existing ATO artifacts, addressing continuous monitoring needs, and helping to establish virtual private network (VPN) traffic to secure connections between the installation and certified cloud application.
4. **Workflow Integration:** Just having an EMIS capability will not automatically yield benefits. EMIS is a tool that must be integrated into existing or new workflows to be effective. This is why many EMIS providers offer periodic training to help use EMIS systems or owners assign new maintenance tasks to address any backlogs the EMIS system finds. It is also important to factor in the skills of the facility staff in understanding building controls and energy management. At Army installations, the Department of Public Works (DPW) may have limited resources to manage FDD or EIS software. If practical, it can be helpful to hire a contractor or additional government employee to work with the maintenance team on a monthly basis to review and resolve any issues uncovered by an EMIS.
5. **Controls point naming convention:** Consistent, logical control system point naming and metadata structure can significantly reduce the effort required to install and configure an EMIS. Employing industry-standard metadata tagging standards (such as Haystack or Brick Schema; ASHRAE Standard 223P) should also be adopted when installing a control system to facilitate easier EMIS setup and ongoing maintenance.

Below is a case study that used physical characteristics and control system data to assess EMIS readiness for Army buildings. It demonstrates one approach that could be used to prioritize the buildings where the suitability and benefits of implementing EMIS are greatest.

## Case study: Assessing EMIS readiness at the Army

An anonymized dataset (n = 56,622) of Army buildings was extracted from the “BUILDER” database, and buildings that had digital controls (often called *DDC*) were selected for the EMIS readiness analysis (n = 3,858); the assumption being that buildings with DDC have the most potential to deploy an EMIS. Data-driven feature engineering techniques were applied to pre-process the dataset, followed by a rules-based decision tree analysis technique, and buildings in the dataset were classified into three EMIS readiness categories: High, Medium, and Low.

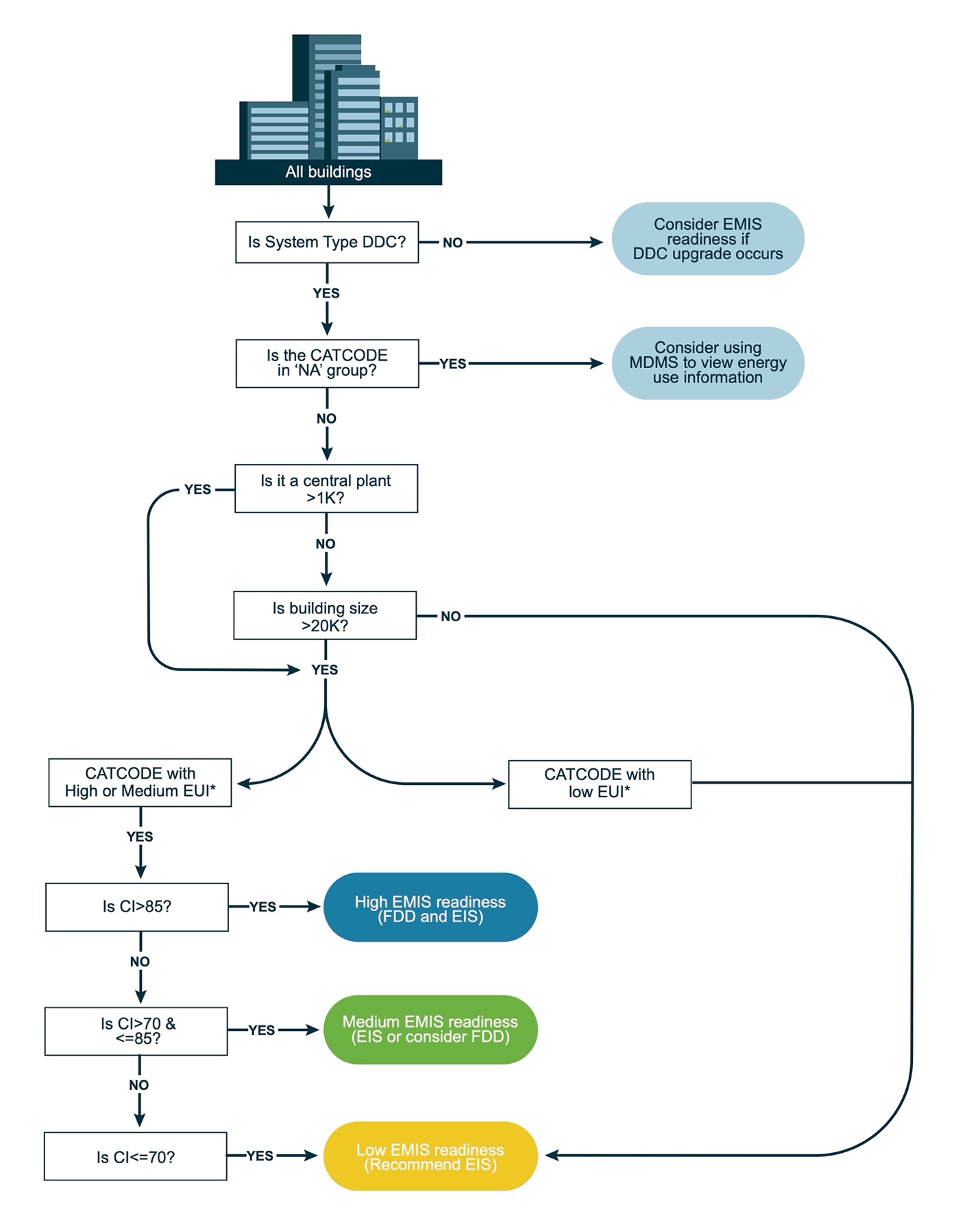


Figure 9: Rules-based decision tree process

Three core variables were used to develop the rules-based decision tree:

1. Building size: The size of the building, as measured by total square footage.
2. HVAC CI: The cost-weighted average of the component-section condition indexes aggregated to the building. CI is a 0 to 100 measure of the physical condition of an asset.
3. CATCODE: This Army-developed five-digit number is used to classify a specific category of facilities. CATCODEs are built digit-by-digit based on a hierarchy of groupings and associated measurement units for facilities within each CATCODE. This variable was further divided into 3 EUI classifications of High, Medium, and Low based on expert interpretations of the energy use of the particular facility the CATCODE represented.

Through applying data-driven, rules-based decision tree analysis, we were able to develop insights into potential EMIS-ready buildings and classify the Army building stock into three EMIS readiness categories. From the 3,858 buildings that were analyzed using the decision tree,458 (12%) were classified as High EMIS readiness, 499 (13%) as Medium EMIS readiness, and 2,901 (75%) as Low EMIS readiness. This approach could be used to assist building operators understand their building’s readiness for EMIS deployment. Figure 10 shows a graphical representation of the rules-based decision tree.



Notes: MDMS = meter data management system, EUI = energy use intensity.

Figure 10: Rules-based decision tree for classifying buildings into High, Medium, and Low EMIS readiness. \* Indicates that this variable was further divided into 2 EUI classifications of High, Medium and Low based on expert interpretations of the energy use of the particular facility the CATCODE represented.

# **Developing the EMIS Business Case**

## Business case development

Procurement processes can be difficult to navigate and use for both the initial EMIS implementation and also the operation and maintenance of the EMIS. A robust business case is a valuable tool that decision makers use to evaluate alternative approaches in the allocation of scarce resources and in developing sound business process solutions. It provides a structured and systematic methodology for assessing the financial consequences of business decisions. A business case is generally divided into different sections, and the sections are grouped with like sections into parts. Figure 11 shows a sample outline for a business case.

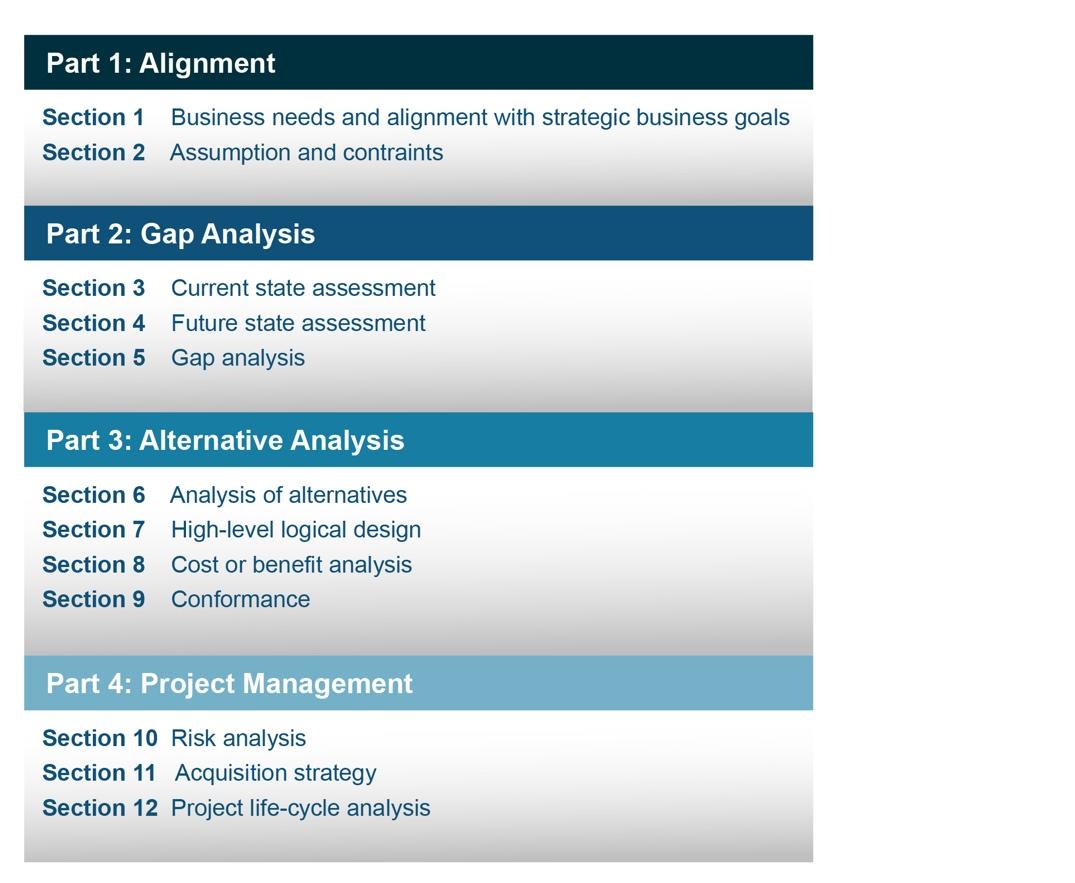


Figure 11: Sample business case outline, Source: *DOD Product Support Business Case Analysis Guidebook*

As part of the overall business case, a Cost-Benefit Analysis requires a formal requirements analysis, typically presented in a Mission Needs Statement, as well as global and alternative assumptions that introduce greater complexity in the analysis of the problem. It also necessitates the consideration of multiple alternative solutions. Greater flexibility is allowed in the use of extrapolated data for developing future costs and benefits of alternative solutions. This analysis may require a sensitivity analysis to test assumptions and constraints, and the presentation of findings in terms of constant dollars, current year dollars, and net present value (NPV). Table 2 illustrates the important factors to consider in the development of a business case when considering implementing an EMIS.

*Table 2: Important factors to be considered for an EMIS business case*

|  |
| --- |
| **Building square footage** |
| **Number of BAS points to be mapped** |
| **ATO/cATO reauthorization fees** |
| **Staff needs and time** |
| **Ongoing maintenance fees** |
| **Service fees** |
| **Savings estimation** |

cATO = continuous authority to operate

Savings specific to a given building may be difficult to assess, since every building will have its own set of operational inefficiencies to be resolved through the use of EMIS, but planning-level estimates can borrow from industry study metrics and apply to installation portfolio data. Real property records, UMCS integration status, building asset lists, and known or estimated energy usage by building are particularly useful datasets to merge for such cost savings purposes. Current industry estimates of average savings from FDD data analytics are 9% (Kramer, 2020) and coupled with energy usage models, initial cost estimates can be developed to preliminarily assess the viability of the business case for implementing an EMIS.

The DoD provides useful resources for development of a business case (DoD, 2011). In addition, the EMIS procurement spec material is a useful resource package to help define EMIS specific requirements that need to be included in a business case (LBNL, 2020).

## Life-cycle cost assessment

Life-cycle cost assessment (LCCA) is an economic method of project evaluation in which all costs arising from owning, operating, maintaining, and ultimately disposing of a project are considered. LCCA is suitable for evaluation of alternatives at different levels of project or program scope, including individual building systems, new construction building designs, major or minor building renovation designs, and facility and campus development and renovation master plans. The life-cycle cost (LCC) is the cost of an asset or its parts throughout its life cycle while fulfilling its performance requirements. The LCC method of economic analysis is the basic building block of LCCA. NIST Handbook 135 2020 (Kneifel and Webb, 2020) is the LCC manual for the Federal Energy Management Program (FEMP) for economic evaluation of high-performance facility projects, including energy efficiency, water conservation, and renewable energy projects in all federal facilities. For Military construction (MILCON) projects, the Army signed a memorandum of agreement that complies with the methods outlined in NIST Handbook 135. The Whole Building Design Guide [[3]](#footnote-3)(WBDG) and the Building Life-Cycle Cost (BLCC) tool could be used to determine the LCC effectiveness of all projects.

## Funding mechanisms

There are multiple ways to fund the implementation of an EMIS: MILCON; sustainment, restoration, and modernization (SRM); Energy Savings Performance Contract (ESPC), or other third-party financing.

***Military Construction (MILCON):*** As part of new military construction or a major renovation project, HVAC controls and EMIS can be integrated into existing base-wide front ends. A specific type of MILCON appropriation — the Energy Resilience and Conservation Investment Program (ERCIP) — is also available to support the installation’s strategy to enhance their EMIS capability. ERCIP is a subsection of the Defense-wide MILCON Program specifically intended to fund projects that save energy and water, reduce DoD energy costs, improve energy resilience and security, and contribute to mission assurance. ERCIP projects are allocated across two categories: (1) energy conservation (renewable energy, energy efficiency, and water conservation); and (2) energy resilience and energy security.

***Facilities Sustainment, Restoration, and Modernization (SRM):*** This effort provides funds to keep the installation’s inventory of facilities in good working order, (i.e., day-to-day maintenance requirements). In addition, it provides resources to restore facilities whose age is excessive or have been damaged by fire, accident, or natural disasters, and to alter facilities to implement new or higher standards to accommodate new functions or missions. Most installations use SRM funding to execute repairs or upgrades to failed building controls system projects (including technologically obsolete controls), and this funding mechanism could be leveraged for EMIS installation.

***Third-Party Financing:*** Another option that is available to the installation is the use of third-party financing to support their energy strategy initiatives. The use of the various third-party-financed programs can be leveraged to implement energy conservation measures (ECMs). UESCs and ESPCs are the two primary third-party financing mechanisms employed in the federal sector. UESCs are limited-source contracts between the installation and its serving utility for energy- and water-efficiency improvements and demand-reduction services while ESPCs are a partnership between the installation and an ESCO. Third-party-financed contracts are innovative arrangements for designing, installing, and financing energy improvement projects where the savings achieved by the project are intended to provide a return on investment over the term of the agreement. UESCs and ESPCs are typically long-term agreements (10+ years) and are adaptable to site-specific needs. In the context of long term UESCs/ESPCs, the use of an EMIS can be viewed as both a source of savings (through resolving inefficiencies) and also as a financial risk management tool (maintaining performance of major capital equipment upgrades funded through the project).

**Third-Party Energy Projects – ESPC Example**

To illustrate how DoD and third-party financing and project delivery occurs, an example of the ESPCs life cycle is shown in Figure 12. DoD works closely with the U.S. Department of Energy to use ESPCs to upgrade outdated DoD infrastructure (Federal Energy Management Program, 2023). An ESPC is a partnership between a federal agency and an ESCO. After being selected for a potential award, the ESCO conducts a comprehensive facility energy audit and identifies improvements to save energy. In consultation with the agency, the ESCO designs and constructs a project that meets the agency’s needs and arranges financing to pay for the project.

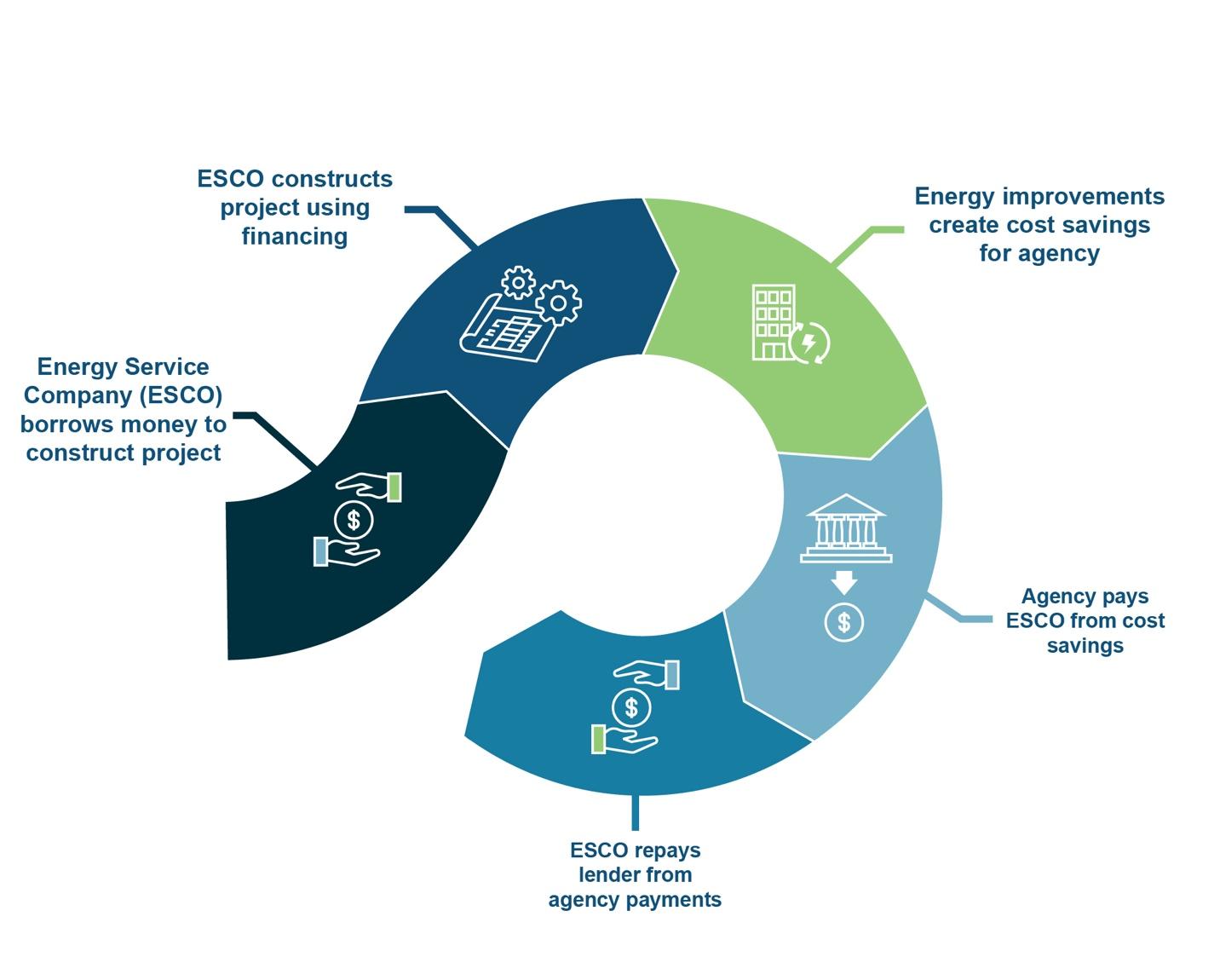
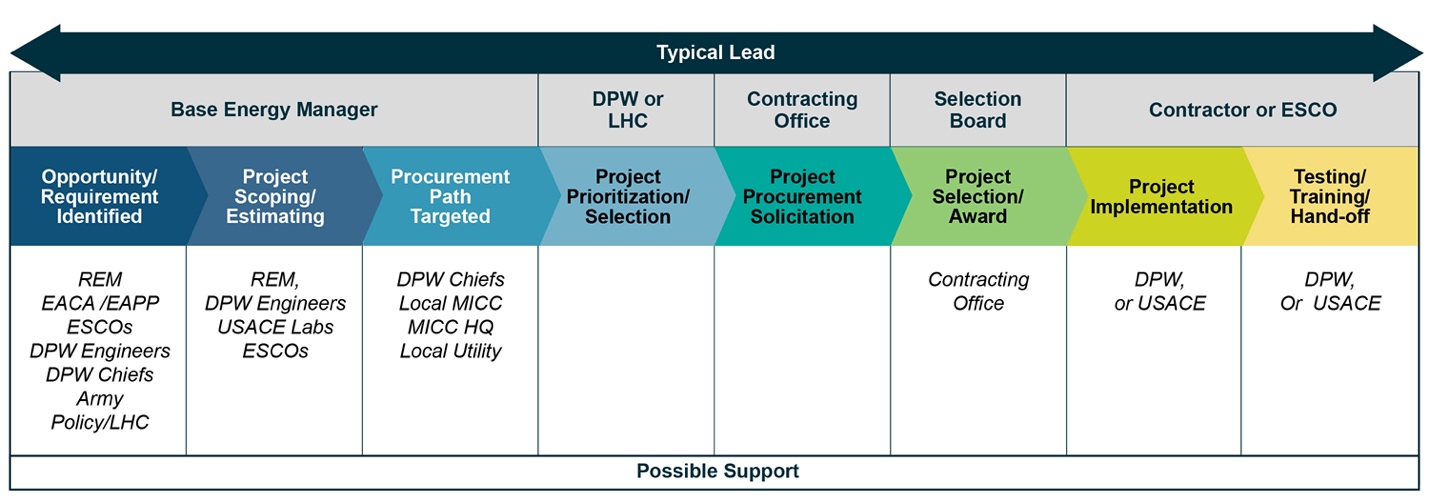


Figure 12: Energy Savings Performance Contract Life Cycle

With third party financed energy projects, the DoD may either become the system owner upon completion, or it may become an end user, with the third-party remaining as the system owner and providing power to DoD as a service. Prior to the engagement with an ESCO (or other contractor, for non-ESPC projects), there are many steps taken to initiate an energy efficiency project, involving many departments/stakeholders. ESCO financing terms may be as long as 20 years, and since the investments are intended to be repaid from energy savings, it is critical to maintain efficient performance; EMIS is well suited for assuring and optimizing energy performance.

The typical sequence to identify the need and procurement of an energy project is outlined in UFC 1-200-02 High Performance and Sustainable Building Requirements (Department of Defense, 2014). As an example, the DoD Army technology implementation process flow shown in Figure 13 has lead roles for different process steps and possible support available at each of those steps. Other DoD service branches will have similar processes.



Notes: DPW = Department of Public Works, LHC = Land Holding Command, REM = Resource Efficiency Manager, EACA = Energy Awareness and Conservation Assessments, EAPP = Energy Engineering Analysis Program, USACE = United States Army Corps of Engineers, MICC = Mission and Installation Contracting Command, HQ = headquarters

Figure 13: Typical DoD Army technology implementation process (other service branches have similar processes)

# **5. Case studies of successful EMIS deployment**

## 5.1: Case Study: EMIS at Marine Corps Air Station Beaufort and Hanscom Air Force Base

An HVAC fault detection pilot with the DoD is underway and scheduled to be completed in 2024. Aimed at improving the energy efficiency and operation of mechanical systems, the team is targeting a 15% reduction in HVAC-related energy usage and a simple payback period of less than two years. In 2022, Cimetrics’ Analytika, a commercial FDD platform and service, was successfully deployed at Marine Corps Air Station Beaufort and Hanscom Air Force Base.

Their approach uses a hardware appliance to poll data directly from sensors, motors, meters, etc. within each site’s existing building control system. The initial configuration was handled almost entirely by the vendor, with minimal workload for DoD facility personnel (mainly to identify BAS points and to coordinate network access). This pilot could be categorized as “Cloud EMIS with hardware changes” configurationcategory(Figure 8). Cimetrics has ported their commercial analytics platform to the AWS GovCloud to have an isolated and more secure environment specific to DoD customers. For this effort, the project aims to achieve ATO on the Cache Poller hardware appliance that polls and stores the BAS data. The Cache Poller stores data locally until upload, and they are pursuing ATO for the Cache Poller. For this pilot, the managed cell modem uploads data to the analytics engine and portal hosted in the secure cloud. The solution is highly scalable. Despite initial plans to address only six buildings per installation, the team was able to onboard and analyze over 100 buildings covering more than 2 million square feet. The EMIS/FDD solution uncovered thousands of energy-saving opportunities and operational faults, including scheduling issues, control logic problems, simultaneous heating and cooling, hunting or leaking valves, sensor failures or calibration issues, and more. Weekly calls with facility teams led to efficient issue tracking, prioritization, and resolution. The project has demonstrated the potential for broader adoption across DoD facilities, indicating substantial energy and cost savings opportunities across service branches.

## 5.2: Case Study: EMIS at Fort Leavenworth

Fort Leavenworth is conducting a comprehensive study to evaluate the effectiveness of energy management within the DoD. The study utilizes a vendor’s EMIS across eight diverse facilities, focusing on FDD as a pilot initiative. The objective is to assess the benefits of these systems on a broader scale within the DoD. The study employs a dual quantitative and qualitative analysis, evaluating four key metrics:

* Facility energy usage;
* System economics;
* Implementation rate; and
* Perceived operational benefits.

The chosen approach aligns with Option 2 of this Playbook, utilizing “EMIS as a UMCS add-on (Figure 5).” This involves integrating standard libraries with custom algorithms at the UMCS front-end interface to facilitate fault detection notifications and alarms for operators. The pilot not only establishes a precedent for future expansions using Option 2, but also highlights the potential for enhanced energy management across the entire DoD portfolio.

## 5.3: Case Study: EMIS at CERL Champaign

This project demonstrated the Modius OpenData platform to the DoD as a middleware solution for effective use of utility and facility data to improve the management, operation, and maintenance of facilities. The initiative centralized and standardized utility data management across DoD Service branches, which was previously hindered by disparate systems and underutilized data, particularly from an increasing number of smart meters.

At its core, Modius OpenData is a full-stack IoT platform with a two-tier architecture, integrating various devices and providing a unified, accessible view of energy consumption data. This system ensured efficient data processing and synchronization, enhancing decision-making for operations and maintenance teams. The platform’s implementation showed substantial benefits: cost-effective metering system deployment, deeper energy usage insights, and validation of the DoD’s 5% energy reduction goal. Moreover, incorporating machine learning technologies provides automated oversight of the DoD’s complex infrastructure, aligning with stringent security and operational requirements.

## 5.4: Case Study: EMIS across large real-estate portfolio

Jamestown is a real-estate investment and management company with nearly $12 billion in assets under management. In 2012, Jamestown launched Jamestown Green to spearhead environmental sustainability at the property, portfolio, and corporate levels. Managing a multistate portfolio of buildings to achieve aggressive sustainability goals is simply not possible without having a good handle on data. In 2017 Jamestown embarked on an effort to make their energy data more transparent and easier to analyze. They chose to implement EIS that allow their operations and sustainability teams and building engineers to view hourly energy data in real time.

With visibility into how the buildings were operating, Jamestown averaged 4% savings in the first year, with five properties achieving savings in excess of 16%. The EIS has provided building engineers with a powerful tool for finding operational issues and seeing the positive impacts of the improvements they make. In this diversified portfolio of office, mixed use, and retail assets, Jamestown takes a customized approach for achieving savings at each building. Where feasible they target annual ENERGY STAR certification for all properties through ongoing operational improvements and retrofits. In 2019, the DOE-funded Smart Energy Analytics Campaign recognized Jamestown for their exemplary use of EIS. While this example is outside of a DoD context, Jamestown provides a model for how to manage EMIS across a large portfolio of buildings.

## 5.5: Case Study: EMIS CERL FDD Pilot

As part of a CERL FDD pilot project, Johnson Controls installed OpenBlue on multiple CERL buildings located at their Champaign, IL campus. Project installation, ease of data ingestion, data lake management, fault rules and user operability were evaluated. Johnson installed a hardware device (bridge) to auto scan the network to find the Tridium JACE devices. BACnet objects for the field controllers were auto populated, sorted and categorized within the cloud, collecting data from three buildings and over 4,000 control points. From there, fault detection rule sets were applied based on the equipment type and function. There are over 800 pre-defined rule sets and endless custom opportunities to accommodate any type of system. Discovered faults are broken down into three different categories: Energy, Maintenance and Comfort. Based on the fault category, the appropriate actions can be assigned to correct the fault. Interconnection with maintenance management systems like Maximo or the Army’s ArMA system is possible. The bridge can either be a hardware device for smaller applications or virtual for larger systems. The Azure cloud has a Palo Alto firewall. This fits the “Cloud EMIS with hardware or software changes (Figure 9)” categories. The CERL installation riser diagram is shown in Figure 14.

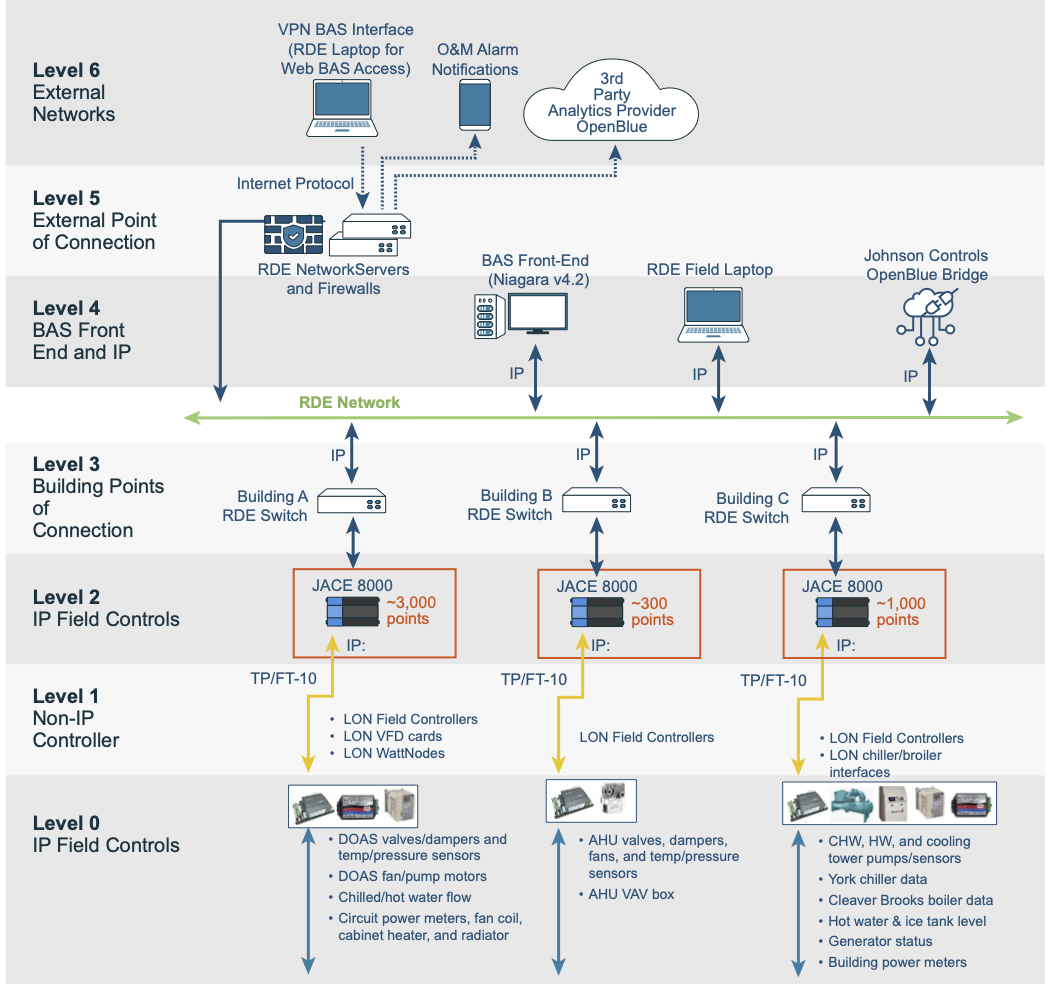


Figure 14: EMIS Installation diagram at CERL

## 

# **6. Cybersecurity Considerations**

Understanding and integrating the correct cybersecurity requirements during the systems engineering and acquisition process for EMIS is critical to delivering building and architectures for DoD that are secure, cyber-resilient, and ready to go through the DoDI 8570 Risk Management Framework (RMF) process and obtain an ATO if they are going to connect to the DoD Information Network (DODIN). A Stand-Alone Contractor Owned and Operated project should also go through the RMF process but would not get a DoD ATO; they would manage their ATO internally.

Cybersecurity requirements are now contractually required for third-party energy service providers to ensure that both DoDIN and DoD Controlled Unclassified Information (CUI) data are protected from cyberthreats, and that third parties who provide energy services to DoD are able to detect, mitigate, and recover from a cyberattack. Energy security, resilience, and cybersecurity are foundational elements for installation Mission Assurance.

It is recommended that the Project Team include experienced contractor Cybersecurity Subject Matter Experts (SMEs) who will prepare the Cybersecurity Basis Of Design and the 25-05-11, 25-08-10, and 25-10-10 specifications. In the case of the Army, personnel from United States Army Corps of Engineers (USACE) Huntsville CSC-MCX provide project review of the Project Team submittals to ensure cybersecurity requirements and controls are in building design and acquisition efforts to deliver low risk and highly cyber-resilient, RMF-accreditable EMIS solutions.

Establishing Service Level Agreements (SLAs) with IT groups may be required. Additionally, it is crucial to involve the IT group, and recommended to have them provide training on the EMIS implementation. This training should cover how the EMIS integrates with the front-end UMCS and emphasize the importance of the IT group's role in the successful implementation and operation of the EMIS.

## Risk Management Framework

Refer to UFC 04-010-06 and UFGS 25 08 11.00 20 (Navy specific RMF procedures) for detailed explanations of, and instructions for, the UFC RMF and ATO processes. For ACSME, the installation IT staff should coordinate efforts for the RMF ATO with DPW staff to include the facility level components in the ACSME accreditation. In the Army, generally the Network Enterprise Center (NEC) hosts the UMCS HVAC DDC and AMI servers and connects over the ICAN.

## Applying cybersecurity during design

It is critical that stakeholders, acquisition professionals, designers, and other contractors work closely together during the entire design process to ensure that the system is designed securely in accordance with DoD cybersecurity requirements, and that risk cost is reduced effectively.

The Facility-Related Control System (FRCS) System Owner (SO) should assemble representatives from the following communities to participate in development of the FRCS Platform Enclave (PE) Authorization Boundary and Network Architecture:

* Facility Engineer/Manager/System Owner
* Facility Operations & Maintenance/Technician
* Physical Security Specialist
* Emergency Manager
* IT Network/Communications Specialist
* Information Assurance Specialist
* Tenants (e.g., Defense Health Agency, Defense Logistics Agency)
* Operations and Maintenance Contractors
* Information Assurance/RMF Contractor
* Authorizing Official
* Authorizing Official Designated Representative
* Information System Security Manager
* Information System Security Officer
* Information System Security Engineer
* USACE Cyber Center of Expertise, NAVFAC Command Information Officer (CIO), Air Force Center Engineering Center

## Security controls and requirements

Security control requirements are mandated on control systems and associated networks by various DoD and Army policies and instructions. UFC 4-010-06 “Cybersecurity of Facility Related Control Systems” states the following:

“DoD Instructions 8500.01 and 8510.01 define the RMF for the DoD and establish a category for ‘special purpose’ systems that are not traditional information technology or information systems, called Platform Information Technology (PIT) systems. These PIT systems, including control systems, use specifically tailored security control sets and require the AO to have expertise in the system. The selection of the set of security controls to implement for a given system is the responsibility of the AO. The designer provides input into security control selection by advising on the feasibility and potential impacts of applying a security control.”

The Designer coordinates with the SO and CIO to confirm the systems to be included within the Authorization Boundary and the Confidentiality, Availability and Confidentiality (C-I-A) Impact Values, and must edit the UFGS 25-05-11, 25-08-10, 25-10-10 and Navy-specific 01-35-13.02 and 25-08-11.0020 specifications to incorporate the correct controls.

## Inherited controls and cybersecurity services integration plan

Cybersecurity services and cybersecurity controls, when appropriate, should be inherited from the installation or regional level ICAN / NEC, the Army DODIN-A network, or other DoD authorized networks as required. These networks and the staff that manage them should provide the following to the ACSME and the FRCS community of interest zones, and are not the responsibility of the designer to implement. The designer and the Army IT staff should collaborate to properly integrate these into the EMIS design. EMIS designers during construction projects or renovation should collaborate closely from the earliest stages of the facility or EMIS project to integrate the facility Level 2 and FPOC into the larger installation UMCS networks and NEC operated by the Army installation IT staff and G6. The following are some but not all the possible requirements that should be designed, planned, and funded in collaboration with Army IT staff and included into the Army Installation Master Plan:

* 1. Network connectivity and network connection management between Level 3 and Level 5 of the Army representative network architecture.
  2. Network segmentation (virtual local area networks (VLANs) and subnets) specific for the ACSME and the different COI zones within the FRCS environment.
  3. Management and deployment of Host Based Security System (HBSS) policies for the ACSME COI and other control systems as required.
  4. Vulnerability assessment and scan policies for FRCS network segments and VLANs from the ACAS.
  5. Cybersecurity situational awareness – security information and event management (SIEM) of FRCS components and network segments.
  6. Intrusion detection system (IDS) and intrusion prevention system (IPS) operations for FRCS network segments and VLANs (within DoD this service is the HBSS/ACAS applications).

## Construction and delivery phases

Cybersecurity during the Construction Phase is a combination of (1) Protecting the CUI, which includes materials such as drawings, specifications, user manuals, configuration, and programming, and passwords that reside on the Project Team business machines to design, construct, and operate the EMIS, and (2) installing and operating the EMIS components per the UFC and UFGS. Figure 16 represents the PIT Life Cycle.

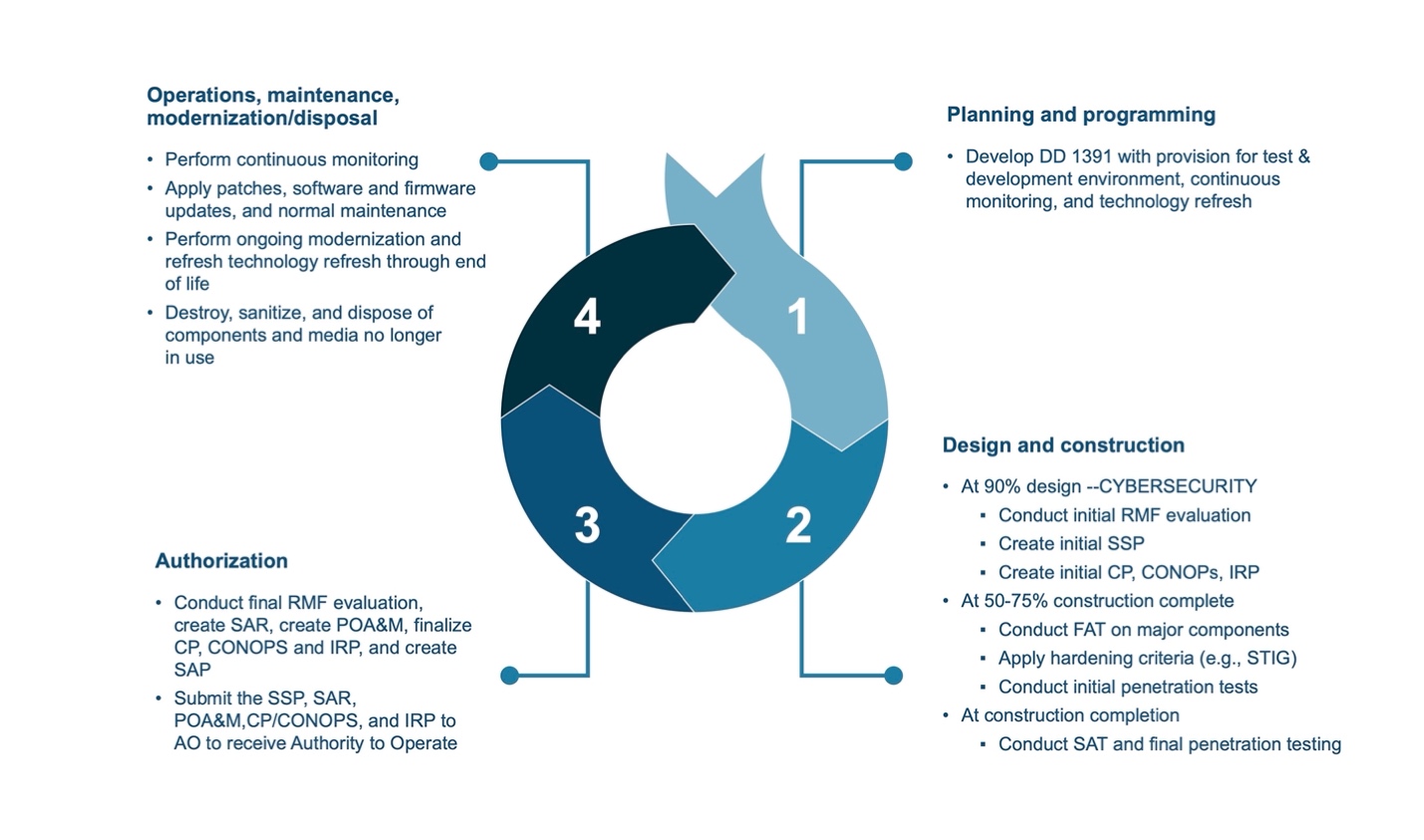


Figure 16: PIT Life Cycle

Key milestones through the 35% Construction Complete Phase are the SD-01 Pre-Construction Submittals, the SD-02 Shop Drawings, and the SD-03 Product Data Sheets. The Cybersecurity Team review ensures the products selected comply with DoD standards.

Key milestones through the 65% Construction Complete Phase are the SD-06 Test Reports, which includes the Factory Acceptance Testing Configuration Baseline Security Audit Report and Artifacts. The Cybersecurity Team provisions all of the servers, workstations, laptops, controllers, and HVAC, while the Controls contractor installs the HVAC and EMIS applications. The Cybersecurity Team captures all operating system (OS) and Application configurations in the Artifacts and Report. The components are installed into the building and begin the process of connecting the various DDC panels to the floors, zones, and equipment. The Controls, HVAC, Lighting, and Fire contractors continue the construction and connecting components, and programming of HMI graphics and reports. The Cybersecurity Team and HVAC and Controls contractors will perform regular OS and Application updates and perform Continuous Monitoring to ensure the system is clean and does not have any malware or vulnerabilities that could be exploited. The Factory Acceptance Testing and Site Acceptance Testing (FAT SAT) Checklist is also completed, along with any Service specific checklists such as the NAVAFC ICS Checklist. During construction, the Cybersecurity Team are the System Administrators and manage the internal completion of the RMF security controls; depending on the service, the Cybersecurity Team may only be required to provide the RMF (CIO ATO repository tool) Artifacts, or may be required to manage the full upload and RMF ATO process.

Key milestones through the 95% Construction Complete Phase are the SD-06 Test Reports, SD-07 Licenses, and SD-11 Close Out Documents. The Cybersecurity Team re-provisions all of the servers, workstations, laptops, controllers, and components that are installed in the building. The Controls, HVAC, Lighting, and Fire contractors conduct Performance Verification Testing. The Information System Security Officer (ISSO) or Information System Security Engineer (ISSE) provisions the switches that will connect each building to the Platform Enclave, and the Controls contractors typically install them in the Master DDC panel. The Project Cybersecurity Team and the Service commissioning team perform activities on the Site Acceptance Testing Cyber Commissioning checklists and upon approval, the ISSO or ISSE will connect to the Platform Enclave, remove the Cyber Team System Administration credentials, and become responsible for maintaining the configuration and OS updates with assistance from the Cybersecurity Team.

Finally at Project Turnover and the completion of the DD Form 1354 Real Property Transfer, the Cybersecurity team moves into an Operations and Maintenance (O&M) Warranty support phase, unless the system will be a Stand-Alone Network UESC or ESPC Owner Owned and Operated one, and *not* be connected to the Platform Enclave, in which case the Cybersecurity Team continues as the System Administrators and performs the Continuous Monitoring.

# **References**

Air Force installation energy vision. (2021). https://www.secnav.navy.mil/eie/Documents/DON-Installation-Energy-Resilience-Strategy.pdf

Army Installation Energy and Water Strategic Plan. (2020). https://www.asaie.army.mil/sites/default/files/PDF/Army\_Installation\_Energy\_and\_Water\_Stategic\_Plan\_FINAL.pdf

Baker, G. D. (2008). The Energy Independence and Security Act of 2007: Toward a More Energy Efficient America (Part 1). Structure, 47(2). https://heinonline.org/hol-cgi-bin/get\_pdf.cgi?handle=hein.journals/infrastr47&section=3

Bush, J., Westervelt, E. T., Clark, B. C., Schwenk, D. M., Briggs, S. J., Shepard, D. A., Long, M. C., Patel, T. C., Johnson, M. D., & Lynch, E. D. (2022). Installation utility monitoring and control system technical guide. https://erdc-library.erdc.dren.mil/jspui/handle/11681/45081

Degette, D, (2020). Clean Energy Innovation and Deployment Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/7516/text

Department of Defence, S. (2014). UFC High Performance and Sustainable Building Requirements. Change, 3, 7.

Department of the Navy Installation Energy Resiliency Strategy. (2020). https://www.secnav.navy.mil/eie/Documents/DON-Installation-Energy-Resilience-Strategy.pdf

DoD. (2011). DOD Product Support Business Case Analysis Guidebook.

Federal Energy Management Program. (2023). Energy Savings Performance Contracts for Federal Agencies. https://www.energy.gov/femp/energy-savings-performance-contracts-federal-agencies

General Services Administration. (2023). Energy Management Information System with Automated System Optimization. https://www.gsa.gov/climate-action-and-sustainability/center-for-emerging-building-technologies/completed-assessments/energy-management/energy-management-information-system-with-automated-system-optimization

Greenley, H. (2019). Department of Defense Energy Management: Background and Issues for Congress. https://sgp.fas.org/crs/natsec/R45832.pdf

Kramer, H., Lin, G., Curtin, C., Crowe, E., & Granderson, J. (2020). Proving the business case for building analytics. Lawrence Berkeley National Laboratory, Berkeley, CA (United States). https://www.osti.gov/biblio/1695762

Lawrence Berkeley National Laboratory. (2020). EMIS Specification and Procurement Support Materials. DOE Better Buildings.

Unified Facilities Criteria: Cybersecurity of facility-related control systems. (2023). https://www.wbdg.org/FFC/DOD/UFC/ufc\_4\_010\_06\_2023.pdf

Utility Monitoring and Control System Front end and Integration. (2018). https://www.wbdg.org/FFC/DOD/UFC/ufc\_3\_470\_01\_2018.pdf

1. <https://www.serdp-estcp.mil/> [↑](#footnote-ref-1)
2. https://www.gsa.gov/technology/government-it-initiatives/fedramp [↑](#footnote-ref-2)
3. https://wbdg.org/ [↑](#footnote-ref-3)