2017

Air Force Civil Engineer Energy Savings Performance Contracts (ESPC) Playbook

This Playbook is an electronic document. The only valid version is the latest version on the CE Portal. Click here to go to the CE Portal. Publish Date: 01/08/2018

Table of Contents

Table of Figures

Table of Tables

Chapter 1 Introduction – Energy Savings Performance Contracts (ESPC)

The objective of the ESPC Playbook is to provide the parameters and guidance used by the United States Air Force for implementing an ESPC. This Playbook replaces Air Force Engineering Technical Letter (ETL) 13-13 Energy Savings Performance Contracts (ESPC) dated 15 Aug 2013. This Playbook contains a basic history of the ESPC program, primary roles and responsibilities, step-by-step instructions, job aids, and reference documents to ensure ESPC procedures are followed. Requirements in this ESPC Playbook are mandatory. Any deviations require written approval from the ESPC program manager, Air Force Civil Engineer Center, Energy Program Development Division (AFCEC/CND). This Playbook applies to all ESPC work.

Job Aids, resources and reference materials are provided digitally in Links and can be modified as required by AFCEC/CND.

Limitations: This Playbook does not replace, supersede, or circumvent existing Department of Defense (DoD) or Air Force (AF) policy.

Applicability: This Playbook is written for the following personnel: AFCEC/CND; Base Civil Engineers (BCE); Base Energy Managers (BEM); Base Financial Managers (BFM); Base Contracting Officers (CO); Resource Efficiency Managers (REM); Assistant Secretary of the Air Force Installations, Environment and Energy (SAF/IE); Energy Services Company (ESCO) personnel; and Air Force Installation and Mission Support Center (AFIMSC) personnel.

Chapter 2 ESPC Background, Authority, Financing and Funding

2.1 ESPC Background

The ESPC legislation allows the AF to implement infrastructure improvements without current year funds. An ESPC is a contract in which an ESCO designs, constructs, implements, operates, maintains, and arranges the necessary funding of improvements that reduce energy and water consumption and promote the use of renewable energy technologies. ESPCs enable the AF to improve energy performance while addressing aging infrastructure concerns and reducing consumption, through a budget-neutral approach.

ESPCs are utilized for reducing energy consumption at an installation through improvements to infrastructure, facilities, and facility systems. ESPCs can be used to replace inefficient energy and water-consuming equipment including HVAC, lighting, electrical power generation, and renewable energy. A full listing of available technologies is provided in the technical categories under Section 4.1. ESPC can also be used to reduce process energy within buildings, including, but not limited to, process equipment; or research, development, test and evaluation (RDT&E) equipment. Any initiative that results in a net decrease in future energy or water costs can be considered for ESPC or other third-party financing options. Under an ESPC, the ESCO:

1. Identifies the building and/or equipment energy savings potential.
2. Finances the capital costs using private sector funding.
3. Acquires, installs, operates, and maintains the equipment for the life of the contract.
4. Guarantees savings for the life of the task order.

The ESCO receives a payment from the agencies utility service account based on meeting the guaranteed energy savings until the individual task order (TO) is paid off. The AF takes ownership of the equipment upon completion of installation.

2.2 Authority

The following table lists the Executive Orders (E.O.), directives, and policies that mandate and support the AF ESPC energy reduction program:

Air Force Policy Directive (AFPD) 32-10, Installations and Facilities
Title 42, United States Code (U.S.C.), Section 8287, National Energy Conservation Policy Act
10 U.S.C. 2911-13, Energy Performance Goals and Plans for Department of Defense
42 U.S.C. 8253, Energy Policy Act of 1992
E.O. 13423, Strengthening Federal Environmental, Energy, and Transportation Management (revoked in 2015). Replaced by: E.O. 13693, Planning for Federal Sustainability in the Next Decade
E.O. 13514, Federal Leadership in Environmental, Energy, and Economic Performance (revoked in 2015). Replaced by: E.O. 13693, Planning for Federal Sustainability in the Next Decade
Energy Policy Act of 2005
10 Code of Federal Regulations (CFR) 436, Federal Energy Management and Planning Programs
Energy Independence and Security Act (EISA) of 2007

Table 1 Authority Documents Mandating the AF ESPC Program

The EISA of 2007 tasked the AF to reduce energy consumption. E.O. 13693 maintains federal leadership in sustainability and greenhouse gas emission reductions. E.O. 13693 specifically states beginning in fiscal year 2016, all federal agencies shall, where life-cycle cost-effective, promote building energy conservation, efficiency, and management. This will be accomplished by reducing building energy intensity measured in MBTU/SF by 2.5 percent annually through the end of fiscal year 2025, relative to the baseline of the agency's building energy use in fiscal year 2015.

2.3 Financing ESPCs

The National Energy Conservation Policy Act (42 U.S.C. 8287) provides legislative authority for federal agencies to enter an ESPC, including:

1. The AF can acquire contracts with ESCOs to obtain energy-conserving infrastructure improvements.
2. ESCO contracts must guarantee savings and overall utility costs to the installation cannot increase because of the contract.
3. The savings generated by the infrastructure improvements must be a result of the ESCO's efforts and investment.
4. The use of an ESPC requires a detailed understanding of its basic principles, how costs are assessed, and how risks are managed.

ESPC projects are funded solely from the cost savings they generate or avoid. All ESPC costs, including mid-contract replacement of capital equipment, are funded from ESPC savings. An installation's post-ESPC utility costs (i.e., energy and operations and maintenance [O&M]) plus the cost of the ESPC project cannot exceed the utilities costs prior to implementation of the ESPC project. Thus, the costs cannot exceed the savings (i.e., energy and O&M) generated by the projects. The payment to the ESCO is contingent upon annual verification by the Government that the guaranteed savings have been realized. Refer to the DoE letter to ESCOs for more information.

The ESCO is responsible for the design, acquisition, installation, Measurement and Verification (M&V), and maintenance of the project's equipment or systems that produce the savings. An ESPC requires the ESCO to guarantee the savings generated by, and the operation of the installed equipment. This guarantee must be satisfied and verified at the acceptance of the equipment and revalidated annually throughout the life of the TO.

2.3.1 Energy Cost Savings

Energy Costs Savings are one time or recurring energy cost savings that can be utilized to fund an ESPC. An ESPC is budget neutral; actual funds need to be saved or generated to pay the ESCO. The funds can be generated from O&M, cancellation of vendor contracts, material reductions, avoided costs or utility savings. An ESPC cannot utilize funding from MILCON or conduct MILCON actions. Additionally, installations should be aware re-vectoring of resources does not generate fiscal savings (e.g., ESPCs do not impact manpower, and thus manpower savings cannot be claimed). Types of cost savings that can be utilized include the following:

1. Reductions in expenses (other than energy costs) related to energy-consuming equipment affecting operations, maintenance, renewal or repair expenses of equipment; and costs associated with waste disposal, such as waste disposal fees.
2. As part of initial award, the costs savings from avoided expenditures for O&M, repair, replacement, or other capital expenditures can be utilized to assist in paying down an ESPC. Coordination with the appropriate AFCEC divisions is required. Investments can include both facility (real property and Real Property Installed Equipment [RPIE]) improvements and equipment (non-RPIE, such as kitchen equipment).
3. Reduction in utility commodity consumption, in comparison to normalized baseline, for natural gas, electrical power, water, sewer, propane, etc.

Certain risks are associated with implementing an ESPC for both the AF and the ESCO. It is essential the AF does not assume any of the ESCO's risk.

AF risks during the life of the TO	ESCO risks during the life of the TO
Utility rates	ECM performance
Hours of operations	ECM maintenance
Mission changes	Guaranteed savings

Table 2 ESPC Risks

The ESCO will provide a guarantee of cost savings to the AF and establish payment schedules reflecting this guarantee, considering any capital costs under the contract. The ESCO provides these figures for each year of the TO. The actual payment to the ESCO is based on an agreed percentage of the calculated energy savings. These awarded TOs, like utility bills, are "must-pay" requirements and are programmed into the annual utility budget process.

Aggregate annual payments by the AF under an ESPC may not exceed the amount the agency would have paid for utilities without an ESPC during the TO term. ESPC costs can never exceed the energy and O&M savings. Forecasted energy costs and the discount rate (present value of future cash flows) are major factors in determining ESPC savings. 10 CFR 436, *Federal Energy Management and Planning Programs*, provides detailed instructions for ESPCs, including the calculation of life cycle costs. Guidance from the Federal Energy Management Program (FEMP) states that the escalation rates for ESPCs are based on the Nominal Escalation Rate for each commodity as calculated by latest version of the National Institute for Standards and Technology (NIST) software program called the Energy Escalation Rate Calculator (EERC). EERC 2.0-17 (use most current version) is available for download from the FEMP website, http://www.energy.gov/eere/femp/energy-escalation-rate-calculator-download. Individual escalation rates must be used for each commodity. Users of the EERC tool need only specify 100% for a single fuel type, identify the state in which their prospective project will take place, select industrial sector for AF installations, the expected start date (award year) and duration of the project. With that, the tool will determine an escalation rate for each fuel type. The provisions in 10 CFR 436.14 are mandatory, and failure to comply will result in the contract being legally insufficient. Refer to the Energy Price Indices and Discount Factors for Life-Cycle Cost Analysis – 2016 Annual Supplement to NIST Handbook 135 (or latest version), which provides detailed forecasted energy cost information. Refer to ESPC Escalation Rate Guidance for more information on how to determine and use escalation rates.

2.3.2 Maintenance Responsibilities and Funding

The ESCO is responsible for all costs relating to the performance guarantee, including labor, supplies, parts, and materials for the term of the TO. ESCOs are responsible for all maintenance and repairs during the term of the TO. The exception to this is when the ESCO and AF mutually agree upon certain cases (such as lighting), where the installation may physically perform the maintenance as long as the ESCO retains the ultimate responsibility for maintenance for the length of the TO. However, this needs approval by AFCEC/CND and the language in the TO must clearly state the ESCO is:

1. Not transferring this responsibility to the installation.
2. Responsible for maintenance and repair services for any energy-related equipment (including computer software systems) and there is no connection between ECM performance and associated ECM maintenance.
3. Required to oversee and ensure all maintenance is performed as required for each ECP within the TO.

If approved by AFCEC/CND, the installation may require the ESCO to provide all parts and materials needed to accomplish installation performed maintenance. All parts and materials needed to maintain and repair an ECM must be paid from captured O&M or energy savings. Without capturing these savings, the government cannot assure the funds are available to cover future O&M costs necessary for maintaining equipment performance.

Note: If equipment is replaced and there is a replacement cost, energy savings can only be captured if the equipment is installed by the ESCO and the ESCO remains responsible for its performance.

2.3.3 Capturing ESPC Savings

The National Energy Conservation Policy Act (42 U.S.C. 8287) does not explicitly state where ESPC savings must come from, however, utility energy savings and avoided maintenance costs can be included. Use caution if applying anticipated cost avoidance to the ESPC due to major repair/replacement that may not be needed because of the ESPC. If these major expenditures are included as captured savings, they become a must-pay bill from O&M funds. Before these funds are included in an ESPC, the installation and Funding Source Program Manager must agree to the funding source and create a record of decision to justify the action and agreement and submit to AFCEC/CND. (See Section 8287a of 42 U.S.C. 8287) Keep in mind that:

1. Savings must be real and verifiable so the installation doesn't run the risk of a savings shortfall. The AF requires that 2/3 of all energy savings must be metered, with a strong preference for IPMVP Option C.
2. Work that encompasses O&M-type savings or other savings that do not eliminate actual costs or produce "actual savings" (real $) versus "avoided costs" (hypothetical $) will not be included.

2.3.4 Annual Reconciliation

Verification of energy savings reconciliation is required to be accomplished for each awarded TO annually. This requirement includes:

1. An approved M&V plan using at least the current International Performance Measurement and Verification Protocol (IPMVP) at the time the TO was awarded.
2. During the annual reconciliation, the ESCO will confirm the adequacy of maintenance. (See paragraph (a)(2)(A) of 42 U.S.C. 8287.)
3. The BEM or substitute must validate that the ESCO's annual reconciliation requirement is performed in accordance with the M&V plan. AFCEC/CND is available to provide support and ensure this requirement is met.

2.3.5 Buy-down and Buyout

ESPCs can be funded in-part with installation funds. For example, end-of-year fallout funds, or current FY or FY+1 project funds, can be used to buy down part of the TO. These one-time funds can be identified in the payment schedule to the ESCO upon acceptance of the ECM and commencement of the performance period. This allows for a lower financed amount and shorter term, thereby reducing interest costs over the term. If, after award, O&M funds are used to buy-down a portion of the TO, several steps are necessary:

1. The use of these funds is identified as soon as possible to the ESCO.
2. The economics are considered and justified.
3. Prepayment penalties are identified by the ESCO.
4. The life expectancy of the equipment is considered (i.e., in year 11 of a 20-year TO term, it would not be wise to buy out a piece of equipment that has a life expectancy of 10 years).

Alternatively, these funds can be applied as scheduled payments during the performance period.

When government actions (e.g., removal or demolition of installed ESCO equipment, or mission changes) result in annual guaranteed savings falling below annual payments to the ESCO and the TO term cannot be extended, the buyout provision of the ECP and/or ECM can be exercised. The TO is required to clearly identify the penalties associated with the buyouts.

2.4 Funding Requirements

42 U.S.C. 8287 requires that energy savings provide the future payments on the initial project capital investment. While the AF is limited to the use of energy savings to pay off the initial investment, there is no such limitation on the type of initial investments (purchases) that an ESCO can make. This allows for a wider range when considering ESPC project types such as test equipment (wind tunnels), maintenance and processes/equipment. As long as the primary savings are energy/water related, ESPCs can be used across multiple AF organizations.

Government actions (post award) on a building that will impact, alter or dismantle ESPC material or equipment, rendering that part of the ESPC contract invalid, the government should buyout the applicable portion of the contract. Examples include demolition, upgrades, construction and privatization.

If possible, buyout funds should be programmed with the same government fund source as the project itself; however, this may not be possible with all project categories. The AF, to the

maximum extent possible, should look to exclude facilities/ECMs that would be affected by any of the factors above at the time of award or during initial scope development.

The following additional funding rules apply:

1. Military Construction (MILCON) funds, including Energy Conservation Investment Program (ECIP), cannot be applied to an ESPC. MILCON rules do not permit augmenting funds (O&M/utility) with MILCON funds.
2. Non-appropriated Fund (NAF) functions may or may not be authorized to supplement appropriated O&M funds. NAF Category C ECPs must use savings only from other NAF ECPs to avoid subsidizing or being subsidized by other than NAF-funded sources. All actions affecting funding must be coordinated with the NAF funds manager.
3. Military Family Housing (MFH) funds are appropriated separately and used specifically for MFH purposes. MFH ECPs must use savings only from other MFH ECPs to avoid subsidizing or being subsidized by other than MFH-funded sources.
4. Reimbursable customers require separate accounting procedures to ensure adequate payments are applied to their accounts.

Chapter 3 ESPC Roles and Responsibilities

This chapter provides an in-depth explanation of the roles and responsibilities associated with the ESPC process.

3.1 AFCEC/CND Roles and Responsibilities

a. Serves as the central Program Management Office (PMO). Refer to the 2013 Policy Memorandum and the 2010 ESPC Policy Letter for more guidance. Oversees **all** ESPC projects. Provides review and approvals for all stages of ESPC projects, including initial scope, Preliminary Assessment (PA), Investment Grade Audit (IGA), pre-award and post award M&V. Responsible for ESPC budgets and schedules.

b. Determines which contracting office to use, either 772 Enterprise Sourcing Squadron (ESS), Defense Logistics Agency (DLA) Energy or Huntsville Engineering and Support Center (HNC).

c. Provides project engineers who manage individual ESPC projects, FEMP approved Project Facilitator (PF), oversee project schedule and timeline, and coordinates with CO/ESCO/COTRs.

d. Develops ESPC procedures and guidance. Provides training on using and implementing the ESPC to the CO, BEM, Civil Engineer (CE) financial manager, BFM, and a representative from the installation's legal office.

e. Assists installations with developing the ESPC project through award and completion of TO terms; evaluates proposals, provides vetting review and approves each state of project development.

f. Maintains and posts all releasable ESPC documentation to the eDash website.

g. Reviews and provides comments and guidance on submissions from the ESCOs, including PAs, IGAs, RFIs and other documents. Refer to the IGA Review Checklist and the PA Review Checklist for guidance.

h. Provides tools and expertise to assist in implementing an ESPC and acts as a clearinghouse for ESPC lessons learned.

i. Maintains oversight and compliance with AF policies and interprets guidance for the installation's ESPC program.

j. Provides access to engineering subject matter experts (SMEs).

k. Provides project vetting and ensures the ESPC contract vehicle is appropriate for the recommended ECMs.

l. Provides M&V expertise and support during development, commissioning, and annual M&V reports.

m. Determines if support services are needed after a proposal is complete. Refer to the FEMP Support Services job aid for more information about available services.

3.2 PF Roles and Responsibilities (AFCEC/CND provides PF)

a. Utilizes the FEMP ESPC Project Development Guide, which charts the ESPC process, providing project development support to agencies developing ESPC projects using the DoE Indefinite Delivery/Indefinite Quantity (IDIQ) ESPC.

b. The guide outlines resources that PFs are required to use in the delivery of project development services and provides project documentation templates.

Note: ESPC projects are required to work with a FEMP approved federal PF. PFs are experienced, unbiased advisors who guide the agency acquisition team through the ESPC process. AFCEC/CND will provide their own DoE approved PFs at no cost to the project.

3.3 772 ESS CO Roles and Responsibilities (If selected as the acquisition agent)

a. Overall responsibility to ensure that ESPC projects serve the best interests of the AF and are consistent with the terms and conditions of the ESPC contracts, legislation, and regulations.

b. Coordinates with AFCEC/CND and Department of Energy (DoE) Federal Financing Specialist (FFS) for use of DoE ESPC contracts.

c. Performs all pre-award acquisition functions and awards ESPC TOs.

d. Provides the total contract cost for each phase of an ESPC and a final signed copy of the TO to AFCEC/CND for tracking the contract ceiling.

1. For a Preliminary Assessment (PA) report, include the estimated investment cost provided by the ESCO. Refer to the PA Review Checklist for guidance.

2. For the Investment Grade Audit (IGA) report, include the final negotiated contract amount encompassing the total cost over the life of the contract. Refer to the IGA Review Checklist for guidance.

3.4 Administration Contracting Officer (ACO) Roles and Responsibilities

a. Overall post-award responsibility to ensure that ESPC projects are administered in accordance with the terms and conditions of the ESPC contracts.

b. Oversees construction management oversight and day-to-day interaction with the ESCO.

c. Ensures M&V is performed and annual report is received from the ESCO annually and all ESCO maintenance is performed in accordance with the TO.

d. Informs CO of any issues/problems arising that changes the scope and/or cost of the task order and issues modifications as necessary after coordination with the CO.

3.5 CO Roles and Responsibilities

a. Overall responsibility to ensure that ESPC projects serve the best interests of the AF and are consistent with the terms and conditions of the ESPC contracts, legislation, and regulations.

b. Develops contract documents.

c. Ensures scope and pricing are in the best interest of the government.

d. Awards TO to the chosen ESCO.

e. Ensures invoices are received and paid through the term of the contract.

3.6 COTR Roles and Responsibilities

a. Acts as technical representative for CO.

b. Identifies and supports project goals and development efforts.

c. Reviews deliverables.

d. Provides oversight during construction and installation.

e. Reviews and approves technical aspects of the annual M&V reports.

3.7 DLA Energy Roles and Responsibilities (If selected as the acquisition agent)

a. Overall responsibility to ensure ESPC projects serve the best interests of the Federal Government and are consistent with the terms and conditions of the ESPC contracts, legislation, and regulations.

b. Performs all pre-award acquisition functions and awards ESPC TOs.

c. DLA Energy acts as ACO.

d. Provides the total contract cost for each phase of an ESPC and a final signed copy of the TO to AFCEC/CND for tracking the contract ceiling.

   1. For a PA report, include the estimated investment cost provided by the ESCO. Refer to the PA Review Checklist for guidance.

   2. For the IGA report, include the final negotiated contract amount encompassing the total cost over the life of the contract. Refer to the IGA Review Checklist for guidance.

3.8 HNC, United States Army Corps of Engineers (USACE) Roles and Responsibilities (If selected as the acquisition agent)

a. Overall responsibility to ensure ESPC projects serve the best interests of the Federal Government and are consistent with the terms and conditions of the ESPC contracts, legislation, and regulations.

b. Performs all pre-award acquisition functions and awards ESPC TOs.

c. Provides the total contract cost for each phase of an ESPC and a final signed copy of the TO to AFCEC/CND for tracking the contract ceiling.

   1. For a PA report, include the estimated investment cost provided by the ESCO. Refer to the PA Review Checklist for guidance.

   2. For the IGA report, include the final negotiated contract amount encompassing the total cost over the life of the contract. Refer to the IGA Review Checklist for guidance.

3.9 ESCO Roles and Responsibilities

a. Responds to Request for Proposal (RFP) or Notice of Opportunity (NoO) for an ESPC.

b. Develops and submits a PA. Refer to the PA Review Checklist for guidance.

c. Conducts an IGA. Refer to the IGA Review Checklist for guidance.

d. Clearly documents the baseline data and ensures the data accurately justifies the baseline.

e. Provides upfront funding for energy reduction project(s).

f. Design and Implements the ESPC project, including purchasing equipment, installing equipment, and overseeing and completing construction during projects.

g. Provides all operation and maintenance for the ESPC.

h. Performs metering and data collection to validate guaranteed savings.

3.10 BCE Roles and Responsibilities

a. Works with the CO to implement the ESPC project. Compiles and provides required project documentation, including site data packages and evaluation criteria to the CO.

b. Ensures that ESPC project documentation is submitted to AFCEC/CND for vetting and approval prior to proceeding to the next phase. Phases include initial scope, PA, IGA, pre-award documentation, M&V plans, post award documentation and M&V reports.

c. Ensures the BEM completes the ESPC training available on the FEMP web page before implementing an ESPC program and newly assigned personnel associated with the ESPC program receive this training for the term of the ESPC. The CE financial manager, BFM, and a representative from the installation's legal office should attend this training to learn their responsibilities with regards to an ESPC project.

d. Ensures the ESCO complies with M&V and O&M requirements for the term of the TO.

e. Annually verifies the ESCO is meeting the guaranteed savings based on the requirements of the M&V plan for the term of the contract.

f. Provides a copy of the ESCO's annual reconciliation report to AFCEC/CND.

g. Appoints a Contracting Officer Technical Representative (COTR) for ESPC project.

h. Provides power, water, and sewer during ESPC construction with laydown yard.

Chapter 4 ESPC Process

This chapter explains the ESPC process, broken down into steps that are clear and easy to follow. For each step, there is a process map to assist in understanding the overall ESPC process. Refer to the ESPC Engagement Guidance document for more information on the ESPC process. (It is important to point out that the AF incurs no cost unless the TO is awarded.) Note: DoE IDIQ H.6.2 proposals will be reviewed in accordance with the instructions set forth in the TO-RFP. The agency will not be responsible for any costs incurred, such as proposal preparation costs or the costs incurred in conducting the IGA, unless a TO is awarded or authorized by the agency CO.

Note: Before an ESPC is underway via contracting, ESCOs are allowed to visit installations to market their capabilities and past performance. During pre-ESPC visits, **ESCOs are not allowed to visit buildings at installations, not allowed to discuss existing conditions at installations, and not allowed to discuss scope of potential future ESPC projects.** Refer to ESPC Engagement Guidance for more information. Doing so puts the ESCO at risk of being eliminated from the competitive selection process. There must be no real or implied government commitments to a specific ESCO. Interaction at this point that constitutes actual or perceived government obligation must be avoided.

4.1 ESPC Initiation

The ESPC process begins at the installation. The BCE initiates the ESPC process by contacting AFCEC/CND to request support in developing and implementing the project.

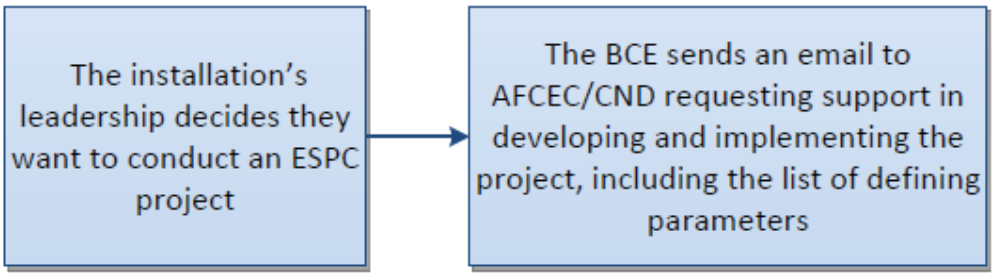


Figure 1 Installation Process Map

Step 1: **The installation's leadership decides they want to conduct an ESPC project.**

The BEM is the primary driver behind improving the installation's energy efficiency. Energy audits and REMs can assist BEMs to identify ESPC candidates and ECMs. Facility managers, process owners and operations staffs are good sources for ideas on improving their building's operational characteristics. The local staff often has the best understanding of what equipment is failing or not operating in a proper manner due to design defects, age, or other reasons. Refer to ESPC Considerations for BEM for information on the BEMs roles and responsibilities in the ESPC process.

When developing the ECM and facility list, the installation should be mindful that an ESCO's costs and overhead will be greater for widely scattered buildings than it will be for buildings clustered together. Ensure the building packages are structured to take maximum advantage of project economics. Include the less desirable projects with the more attractive projects and ensure the ESCO takes them as a package. The best economical ECMs subsidize the less economical work such as chiller and cooling tower replacement. In addition, the best economical ECMs can subsidize energy assurance or resilience ECMs. Note: not all of an installation's opportunities/projects lend themselves to ESPC project execution.

Step 2: The BCE sends an email to AFCEC/CND requesting support in developing and implementing the project, including the list of defining parameters.

Prior to formally engaging with an ESCO, an interaction that constitutes actual or perceived government obligation, the BEM/BCE prepares a summary of the type of ECMs being considered. Use the Base Submittal Spreadsheet job aid to help in preparing the ECM summary. This summary includes relevant baseline information and estimates of installation and individual facility energy usage. Submit the proposed ESPC projects to AFCEC/CND for vetting. Refer to Table 3 below for a general list of approved ESPC energy improvement project categories.

ESPCs are used where they make good business sense and when necessary to achieve energy goals. AFCEC/CND approves each stage of the project development and evaluation process and assists in awarding and administering the TO.

APPROVED ESPC ENERGY IMPROVEMENT PROJECT CATEGORIES	
ESPC TECHNOLOGY CATEGORIES	**ASSOCIATED ECMs**
1. Boiler Improvements - ECMs such as, but not limited to:	Boiler control, including new controls and retrofits to existing controls
	Replacement of existing boilers with high efficiency boilers
	Boiler decentralization
2. Chiller Improvements - ECMs such as, but not limited to:	Chiller retrofits or replacements
	Chiller plant pumping, piping, and controls retrofits and replacements
	Replacement of ice/refrigeration equipment with high efficiency units
3. Utility Monitoring Control Systems - ECMs such as, but not limited to:	Metering systems
	Digital control systems
	Monitoring systems
4. Heating, Ventilating, and Air-Conditioning (HVAC) (Not including Boilers, Chillers, and Utility Control Systems) - ECMs such as, but not limited to:	Packaged air conditioning unit replacements
	HVAC damper and controller repair or replacement
	Window air conditioning replacement with high efficiency units
	Cooling tower retrofits or replacements
	Economizer installation
	Fans and pump replacement or impeller trimming
	Thermal energy storage
	Variable air volume retrofit
5. Lighting Improvements* - ECMs such as, but not limited to:	Interior and exterior lighting retrofits and replacements
	Intelligent lighting controls
	Occupancy sensors
6. Building Envelope Modifications - ECMs such as, but not limited to:	Insulation installation
	Weatherization
	Window replacement
	Reflective solar window tinting
7. Water and Steam Distribution Systems - ECMs such as, but not limited to:	Piping insulation installation
	Hot water heater repair and replacement
	Steam trap repair and replacement
	Repair or replacement of existing condensate return systems and installation of new condensate return systems
8. Electric Motors and Drives - ECMs such as, but not limited to:	Motor replacement with high efficiency motors
	Variable speed motors or drives
9. Distributed Generation - ECMs such as, but not limited to:	Cogeneration systems installation
	Micro turbines installation
	Fuel cells installation

ESPC TECHNOLOGY CATEGORIES	ASSOCIATED ECMs
10. Renewable Energy Systems - ECMs such as, but not limited to:	Photovoltaic system installation
	Solar hot water system installation
	Solar ventilation preheating system installation
	Wind energy system installation
	Passive solar heating installation
	Landfill gas, waste water treatment plant digester gas, and coalbed methane power plant installation
	Wood waste and other organic waste stream heating or power plant installation
	Replacement of air conditioning and heating units with ground coupled heat pump systems
11. Energy/Utility Distribution Systems - ECMs such as, but not limited to:	Transformers installation
	Power quality upgrades
	Power factor correction
	Gas distribution systems installation
12. Water and Sewer Conservation Systems - ECMs such as, but not limited to:	Low-flow faucets and showerheads
	Low-flow plumbing equipment
	Water efficient irrigation
	On-site sewer treatment systems
13. Electrical Peak Shaving/Load Shifting - ECMs such as, but not limited to:	Thermal energy storage
	Battery energy storage system
	Gas cooling
14. Commissioning - ECMs such as, but not limited to:	Retro-commissioning services
	Continuous commissioning services
15. Requirements Ancillary to Energy Measure - Work efforts such as, but not limited to:	Envelope modification or improvements
	Interior modifications or improvements
	Electrical modification or improvements
	Plumbing modifications or improvements
	Protective housings for ECMs
16. Miscellaneous - ECMs such as, but not limited to:	Production and/or manufacturing improvements
	Recycling and other waste stream reductions
	Industrial process improvement
	Replace air-cooled ice/refrigeration equipment
	Replace refrigerators
	De-lamp vending machines
	Plug timers
	Energy Star® products
	Project Development Costs if separated

Table 3 Approved ESPC Energy Improvement Project Categories

*Note: Refer to UFC 3-530-01 Change 3 on TLED Requirements for more information in lighting requirements.

Note: Refer to ESPC Technology Categories and Associated ECMs for HNC, DLA or 772 executed ESPC projects.

4.2 AFCEC/CND

AFCEC/CND is responsible for assisting the installation with the ESPC process.

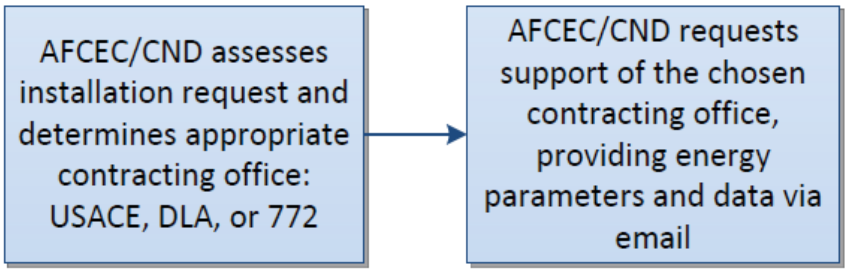


Figure 2 AFCEC/CND Process Map

Step 3: AFCEC/CND assesses the installation's request and determines the appropriate contracting office: HNC, DLA Energy or 772 ESS.

AFCEC/CND and the BCE form the Energy Team, which consists of various AFCEC/CND members, CEs, the Judge Advocate (JA), customers, and the PF (assigned by AFCEC/CND). The Energy Team assesses the proposed energy conservation opportunities to determine if an ESPC is the appropriate tool for the installation's proposed project. If yes, AFCEC/CND coordinates with the DoE FFS to access the DoE ESPC contract.

The Energy Team coordinates the date and time for an onsite meeting or teleconference with the installation, AFCEC/CND, and the PF to explore opportunities, develop ESCO selection criteria, and acquisition strategies.

Step 4: AFCEC/CND requests support of the chosen contracting office, providing energy parameters and data via email.

The Energy Team develops a site data package and provides it to the chosen contracting office via email. The site data package includes general site data such as building type (e.g., hangar, classrooms, offices); square footage; building schedule; utility rates; and specific requirements (e.g., temperature, lighting level, humidity controls).

4.3 Contracting Processes

AFCEC/CND chooses from the following contracting offices to complete the ESCO selection TO award process: DLA Energy, HNC or 772 ESS. The following sub-sections walk through the steps each contracting office completes in order to award the TO for the ESPC project.

4.3.1 DLA Energy Contracting Process

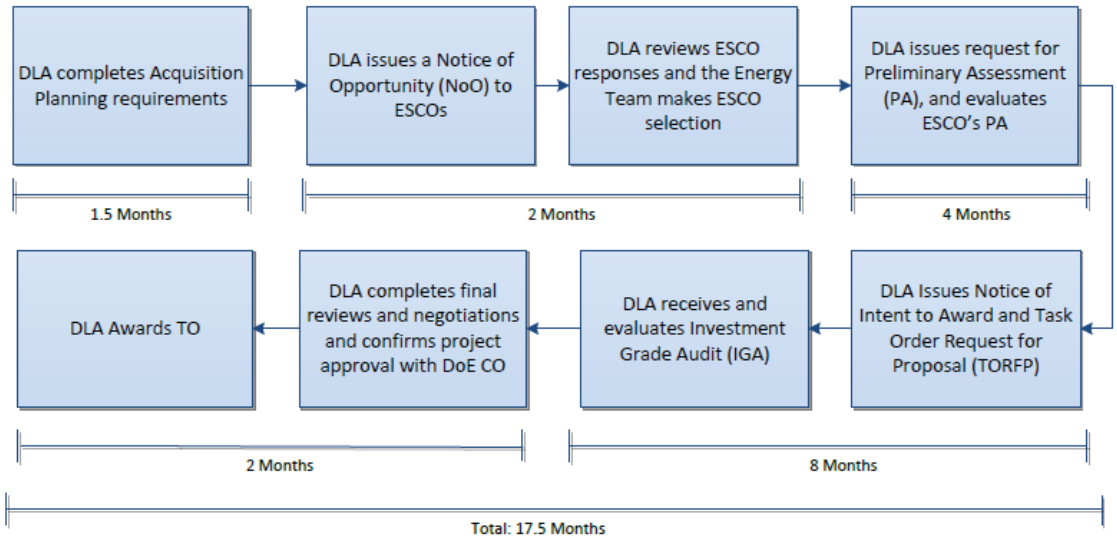


Figure 3 DLA Energy Process Map

Step 5: DLA Energy completes the acquisition planning requirements.

Based on information obtained during meetings with the installation and stakeholders, DLA Energy and the PF discuss the installations requirements and preferences which allows them to determine the appropriate solicitation method and evaluation criteria. After developing the NoO and Acquisition Plan documents, the CO submits them to their policy and legal departments for approval.

Step 6: DLA Energy issues a NoO to the ESCOs.

DLA Energy CO issues the approved NoO for ESCO review and response. The ESCOs have 30 days to respond to the NoO with the appropriate response and documents. The installation and AFCEC are engaged during the NoO period. The ESCOs commonly submit Requests for Information (RFI) regarding the NoO. These RFIs need to be responded to by the government prior to the ESCO's response submission.

Step 7: DLA Energy reviews ESCO responses and the Energy Team makes an ESCO selection.

The CO does a responsiveness and responsibility check for each offeror and convenes the evaluation team for their evaluation, which includes independent write-ups by team members. The Energy Team reviews the evaluations provides a combined rating to the CO. All issues are resolved through technical evaluation. The CO prepares the decision document. The CO completes the selection process, which includes a review period prior to completion, and issues unsuccessful letters to offerors not selected.

Step 8: DLA Energy issues the request for the PA and evaluates ESCO's PA.

DLA Energy issues a letter to the selected ESCO to begin the PA. After receipt of the PA request, a kickoff meeting is held to establish the ground rules and objectives between the ESCO and the installation. On average, the ESCO has 60 calendar days to complete the PA; which is dependent upon receipt of requested data from the AF. Once the PA is received, the CO convenes the review team. The review team conducts the PA review; the CO consolidates their comments and provides them to the ESCO. The ESCO is given a date to have each comment addressed. Once comments are addressed by the ESCO, then DLA Energy and AF determine if they will proceed and which ECMs will be pursued.

Note: The agency will not be liable for any costs associated with PA audits or preparation of the PA unless the project addressed by the PA later becomes a TO award.

Step 9: DLA Energy issues a Notice of Intent to Award (NOITA) and the TO-RFP.

DLA Energy hosts the IGA kickoff meeting, which is held shortly after issuance of the NOITA; all concerned parties attend. At the time of the NOITA, the DLA Energy will start the development of the TO-RFP and will request information from the installation and AFCEC. The required information is not part of the standard IDIQ, but contains AF and installation specific requirements and restrictions. Use the PA/IGA Kickoff Checklist job aid to assist with the PA and IGA steps. Refer to the IGA Review Checklist and the PA Review Checklist for guidance.

Step 10: DLA Energy receives and evaluates the IGA.

Once DLA Energy receives the IGA, a technical review is completed, comments are shared and the pricing team begins their analysis. The entire IGA review team should have all comments returned to the CO within 21 days. Each team member is responsible to research related reviews from operations engineers or mechanical engineers. The CO consolidates reviewers' comments and forwards them to the ESCO to address. The ESCO provides resolution to the comments. The Energy Team validates the proposed Life Cycle Cost Analysis. Once the CO closes all comments, the ESCO is advised to submit a clean IGA to move forward for approvals. Use the PA/IGA Kickoff Checklist job aid to assist with the PA and IGA steps. Refer to the IGA Review Checklist for guidance.

Step 11: DLA Energy completes final reviews and negotiations and confirms project approval with the DoE CO.

DLA Energy provides the final technical project to AF for approval. The DLA Energy review is a combination of pre-negotiations and the contract award review. It is done as one step due to the nature of an ESPC and is completed simultaneously with the AF approval process. If the Pre-negotiation Milestone (PNM) briefing is accomplished prior to AF approval, negotiations are held with the ESCO to close the cost, pending the receipt of AF project approval. No award is made until all approvals are rendered to the CO. The CO will finalize the final PNM.

Step 12: DLA Energy awards the TO to the ESCO.

DLA Energy submits the request for final pricing revisions and schedules based on negotiated settlement. The ESCO needs to revise the price proposal to match the negotiated amount and update the schedules. These should be delivered along with the final IGA write up. The CO updates the award document, TO-RFP with negotiation revisions. Once this is complete, the ESCO is awarded the TO. Contract administration services are delegated to the DLA Energy ACO.

4.3.2 HNC Contracting Process

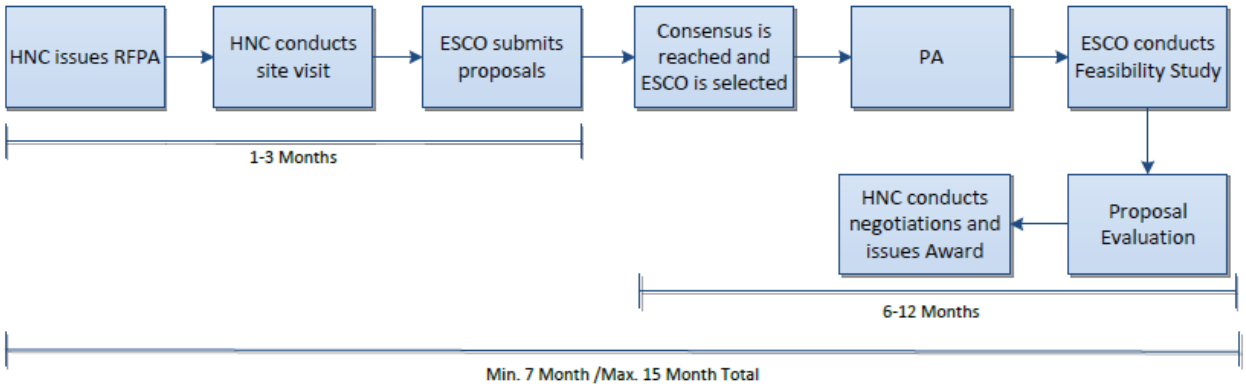


Figure 4 HNC Process Map

Step 5: HNC issues a Request for Preliminary Assessment (RFPA).

Once AFCEC/CND identifies HNC as the contracting agency, AFCEC/CND identifies funding for the HNC fee, and issues a "Go to Work" letter, the HNC develops the Acquisition Plan and the RFPA.

Step 6: HNC conducts a site visit.

The HNC conducts a kickoff meeting and training with the installation, AFCEC, and other necessary stake holders. A date is determined for the ESCO site walk as part of the RFPA process. The HNC utilizes this date to issue the RFPA and coordinates an onsite meeting with all Government parties and ESCOs. The RFPA consists of a limited number of facilities that the ESCO will address. Potential ECMs are identified.

Step 7: ESCOs submit their proposals.

ESCOs are competed through the evaluation of the best technical approach and experience using a broad scope of work. Upon the receipt of the ESCO responses to the RFPA, the submissions are evaluated by the selection panel, including the HNC and the customer. A consensus meeting is held with the installation, AFCEC, and Huntsville Corps (government personnel only) to select the ESCO. This is a streamlined process, which reduces the timeline and cost.

Step 8: Consensus is reached to select an ESCO to perform the ESPC work.

The Energy Team is assembled to reach consensus on a consolidated response for submission to HNC contracting. The HNC issues the Notice to Proceed (NTP) to the selected ESCO.

Step 9: The ESCO completes the PA.

The ESCO conducts a site survey to support the PA, and provides RFIs for collection of additional information. Once the RFIs are addressed, the ESCO submits the PA. The PA is reviewed by the installation, AFCEC, and HNC. Comments generated during the PA review are addressed by the ESCO. Once the ESCO has addressed the comments, a meeting is held to discuss whether to proceed with the ESPC and which ECMs should be considered. The ECMs to be considered will form the basis of the IGA. Use the PA/IGA Kickoff Checklist job aid to assist with the PA and IGA steps. Refer to the IGA Review Checklist and the PA Review Checklist for guidance. Note: The agency will not be liable for any costs associated with PA audits or preparation of the PA unless the project addressed by the PA later becomes a TO award.

Step 10: ESCO conducts a Feasibility Study (FS).

The HNC requests the start of the FS. The ESCO conducts and submits their FS findings. The ESCO establishes protocols for baseline development and M&V. The Energy Team reviews the FS and submits comments to the ESCO. The installation determines which ECMs to pursue for the FS. This FS bundles rapid payback improvements with longer payback improvements to maximize the number of upgrade or modernization opportunities.

Step 11: Proposal Evaluation.

The ESCO submits their final proposal. The Energy Team conducts a proposal evaluation and issues comments to the ESCO.

Step 12: HNC conducts negotiations and issues award.

Once the comments are answered and the final proposal is submitted by the ESCO, the HNC approves the project, conducts contract negotiations, and awards the TO to the ESCO. HNC delegates contract administration services to the installation contracting office and provides the award and proposal documentation to the installation ACO.

4.3.3 772 ESS Contracting Process

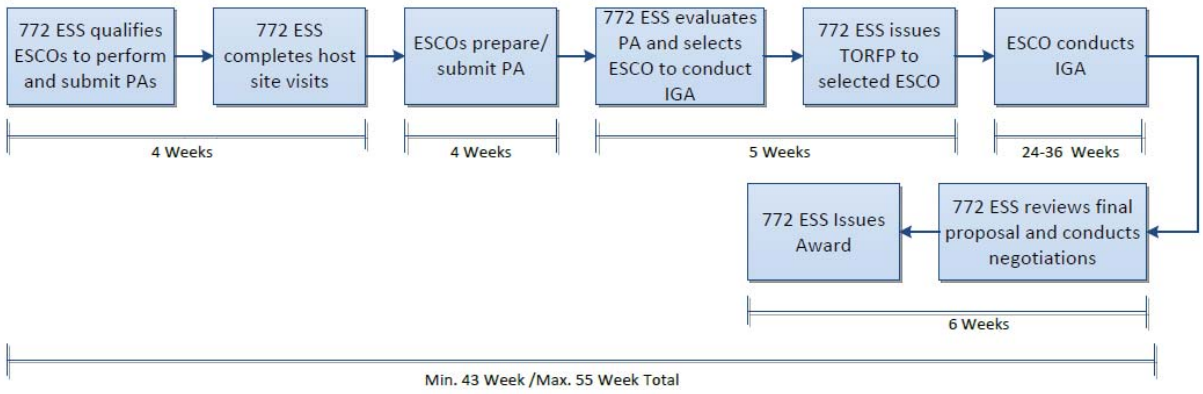


Figure 5 772 ESS Process Map

Step 5: The 772 ESS CO qualifies the ESCOs to perform and submit PAs.

The 772 ESS CO sends the NoO letter to the ESCOs. Interested ESCOs submit a qualification package in response to the NoO. The Energy Team reviews submitted qualification packages and select one or more ESCOs and have discussions about their qualifications. After the

discussions, the CO provides the selected ESCOs a letter to conduct a PA that includes:

1. A statement of the requirements.
2. Disclosure of the significant factors and sub-factors used to evaluate proposals, including their relevant importance.
3. The date and time of a pre-proposal meeting and onsite visit.
4. The date for submission of proposals.
5. Attachments, as needed.

The CO provides a debriefing to any ESCO not selected to conduct the PA if requested in accordance with Federal Acquisition Regulation (FAR) 15.505.

Step 6: The 772 ESS CO completes host site visits.

The installation CO and BEM or representative orchestrate the pre-proposal conference and onsite visit with interested ESCOs and address any questions.

Step 7: ESCOs prepare and submit their PAs.

The ESCOs conduct their PAs and submits them to the CO.

Step 8: The772 ESS CO and Energy Team evaluate the submitted PAs and select an ESCO to conduct an IGA.

The CO provides the submitted PAs to the Energy Team, who evaluates the proposals solely against the factors and sub-factors identified in the NoO and selects one (or more if evaluated equally) ESCO to move forward with an IGA. The CO prepares written determination for selection and submits for internal review and approval. Once the reviews and approvals are completed, the CO notifies the unsuccessful ESCOs and conducts debriefings with these ESCOs when requested.

Note: The agency will not be liable for any costs associated with PA audits or preparation of the PA unless the project addressed by the PA later becomes a TO award.

Step 9: The 772 ESS CO issues a TO-RFP to the selected ESCO.

The CO drafts the NOITA letter and schedules a kickoff meeting with the selected ESCO. At the kickoff meeting, the CO issues the NOITA letter to the ESCO which authorizes the ESCO to commence an IGA. The Energy Team completes the AF/DoE TO-RFP and provides it to the selected ESCO. The AF/DoE TO-RFP template is provided by the PF and allows Federal agencies to modify Sections C through I of the basic DoE IDIQ contract to suit specific installation requirements; therefore, it should be provided to the ESCO as soon as possible after issuance of NOITA letter and commencement of the IGA.

Step 10: ESCO conducts an IGA.

The Energy Team and ESCO collaborate during the project development design phase to resolve any issues prior to submitting the final IGA proposal.

Step 11: The 772 ESS CO reviews the final proposal and conducts negotiations.

Upon submission of the final IGA proposal, the Energy Team reviews and provides the comments, as necessary, and the CO negotiates terms/conditions and/or costs if necessary. The ESCO provides a final proposal based on negotiations, including revisions and corrections as directed by the CO. Refer to the IGA Review Checklist for guidance.

Step 12: The 772 ESS CO issues the award to the ESCO.

The CO awards the TO and provides copies to AFCEC/CND. The CO delegates contract administration services to the installation contracting office and provides the award and proposal documentation to the installation ACO.

Chapter 5 ESPC Post Award

This chapter explains the post award process, broken down into steps that are clear and easy to follow. The process map below assists in understanding the post award process.

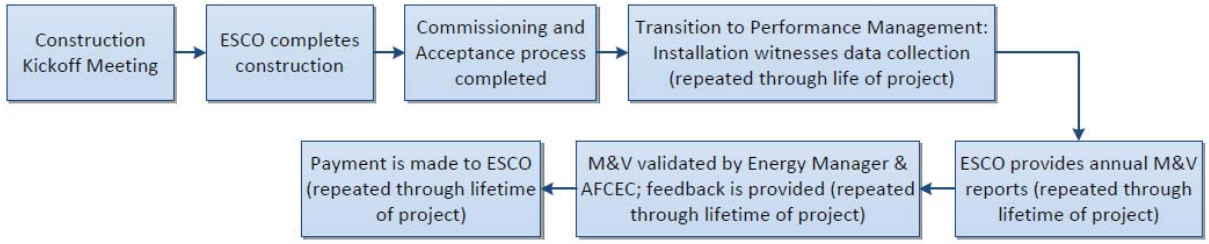


Figure 6 Post Award Process Map

5.1 Construction

Step 13: The ACO holds the construction kickoff meeting at the installation.

The ACO, COTRs, inspectors, ESCO project manager; and managers for design, construction, commissioning, M&V, and performance-period services meet to discuss and review the following for the construction phase:

a. Roles and responsibilities
b. Expectations
c. Construction timelines
d. Communication protocols
e. Schedules for design
f. Schedules for construction
g. Protocols for site access
h. Protocols for submittal review

The ACO issues a notice to proceed after the installation and project managers review the ESCO's designs, construction plans, and related submittals. The ESCO provides acceptable performance and payment bonds (as required) and insurance certificates.

Step 14: The ESCO completes the construction.

During the construction phase, the ACO, COTRs and inspectors are responsible for ensuring the ESCO is adhering to the agreed schedule and plans by:

a. Monitoring the construction.
b. Reviewing the ESCOs plan logs.
c. Ensuring space access.
d. Reviewing punch lists.
e. Verifying proper ECM installation per TO requirements, design/installation plans, and approved submittals.

Follow the Contract Management Plan, which establishes continuity of contract administration as individuals come and go. If there are variances between design and as-built installation, the ESCO and agency identify and document the changes in the post-Installation report. Refer to the COTR training for more information.

Step 15: Commissioning and acceptance process completed.

Once construction is complete, the ACO commissions the project as long as the project meets design intent, per the directives of the TO. While construction is usually completed before acceptance, some checks after acceptance are required, such as summer performance of chillers installed in winter, and steam trap performance in winter.

Before providing acceptance of the project, ensure the following:

a. ECMs are performing as specified.
b. Required submittals are received.
c. Acceptance checklist is noted with dates for each item, signed off by the COTR, and forwarded to the ACO.

Note: Partial or early acceptance of individual ECMs is common when they are producing savings prior to full project acceptance. Interest costs can be reduced by making payments based on savings from provisionally accepted ECMs before project acceptance. These implementation-period payments must be specified in Schedule Task Order 1, per the DOE IDIQ ESPC.

As part of the commissioning and acceptance process, the ESCO provides the following:

a. As-built drawings
b. Spare parts lists
c. Manufacturer warranties
d. ECM training materials
e. O&M training materials, manuals, procedures
f. Commissioning report
g. Post-installation M&V report

5.2 Performance Management

The ACO is responsible for the ESCOs complying with its contractual responsibilities and ensuring guaranteed savings are achieved.

Step 16: Transition to Performance Management: The Installation witnesses data collection (repeated through life of project).

The installation's ACO provides support to the ESCO for the data collection process, including:

a. Access to the buildings/locations
b. Installation data per ESCO request
c. Records (such as utility bills, maintenance data, and occupancy)

The ACO coordinates the ESCO site visit and schedules for M&V inspections/data collection, considering actual operating conditions and the availability of key personnel. The ACO designates a knowledgeable witness to accompany the ESCO during M&V activities. M&V activates focus on:

a. Critical systems, such as Energy Monitoring and Control System (EMCS) set points, chiller/boiler performance tests

b. ECMs generating the most energy/cost savings

c. Sampling proper installation of ECMs such as lighting, motors, and variable frequency drives (VFDs)

Refer to the Guide to Government Witnessing and Review of Post-Installation and annual M&V Activities for M&V witnessing guidance.

Step 17: The ESCO provides annual M&V reports (repeated through lifetime of project).

The annual M&V report must be in accordance with the M&V plan in the awarded TO.

The ESCO:

1. Performs M&V activities per the M&V plan.
2. Produces the M&V report annually to the ACO.
3. Revises the M&V report, as requested by ACO.

Step 18: M&V validated by BEM & AFCEC/CND; feedback is provided (repeated through lifetime of project).

The ACO ensures prompt review of the ESCO's annual M&V report. These reports document whether all parties and the delivered energy and cost savings meet the TO requirements. Review of M&V report verifies that:

a. The M&V plan was followed.

b. The field-measured values were carried over to report.

c. Calculations are correct and follow the M&V plan.

d. Utility and escalation rates used to calculate cost savings are correct.

e. The report provides all required information.

f. Savings guaranteed were met.

If the M&V report shows savings shortfall, the ESCO is responsible for resolving ECM performance issues and proposing remediation options. Shortfall determinations are deducted from the next year's annual payment. AFCEC/CND is available to provide support for validation of the annual M&V report.

Step 19: Payment is made to ESCO (repeated through lifetime of project).

Invoices begin after the ACO has formally accepted the project. Invoices are annual and provided at the beginning of the performance year. The ACO is responsible for verifying that invoices contain any required documentation of services provided before paying the ESCO.

Chapter 6 ESPC Business Practices

The following business practices help the installation implement an ESPC, translate the legislative requirements, and apply lessons learned to achieve a successful ESPC. Refer to AFCEC M&V Requirements for more information.

6.1 M&V Plan

The M&V plan is measurement-based, ensuring the AF's ability to confirm that actual energy savings are occurring and are verified in a reasonable, cost-effective manner. Refer to ESPC M&V Best Practices for ESCOs for more information on energy savings guidance. Using this plan annually guarantees the installed equipment is performing as predicted. A well-written M&V plan:

a. Mitigates risk to the installation.

b. Eliminates conflict when systems fail to meet their expected savings.

c. Ensures the ESCO remains engaged with the installation over the full term of the contract.

Multiple building ECMs may be combined in one M&V plan, saving M&V costs on the project and simplifying the overall process. All M&V plans **at a minimum** must comply with both the latest version of IPMVP and the DoE M&V Guidelines: Measurement and Verification for Performance-Based Contracts Version 4.0. The guidelines have the following M&V options:

a. Option A: Retrofit Isolation uses key parameter measurements in conjunction with statistical sampling. This option can only be used with AF approval.

b. Option B: Retrofit Isolation with Continuous Metering is used when synergistic energy impacts are fully mitigated.

c. Option C: Whole Facility uses meters connected to the building to establish an accurate baseline and accurate post-implementation utility consumption profiles. This is the preferred option for most M&V efforts.

d. Option D: Calibrated Simulation may not be used in any AF ESPC contract.

Refer to the Overview of M&V Options to view examples for each of the Options listed above.

6.2 Baseline Development

The ESCO documents the baseline data and ensures the data supports the baseline. The ESCO performs the metering and data collection and the installation verifies it to ensure the baseline reflects realistic energy consumption upon which the savings calculations are based. Data collection requirements vary by ECP and M&V method, but a minimum of 6 months' data is required for weather-impacted ECPs. Previously installed meters are used to collect this data. Refer to ESPC M&V Best Practices for ESCOs for more information on baseline development.

Note: It is extremely important that equipment controlled by ambient temperature devices has valid measurements. Savings validation as well as future baseline adjustments will require this accurate data before adjustments can be applied to the existing baseline.

Assumptions made in the PA report should be validated in the IGA by the ESCO. Validation includes documenting all pertinent data and formulas used to compute the energy savings so the BEM can easily explain these savings now or in the future. Baseline development and data collection begins

immediately after the ESCO is selected to perform the IGA. The longer the data collection period, the lower the risk to the installation and the ESCO, which minimizes cost. AFCEC/CND review and approval of the baseline is required.

6.3 Performance Tests

A performance test is a process for achieving, verifying, and documenting the performance of equipment installed or modified as part of an ECP. The performance test plan is developed as part of the IGA, prepared for each ECP and implemented after the TO award. Performance tests are completed during the construction phase to certify that all equipment is operating properly and the results are approved before conducting the energy savings verification tests. The performance test plan describes all aspects of the test process, including:

a. Schedules
b. Responsibilities
c. Documentation requirements
d. Functional performance test requirements

Functional performance tests describe the following:

a. What conditions or loads the tests are to be performed
b. Location of test sensors
c. Type of test equipment
d. Test methods
e. Acceptable range of results

The level of detail depends on the complexity of the ECP. The performance testing plan is detailed so the installation knows exactly which tests will be performed prior to awarding the TO. After completing the performance tests, a final acceptance report is submitted for approval to the CO, ACO and BEM. The final acceptance report is submitted after all functional performance tests are completed and includes the following:

a. Executive summary
b. ECP description
c. Performance plan
d. Test results

The CO will approve the performance test results after coordination and verification of results by the BEM.

6.4 Energy Savings Validation

A formal set of test procedures with the acceptable range of results are developed to validate energy savings. These test procedures are submitted by the ESCO at IGA and approved before awarding the TO. The tests describe the following:

a. Under what conditions or loads the tests are to be performed.

b. Location of test sensors.

c. Frequency of measurements.

d. Type of test equipment.

e. Test methods.

f. Acceptable range of results.

Test procedures verify all energy savings guaranteed under the ECP/ECM. After the installation and AFCEC/CND approves the performance test results for each ECP, the ESCO will perform the approved energy savings test procedures to validate the energy savings for each ECP after TO award for each year of the performance period. Each ECP must have lifecycle cost effective on its own merits, unless specifically approved by AFCEC/CND. Once the validated energy savings are approved for all ECPs, the ESCO submits an invoice for payment the first full month after acceptance of the ECM.

6.5 Annual Reconciliation Plan (Audit of Savings)

Each ECP listed in the TO has a detailed annual reconciliation plan approved prior to the award of the TO. The plan includes:

a. A formal set of test procedures.

b. The acceptable range of results.

c. The schedule of how reconciliation payments will be assessed if savings fall below the guarantee.

d. A certification by the ESCO that all O&M requirements and conditions have been met for each ECP in the TO.

The test procedures are similar to those developed to validate energy savings. The purpose is to test, validate, and document the energy savings. The ACO must approve the annual reconciliation of savings after coordination and verification of savings by the BEM.

6.6 Maintenance Related to the TO

All maintenance is an ESCO responsibility and is performed by the ESCO for the TO term unless AFCEC/CND has provided in writing allowance for a deviation. The TO defines ESCO and installation maintenance responsibilities. In facilities and areas where ESCO and installation equipment operate, a clear line of demarcation is identified.

In simple cases (such as lighting) and only after approval by AFCEC, the installation may perform maintenance; however, the installation must carefully consider the consequences if it is unable to perform in accordance with the maintenance schedule. Since the ESCO is ultimately responsible, the ESCO determines if the government is meeting the TO requirements. If the installation fails to perform proper maintenance, the ESCO may take over the maintenance and charge the installation for performance. This requires modifying the TO, reworking the TO's financial provisions, and possibly extending the TO's term length or a buyout if the TO term cannot be extended. When the installation assumes maintenance, the ESCO provides a detailed maintenance schedule reflecting when, how often, and by whom the maintenance is to be performed, as detailed in the IGA report.

Since all costs must be accounted for, the estimated cost of the ESCO performing the maintenance is captured in the proposal and reflected in the cost analysis, but may not be included as a cost to the ECM. Additional costs are reflected in the cost analysis as a cost to the ECM if maintenance costs increase over pre-ECP levels.

6.7 Pricing of TO Work

The ESCO provides detailed supporting documentation to determine price reasonableness. ESCO estimates for each ECP identify all major costs including:

a. Equipment
b. Labor
c. Design
d. Maintenance
e. Repair
f. Parts
g. Overhead and profit (OH&P)
h. Travel
i. M&V

The government should prepare an independent estimate. Contingencies are clearly identified and negotiated for each ECP. Contingency costs mitigate a project's risk, which is a factor in the profit negotiated. Refer to the FAR 31.205-7, Contingencies for additional information. Note: Contingency costs are generally not allowed.

a. Ancillary savings, which are generally not allowed, are those not attributed to utility savings, such as manpower, materials, or eliminating contract-operated functions. Maintenance, repair, or operations costs for tasks currently being performed by the government or by a contractor hired by the government are ancillary savings if the ESCO assumes the tasks, reduces the tasks, or eliminates the tasks. Savings must be real and verifiable. The BEM determines whether an ESCO-proposed task elimination or reduction is considered an ancillary savings available for sharing. The government provides the dollar value of the ancillary savings.

b. The final negotiated savings shall be applied to the ESPC contract. The cost of elimination contract-operated functions are not negotiated until after TO award. These costs are estimated and added into the TO.

c. The ESCO may not represent the government to negotiate a lower utility rate in an ESPC project.

6.8 Equipment Ownership

Generally, the AF owns the equipment post-construction and must update real property records to show ownership of the ESCO-installed equipment. The ESCO is required to provide to the AF, prior to contract completion, O&M manuals for the equipment, as well as required maintenance training.

However, due to taxes and/or rebates, occasionally the ESCO retains ownership post-construction. In either case, the ownership determination should be defined and agreed upon within the TO.

6.9 Infrastructure Privatization

Any utility system or family housing being considered for privatization should not be included in ESPC efforts. "Any utility system" is defined as infrastructure outside the 1.5-meter (5-foot) line of the using facility, and includes production and distribution assets. If it is necessary to include a utility system in the ECP, the installation obtains a written agreement with the ESCO for the new utility system's owner to buy out that system if privatization takes place.

6.10 ESCO Quality Control

The AF requires ESCOs to provide consistency in ESCO submittals, such as the PA, IGA, and other related documents. Inaccurate or inconsistent information provided in submittals from ESCOs result in unnecessary extensions or delays in ESPC projects. ESCOs shall ensure they have the proper quality controls in place and must describe their quality assurance process within each ESCO submittal during the ESPC process. Refer to the IGA Review Checklist and the PA Review Checklist for guidance.

Appendix A Acronym List

Acronym	Definition
ACO	Administrative Contracting Officer (Installation)
A-E	Architect-Engineering
AF	Air Force
AFCEC	Air Force Civil Engineer Center
AFIMSC	Air Force Installation and Mission Support Center
AFPD	Air Force Policy Directive
AMRS	Advanced Meter Reading System
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BCE	Base Civil Engineer
BEM	Base Energy Manager
BFM	Base Financial Manager
CE	Civil Engineer
CEAS	Comprehensive Energy Acquisition Strategy
CFR	Code of Federal Regulations
CO	Contracting Officer
COTR	Contracting Officer Technical Representative
DLA Energy	Defense Logistics Agency- Energy
DMAG	Depot Maintenance Area Group
DoD	Department of Defense
DoE	Department of Energy
EO	Executive Order
ECIP	Energy Conservation Investment Program
ECM	Energy Conservation Measures
ECP	Energy Conservation Project
EEAP	Energy Engineering Analysis Program
EEIC	Element of Expense Identification Code
EERC	Energy Escalation Rate Calculator
EISA	Energy Independence and Security Act
EMCS	Energy Monitoring and Control System
ESCO	Energy Services Company
ESPC	Energy Savings Performance Contract
ESS	Enterprise Sourcing Squadron
ETL	Engineering Technical Letter
EVO	Efficiency Valuation Organization
FAR	Federal Acquisition Regulation
FEMP	Federal Energy Management Program
FFS	Federal Financing Specialist
FS	Feasibility Study
HNC	Huntsville Engineering and Support Center
HVAC	Heating, Ventilation, and Air-Conditioning
IDIQ	Indefinite Delivery/Indefinite Quantity
IGA	Investment Grade Audit for DOE contracts
IPL	Integrated Process List
IPMVP	International Performance Measurement and Verification Protocol
JA	Judge Advocate
M&V	Measurement and Verification
MFH	Military Family Housing
MILCON	Military Construction
NAF	Non-Appropriated Funds
NIST	National Institute of Standards and Technology
NOITA	Notice of Intent to Award

Acronym	Definition
NoO	Notice of Opportunity
NTP	Notice to Proceed
O&M	Operations and Maintenance
PA	Preliminary Assessment
PF	Project Facilitator
PMO	Project Management Office
PNM	Pre-negotiation Milestone
POC	Point of Contact
POM	Program Objective Memorandum
RDT&E	Research, Development, Test and Evaluation
REM	Resource Efficiency Manager
RFI	Request for Information
RFPA	Request for Preliminary Assessment
RFP	Request for Proposal
RPIE	Real Property Installed Equipment
SIA	Sustainment Infrastructure Assessment
SME	Subject Matter Expert
SRM	Sustainment, Restoration and Modernization
TC	Technology Categories
TO	Task Order
TO-RFP	Task Order- Request for Proposal
U.S.C.	United States Code
USACE	Unites States Army Corps of Engineers
VFD	Variable Frequency Drive

Appendix B References and Master List of Links

Section	Type	Name of Item Linked	Link
Chapter 2	Bookmark	Section 4.1	Bookmarked to Chapter 4 ESPC Process, Section 4.1 ESPC Initiation
Chapter 2	External	AFPD 32-10, *Installations and Facilities*	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afpd32-10/afpd32-10.pdf
Chapter 2	External	Title 42, U.S.C., Section 8287, *National Energy Conservation Policy Act*	https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap91-subchapVII-sec8287.pdf
Chapter 2	External	10 U.S.C. 2911-13, *Energy Performance Goals and Plans for Department of Defense*	https://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap173-subchapI-sec2911.pdf
Chapter 2	External	42 U.S.C. 8253, *Energy Policy Act of 1992*	http://uscode.house.gov/view.xhtml?req=(title:42%20section:8253%20edition:prelim)
Chapter 2	External	E.O. 13423, *Strengthening Federal Environmental, Energy, and Transportation Management*	https://www.fedcenter.gov/programs/eo13423/
Chapter 2	External	E.O. 13693, *Planning for Federal Sustainability in the Next Decade*	https://energy.gov/lm/downloads/executive-order-13693-planning-federal-sustainability-next-decade
Chapter 2	External	E.O. 13514, *Federal Leadership in Environmental, Energy, and Economic Performance*	https://www.fedcenter.gov/programs/eo13514/
Chapter 2	External	Energy Policy Act of 2005	https://www.gpo.gov/fdsys/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf
Chapter 2	External	10 CFR 436, *Federal Energy Management and Planning Programs*	https://www.gpo.gov/fdsys/granule/CFR-1999-title10-vol3/CFR-1999-title10-vol3-part436
Chapter 2	External	EISA of 2007	https://www.gpo.gov/fdsys/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf
Chapter 2	Internal	DoE letter to ESCOs	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/DoE_Letter%20to%20ESCOs_Final.pdf?Web=1
Chapter 2, ESPC Escalation Rate Guidance	External	Energy Escalation Rate Calculator (EERC)	http://www.energy.gov/eere/femp/energy-escalation-rate-calculator-download (use most current version)
Chapter 2	External	Energy Price Indices and Discount Factors for Life-Cycle Cost Analysis–2016 Annual Supplement to NIST Handbook 135	https://www.nist.gov/publications/energy-price-indices-and-discount-factors-life-cycle-cost-analysis-150-2016-annual
Chapter 2	Internal	Escalation Rate Guidance	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/AFCEC%20Escalation%20Rate%20Guidance_Final.docx
Chapter 2	External	Section 8287a of 42 U.S.C. 8287	http://uscode.house.gov/view.xhtml?req=(title:42%20section:8287a%20edition:prelim)
Chapter 2	Bookmark	Option C	Bookmarked to Chapter 6 ESPC Business Practices, 6.1 M&V Plan.
Chapter 2	External	Paragraph (a)(2)(A) of 42 U.S.C. 8287	https://www.law.cornell.edu/uscode/text/42/8287

Section	Type	Name of Item Linked	Link
Chapter 3	Internal	2013 Memorandum	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/23%20Oct%202013%20Policy%20Memorandum.docx
Chapter 3	Internal	2010 ESPC Policy Letter	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/2010-10-04%20Updated%20ESPC%20and%20UESC%20Policy%20Ltr.pdf?Web=1
Chapter 3	Internal	eDash	https://cs.eis.af.mil/sites/10040/WPP/HomePage/Home.aspx
Chapter 3, 4, 6	Internal	IGA Review Checklist	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/IGA%20review%20checklist_Final.pdf?Web=1
Chapter 3, 4, 6	Internal	PA Review Checklist	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/PA%20review%20checklist_Final.pdf?Web=1
Chapter 3	Bookmark	FEMP Support Services	Bookmarked to FEMP Support Services
Chapter 3	External	FEMP ESPC Project Development Guide	https://energy.gov/eere/femp/downloads/femp-espc-project-development-resource-guide
Chapter 3	External	FEMP web page	https://www4.eere.energy.gov/femp/training/
Chapter 4	Internal	ESPC Engagement Guidance	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/Reference_3%20ESPC%20%20Engagement%20Guidance_Final.docx
Chapter 4	Internal	ESPC Considerations for BEM	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/ESPC_Considerations%20for%20BEM_Final.docx
Chapter 4	Bookmark	Base Submittal Spreadsheet	Bookmarked to Appendix C, AFB Blank Building Data Sheet
Chapter 4	Internal	UFC 3-530-01 Change 3 on TLED Requirements	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/UFC%203-530-01%20Change%203%20on%20TLED%20Requirements_Final.docx
Chapter 4	Internal	ESPC Technology Categories and Associated ECMs	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/ESPC%20Technology%20Categories%20and%20Associated%20ECMs_Final.docx
Chapter 4	Bookmark	PA/IGA Kickoff Checklist job aid	Bookmarked to Appendix C, PA/IGA Kickoff Checklist
Chapter 4	External	Federal Acquisition Regulation (FAR) 15.505.	https://www.acquisition.gov/far/current/html/Subpart%2015_5.html
Chapter 4	External	The AF/DoE TO-RFP template	https://energy.gov/eere/femp/downloads/doe-espc-task-order-request-proposal-rfp-template
Chapter 5	Internal	COTR training	https://afcec-portal.lackland.af.mil/cp/cpe/SitePages/772%20COR%20Training.aspx
Chapter 5	External	Guide to Government Witnessing and Review of Post-Installation and Annual M&V Activities	https://www.energy.gov/eere/femp/downloads/guide-government-witnessing-and-review-measurement-and-verification-activities
Chapter 6	Internal	AFCEC M&V Requirements	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/AFCEC%20M%20and%20V%20Requirements_Final.docx
Chapter 6	Internal	IPMVP	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/IPMVP_instructions_Final.docx
Chapter 6	External	Measurement and Verification for Performance-Based Contracts Version 4.0.	https://energy.gov/sites/prod/files/2016/01/f28/mv_guide_4_0.pdf
Chapter 6	External	Overview of M&V Options	https://energy.gov/sites/prod/files/2016/01/f28/mv_guide_4_0.pdf#page=22
Chapter 6	Internal	ESPC M&V Best Practices for ESCOs	https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/MV%20Best%20Practices_Final.docx
Chapter 6	External	FAR 31.205-7, Contingencies	https://www.acquisition.gov/sites/default/files/current/far/html/Subpart%2031_2.html
ESPC Considerations for BEM	External	ENERGY STAR	https://www.energystar.gov

Section	Type	Name of Item Linked	Link
Instructions to Access IPMVP	External	Efficiency Valuation Organization	http://evo-world.org/en/subscribe-join-en

Appendix C Job Aids

FEMP Support Services

FEMP Services List Statement of Work - Optional Service Offerings for Contractor-Identified Project				
Phase Two - Initial Project Development				
Task #	**Task Title**	**Work Scope**	**Deliverable**	**Agency Requirements**
Replace Std Task# 2-1	DO RFP Development - On Site Consultation	FEMP Services will provide technical consultation resources at the Agency's site to assist in the integration of the site's requirements into the DO RFP template.	Oral Comments	Agency staff will draft DO RFP. Provide copies to FEMP Services staff for review.
Phase Three - Negotiations and Award				
Replace Std Task# 3-4	Final Proposal Review - Direct Support	FEMP Services will provide direct technical resources to review final proposal. Review will include assessment of ESPC-unique data such as markups, performance period expenses, and financing interest rates. FEMP Services will assure that price schedules have been filled out correctly. ESCO specified equipment will be evaluated for its appropriateness and installation expense (labor and material). FEMP Services will coordinate and assemble agency and FEMP Services questions and issues for Agency CO to be presented to ESCO for discussions and negotiations.	Telecon Advice and Written comments and Recommendations	Agency will provide FEMP Services staff copies of final proposal with emphasis on selected equipment compatibility with agency performance requirements. Agency shall ensure applicable acquisition team members review final proposal. Agency will generate site questions or issues prior to scheduled telecons with FEMP Services staff. Agency will review questions and issues for ESCO discussions. Agency CO will submit questions and issues to ESCO.

Phase Four - Implementing the Delivery Order				
Task #	**Task Title**	**Work Scope**	**Deliverable**	**Agency Requirements**
Insert after Std Task# 4-1	Design & Construction Package Review - Consultation Support	FEMP Services will provide consultation and technical review advice to support Agency review of Design & Construction Packages, submittals, shop and working drawings, manufactures data, planned service interruptions, permit acquisition plan and installation schedules for compliance, feasibility, consistency and reasonableness.	Telecon Advice and/or Written Comments/ Recommendations	Agency will review all contractor submittals and generate comments, questions and issues for FEMP Services consultation and advice. Provide copies of Agency comments, questions, issues, and applicable portions of submittals. Coordinate telecons with FEMP Services and Agency acquisition team. Submit Agency recommendations to ESCO for action.
Insert after Std Task# 4-1	Design & Construction Package Review - Direct Support	FEMP Services will provide direct on-site technical resources necessary to inspect and accept the installed ECMs. FEMP Services will assist Agency with development and monitoring of punch list items through completion/acceptance .	Telecon Advice and Design & Construction Package Review Report(s)	Agency will provide FEMP Services a set of Agency design/construction standards. Agency will review the Design & Construction Package Review Report(s) for concurrence. Agency provide copies of ESCO responses to Design & Construction Package review comments. Agency to submit notice to proceed to ESCO..
Insert before Std Task# 4-2	Project Construction Installation Commissioning - Consultation Support	FEMP Services shall provide telecon consultation support to assist Agency in QA verification for compliance w/installation plan(s), including monitor/inspect installation and start-up activities.	Written Comments/ Recommendations	Agency staff will verify that commissioning activities are conducted and are acceptable per contract requirements.
Insert before Std Task# 4-2	Project Construction Installation Commissioning - Consultation Support	FEMP Services shall provide telecon consultation support to assist Agency in QA verification for compliance w/installation plan(s), including monitor/inspect installation and start-up activities.	Written Comments/ Recommendations	Agency staff will verify that commissioning activities are conducted and are acceptable per contract requirements.

Task #	Task Title	Work Scope	Deliverable	Agency Requirements
Insert before Std Task# 4-2	Project Construction Installation Commissioning - Direct Support	FEMP Services will provide direct technical resources necessary to perform QA verification for compliance with/ installation plans. FEMP Services services may include acting as the commissioning agent and providing commissioning services consistent with the DOE/GSA commissioning guide.	Project Commissioning Report	Agency staff will facilitate access to the site(s) for FEMP Services staff. Agency staff will review the Project Commissioning Report.
Insert before Std Task# 4-2	Compliance with Inspection and Acceptance Plan - Direct Support	FEMP Services will provide direct on-site technical resources necessary to inspect and accept the installed ECMs. FEMP Services will assist Agency with development and monitoring of punch list items through completion/acceptance.	Installation/ Acceptance Report; Punch Lists	Agency will provide FEMP Services a set of Agency design/construction standards. Agency will provide inspection scheduling information and site access, and will act on recommendations to direct ESCO to correct any defects found and sign off on all acceptable work
Insert before Std Task# 4-3	Provide or Assist with Data Acquisition	FEMP Services will provide assistance M&V data collection consistent with the M&V plan. Activities may include metering and performance parameters in support of the M&V plan and /or review of M&V activities and services by others.	Data Collection Logs	Agency will collect data in support of the M&V plan and/or review the data collection activities of the ESCO. Agency will generate comments and/or questions for FEMP Services technical advice.
Insert before Std Task# 4-3	Provide or Assist with Data Reduction & Analysis	FEMP Services will provide assistance with M&V data analysis consistent with the M&V plan. Activities may include calculations, simulations and/or review of M&V activities and services by others.	Summary Findings and Recommendations Report/M&V Performance Report	Agency will compile and review data collected in support of the M&V plan and generate any comments and/or question for FEMP Services technical advice. Agency will review all reports generated for concurrence.

Task #	Task Title	Work Scope	Deliverable	Agency Requirements
Insert after Std Task# 4-3	Assist in Negotiation of Baseline Adjustments	FEMP Services will assist with the development of strategies for making baseline adjustments. Provide technical advice to account for changes in operations, etc affecting baseline(s) over time and assist Agency with negotiations with vendor for baseline adjustment.	Telecon Advice and/or Written Comments/ Recommendations	Agency will facilitate negotiations with ESCO during reconciliation of baseline. Agency will review any proposed changes to the baseline and generate comments and/or questions for FEMP Services technical advice.
Insert after Std Task# 4-3	Provide Project 1st year Performance Results presentation to Agency Management and Staff	FEMP Services will coordinate with Agency Acquisition Team & ESCO to provide "Project 1st Year Performance Results" presentation and discuss Agency/ESCO activities to maintain persistence of ESPC project performance beyond year 1.	On-site Presentation with ESCO & Designated Agency Acquisition Team Members; Provide Agenda and Agency Requested Copies of Presentation	Agency will coordinate facility and date with FEMP Services, ESCO and agency staff and notify invited Agency Management and staff to attend presentation.
Travel				
Task #	**Task Title**	**Work Scope**	**Agency Requirements**	
Insert after Std Travel 3-3 **Label** "4-2"	Travel to Site for Std task 4-2	On Site Support for Project Acceptance Discussion of Findings and Recommendations	Agency coordinate agency staff for FEMP Services presentation of Project Acceptance Recommendations. Agency provides at least 2-weeks notice for best airfare.	
Insert after Std Travel 3-3 **Label** "4-2"	Travel to site for Project Results Presentation	On Site Support for "Project 1st Year Performance Results" presentation with Agency and ESCO	Agency coordinate agency staff for "Project 1st Year Performance Results" presentation. Agency provides at least 2 weeks' notice for best airfare.	

PA/IGA Kickoff Checklist

PA/IGA Kickoff Checklist		
Responsibilities	Installation	☐ Introduction ☐ Overview of installation mission and facility operation. ☐ High level description of special needs and/or desires for scope and operations. ☐ Review of Installation projects on the FY and FY+1 IPL (integrated process list)
	Contracting Officer	☐ Ensures agenda covers all required topics ☐ Establishes initial meeting dates ☐ Establishes communication protocols to include frequency and method of communication ☐ Approves all proposed contractual actions
	ESCO	☐ Agenda o Describe expectations on ECMs to be investigated and developed. o Describe the detailed plan to return and complete audit. o Explain the process and order in which elements of the project will be completed and sent for Government review, coordination, and approval. ☐ Schedule ☐ Timeline ☐ Baseline development ☐ Data Collection ☐ Operations and Maintenance
	AFCEC	☐ Roles & Responsibilities ☐ Escalation determination process ☐ M&V expectations ☐ SME contact info ☐ This Playbook ☐ Coordination of meter installations with AMRS
	All Parties Involved	☐ Conduct site visit and/or discuss data

AFB Blank Building Data Sheet

Blank AFB Bldg Data.xlsx

Link to Blank AFB Bldg Data Sheet:

https://cs2.eis.af.mil/sites/10041/CEPlaybooks/ESPC/References/Worksheet%20in%20Consolidated%20ESPC%20Playbook.xlsx

Appendix D Guidance

AFCEC M&V Requirements

ESPC M&V Plan Options Requirements

After reviews of various Preliminary Assessments (PAs) on various ESPC projects, it appears there is some resistance to providing option "C" as the primary M&V solution requested by the Air Force (AF) per the FEMP 4.0 or latest version of the M&V guidelines. This is a concern because the AF requirement, per audit and write ups, is to ensure savings are verified with actual meter readings. The M&V options being proposed on most Energy Conservation Measures (ECMs) are related to system performance assurance, stipulated savings and not actual savings verification.

Our expectations and requirements are that a MINIMUM 2/3 of the guaranteed savings for any ESPC project be validated with meter readings confirming the actual savings. If individual building savings are predicted to be greater than 10% of the overall BASELINE consumption per FEMP Guidelines for M&V, Option C shall be used. Option C requires 12 months of metering data per the FEMP Guidelines for M&V. AFCEC is willing to except less on a case by case analysis, per ECM, and due to weather dependence. Option B may contribute to the metered M&V requirement and shall sub-meter consumption (e.g., electrical, natural gas, etc.) of the selected ECM, not an estimate from the BAS or a calculation from other parameters.

The AF will not accept an M&V plan that proposes Option C for a minimal number of years in the beginning and complete the performance period under an Option A or B. AFCEC is open to have discussions to have some transition to Option A or B on a case by case bases.

Example, where there are multiple ECMs in a building where mostly option A with some option Bs are proposed, AFCEC recommends the ESCO has a single M&V option C and aggregate all savings from those ECMs, as a whole and perform a one-time comparison to the facility meter for verification. This is considerably less expensive than the proposed Option A or B solutions for each individual ECM, and provides a more precise measurement of overall savings and verification that the savings have been achieved.

ESPC Considerations for BEM

Although an ESCO brings technical energy expertise to the installation's energy program, the BEM is the champion for achieving the installation's energy goals and reporting requirements. The BEM has many resources available to assist in completing tasks, including:

a. Energy audits
b. AFCEC/CN
c. REMs
d. Facility managers
e. Process owners
f. Operations staffs

One of the primary components of an ESPC Energy Team is local staff and building managers. Installation personnel have the best understanding of what equipment is non-operational due to design defects, age, or other reasons. As part of the development of an ESPC, the AF develops a consensus with all stakeholders in an attempt to address the installation's needs and wishes, while considering the AF's risk level to various actions.

Many factors impact the requirements of an ESPC. Overhead and interest charges can make some ECMs not economically viable. In this case, direct funding may be a better solution than an ESPC. To ensure energy projects are executed in the most efficient manner, AFCEC/CND practices a vetting process to review potential ESPC projects and analyze them with the Energy Team to determine the best execution method within the AF energy program.

Once the ESPC execution method is determined, the AF awards a TO that best satisfies the AF's stated scope (saving the maximum energy/water) with the best financing terms and supports the broadest AF goals and mandates. During the development period (PA, IGA) do not accept submissions from the ESCO that fail to address the concerns and goals of the AF. Note: ESCOs tend to consider the ECMs that fit their risk case scenario over AF goals. If the ESCO is not meeting the installation's goals, the ESCO should address the reasons in writing. Consider the following for successful ESPC projects:

a. Use a multidisciplinary team to evaluate proposals and consider the cost of maintenance after the equipment is installed. Each ECM should be evaluated on a life-cycle cost basis. Energy-efficient or ENERGY STAR equipment should be used in the project when possible.
b. Establish the energy use baseline early in the process by installing meters or data logging equipment as part of the contract, when practicable.
c. Communicate with the ESCO often. The installation should provide their expectations and goals early in the process and provide what actions and efforts they are not interested in pursuing. This will allow the ESCO to focus their resources to maximize the costs incurred.
d. Keep the terms and provisions of the ESPC as clear as possible. Minimize adding additional O&M savings or escalators for cost of fuel and services. Examine each ECM to determine how it contributes to the overall project. Review its length of payoff and the impact of its removal or inclusion on the overall project economics. Make appropriate business trade-offs and

establish an optimal scope of work for the project. Package less economical work such as chillers and cooling towers replacements with the most economical ECMs.

e. Identify and define variables that impact energy consumption during the development of the project. The ESCO and AF should identify variables that create risk and define or eliminate them as part of the TO. Include as many of these variables as possible in the "normalized" baseline model so that the energy savings will automatically "correct" to changing conditions (e.g., weather variations, variable operating schedules). Document the remaining variables or variables that are not expected to change (e.g., non-routine variables such as building square footage, occupancy, size and type of equipment) as "static" variables that affect facility energy consumption. If these static variables change during the ESPC project term, an engineering analysis may be necessary to estimate the energy impact and provide fair and equitable compensation.

f. Obtain load profiles and tour the building during the peak energy-use period. Make observations about the operation of energy-using equipment. Determine if any equipment use or power loads could be shifted to a non-peak period of energy use. If not, explore peak shaving, thermal load shifting, and other means of saving energy and costs that could be used to cut expenses. Consider the use of automated building management systems and timed-out electronic locks on non-essential equipment so it cannot be operated during periods of peak demand.

g. Coordinate with AFCEC/CND, Civil Engineering, installation construction, installation contracting, installation finance, and installation legal functions before awarding the TO.

Make sure there is a clear understanding and clear contract language addressing how much M&V is to be performed. As part of the development of an ESPC, the AF does not allow for rate adjustments to account for savings within an ESPC. Additionally, as part of any power generation ECMs, (e.g., CHP, solar photovoltaic), the consideration/discussion of an interconnect agreement with the local utility is paramount, and if not addressed early can result in a signification delay. Become familiar with the latest version of the IPMVP and make use of the M&V protocols in your contract. M&V must comply with the requirements of the Energy Policy Act of 2005.

ESPC Engagement Guidance

This guidance applies to all ESPC acquisition activities prior to the release of the ESPC NoO. The guidance is not intended to limit ESCO opportunities to introduce and market their capabilities to AF installations and AFCEC or to limit the sharing of energy conservation ideas among AF installations. The guidance does caution ESCOs from engaging in any Pre-NoO activities that could affect fair and open competition between ESCOs. AFCEC provides overall project management and contracting support for most subsequent ESPC projects.

Installation/AFCEC Guidance

1. AF installations and AFCEC are encouraged to entertain marketing visits requested by ESCOs. Scheduling and timing of any such visit will be at the discretion of the designated energy program personnel at that location.
2. While ESCOs are encouraged to market their firm's ESPC capabilities to government designated energy program personnel and introduce and/or share conceptual energy conservation ideas, government personnel are reminded to not begin any real or perceived acquisition activities prior to release of an NoO.
3. ESCOs remain free to propose energy conservation ideas in the form of a non-proprietary document prior to the release of an ESPC NoO.
4. AFCEC may post on an AF-internal website all non-proprietary ESCO provided conservation measures in order to facilitate the exchange of ideas among AF personnel.
5. When the government decides to the potential acquisition of an ESPC, all ESCO engagement is at the direction of the designated government CO.
6. Installations must keep AFCEC informed as ESPC projects develop.

ESCO Guidance

1. ESCOs are encouraged to market their firm's ESPC capabilities to government designated energy program personnel and share conceptual energy conservation ideas. Before an ESPC is underway via contracting, ESCOs are allowed to visit installations to market their capabilities and past performance. During pre-ESPC visits, ESCOs are not allowed to visit buildings at installations, not allowed to discuss existing conditions at installations, and not allowed to discuss scope of potential future ESPC projects. There must be no real or implied government commitments to a specific ESCO. Interaction at this point that constitutes actual or perceived government obligation must be avoided.
2. Any marketing literature or conceptual ideas proposed in presentations or papers freely provided by the ESCO to government personnel is handled by the government as non-proprietary and may be shared with other AF installations and AFCEC personnel. Proprietary info, if provided by an ESCO and annotated as "proprietary" is protected by the AF Energy Team.
3. The scheduling and timing of any marketing visit is at the discretion of the designated energy program personnel at that location.

4. Once the government has decided to pursue potential acquisition (NoO) of an ESPC, the ESCO may not request information regarding the scope, cost, or timing of that particular initiative from any government personnel except through the government's designated CO.

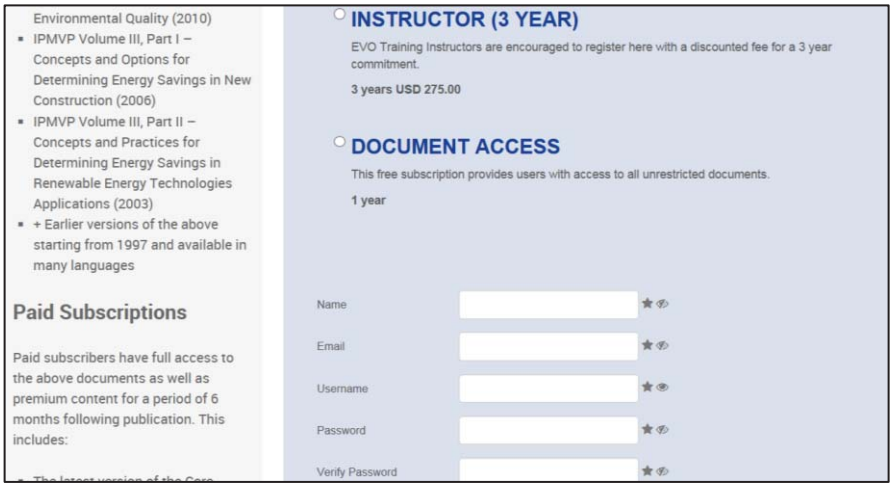
IPMVP Access Instructions

Please follow the instructions below to access the latest available version of the IPMVP:

1. Go to the Efficiency Valuation Organization (EVO) world website.

   (http://evo-world.org/en/subscribe-join-en)

2. Scroll to the bottom of the page and select "Document Access". This will grant you a temporary and free subscription to EVO and allow access to the most recent PDF version of



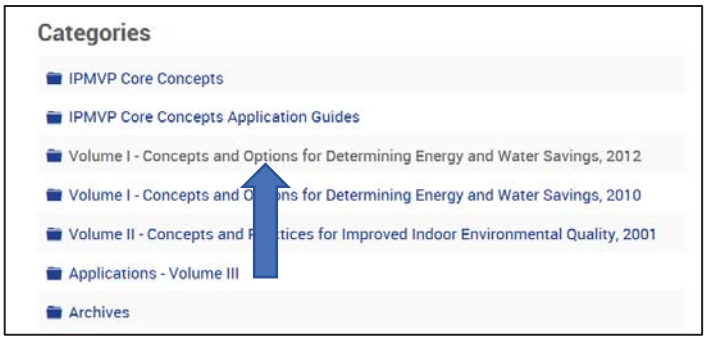
   the IPMVP.

3. Complete the "Sign Up" process.

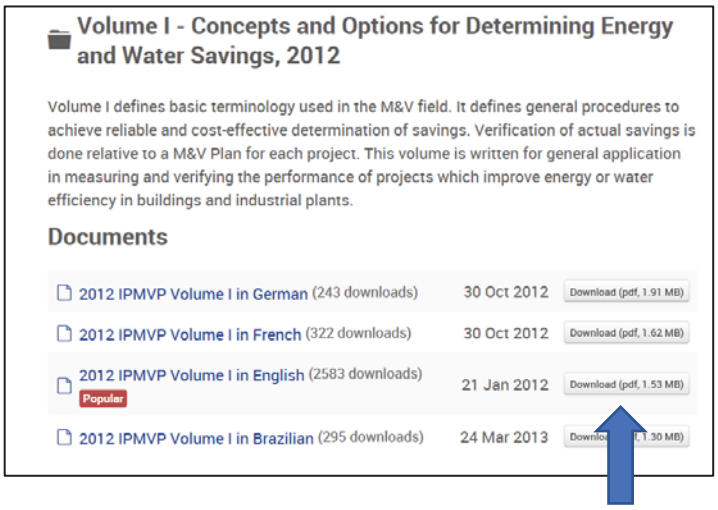
4. Using the user id and password you created, login to EVO using the login key in the top right corner.

5. Select "Library", and then select "IPMVP Documents".

6. Select “Volume I - Concepts and Options for Determining Energy and Water Savings, 2012”, or the most current version available.



7. Select “Download” for the English version, as seen below.



Note: You can save the PDF version for personal use, but check the EVO website regularly for updated documents.

Department of Energy
Golden Field Office
15013 Denver West Parkway Golden,
Colorado 80401

11/14/2016

John C. Guregian
Energy Performance Services, Inc.
116 John Street
Boott Mills South
Suite 200
Lowell, MA 01852

Dear Mr. Guregian,

The Department of Energy is in the process of implementing recommendations to the U.S. Government Accountability Office's (GAO) June 17, 2015, report entitled, "Energy Savings Performance Contracts: Additional Actions Needed to Improve Federal Oversight." We believe the implementation of these recommendations will serve to strengthen our Energy Savings Performance Contracting (ESPC) program.

This communication addresses GAO recommendations related to improving two key areas identified: First, reporting on government impacts to energy savings, which include changes the government has made to equipment and operations, that increase or decrease savings, and secondly, Government witnessing of measurement and verification reports. We ask that your company help to implement these recommendations for your Measurement and Verification reporting (M&V) for existing Delivery Order contracts through increased reporting transparency per the following discussion.

Reporting on government impacts to energy savings:

DOE's IDIQ Regional and Technology Specific contracts M&V reporting requirements have evolved over the years. Initially, only general M&V reporting requirements were included in the IDIQ and the ordering agencies specified the actual report format for each delivery order. With the introduction of standardized M&V guidelines, such as FEMP M&V v3.0, the annual report transitioned to a more structured format. By 2005 almost all DOE IDIQ's were modified to address agency impacts to an ESPC project for annual M&V in Attachment J-7; Measurement and Verification (M&V) Plan and Reporting Outlines. The contract sections which state reporting requirements include:

J-7: Annual Report Outline: Activities Conducted this Period.

2.2.7: Detail any performance deficiencies that need to be addressed by the ESCO or Agency.

2.2.8: Note impact of performance deficiencies or enhancements on generation of savings.

FEMP requests that your company standardize the reporting of impacts on savings using the annual M&V report template found within FEMPs M&V guideline version 4.0 (M&V v4.0), released November 25, 2015, which includes Table E-3 and E-4. Standardization of reports and reporting on deficiencies that need to be addressed, and noting performance deficiencies or enhancements on savings will help agencies to improve operations and also strengthen our ESPC program. We believe standardizing on M&V v4.0 is an efficient way to meet your contractual requirements for existing orders and should help your company standardize its efforts to meet the requirement for all its ESPC awards.

FEMP provides the following guidance related to orders awarded before the introduction of M&V v4.0. For these orders, simplified methods are required to ensure that table E-3 and E-4 of the annual M&V report can be provided annually with no additional cost of M&V performed by the ESCO. The guidance covers two areas: 1. ESCO inspections, and 2. Simplified estimates for energy and cost impacts.

First, ESCO inspections should continue per the existing M&V plan of the order and the estimates of energy and cost impacts will depend on the method of inspection. For example, if an ESCO inspects an adjustable speed drive (ASD) and the method of inspection is visual to determine if the ASD is in “hand or override” or “normal” operation, then the exact time of the agency impact, if in “hand” mode, will be unknown and the impact to energy and cost savings is undeterminable and a “n/a” should be noted. In the next inspection cycle, if the ASD is still in “hand” operation, then the energy and cost impacts will be estimated with simplified methods with the cumulative duration of time between the inspections, or an annual basis, whichever is shorter. Conversely, if the ESCO normally inspects energy management system (EMS) trends to determine operation, then the date the ASD was put into “hand” operation can be determined and the energy and cost impacts can be determined for the time period determined from the EMS with the cumulative duration of time between the inspections, or an annual basis, whichever is shorter.

Second, results of the ESCO inspection can be combined with simplified estimates of energy and cost impacts including, but not limited to, estimates from the order Detailed Energy Survey (DES) or Investment Grade Audit (IGA) based on square feet, scaling based on relevant parameters, or equations. Cost impacts should be determined using the cost of utilities agreed to in the order for the year of the M&V evaluation.

Standardizing on M&V v4.0, annual M&V report table E-3 and E-4, can benefit both the Government reviewer and your company. The information obtained through use of the new annual M&V report template will be used to better inform agencies of the impact that their actions or changes affecting ESPC project related equipment or other circumstances have on cost savings. Furthermore, this information will help agencies to improve government operations and increase the confidence and integrity of ESPC projects.

Lastly, FEMP asks that you consider adding an additional table that is not yet in M&V v4.0 that shows the cost and energy savings for each agency impact on an annualized basis. This table would be used by agencies to review the relative impact of each agency action if the issue was not addressed over a year. This table would help agencies determine where to focus attention to improve energy and cost savings.

ESCOs are encouraged to provide this value-added information in their annual M&V report until the next FEMP update to the M&V guidelines.

Government witnessing of measurement and verification reports:

Government witnessing of M&V measurements has long been incorporated into the DOE IDIQ contracts, M&V versions 3.0 and 4.0, and FEMPs guidance. Reporting of whom in an agency witnessed M&V and any associated documentation was modified into the Regional and Technology Specific IDIQ contracts about 2005 for Annual M&V, per Attachment J-7: Annual Report Outline 2.2.3. We ask that your company continue to fulfill your contractual requirements to collect information about agency witnessing and documentation that is available, and document them in your M&V reports in a transparent manner to aid in an efficient review of your reports. For orders issued prior to this requirement we ask that your company standardize its collection and reporting documentation, and include government witnessing information in your M&V reports.

Our records show that the following Regional Super and Technology Specific, Energy Savings Performance Contracts are associated with Energy Performance Services, Inc.:

DE-AM36-99OR22702 (Energy Performance Services).

Sincerely,

Wayne M. Latham, DOE IDIQ Contracting Officer

Cc: Kurmit Rockwell, Department of Energy
Schuyler Schell, Department of Energy
John Shonder, Department of Energy
Sharon Conger, General Services Administration
Laura Gast, Department of Veterans Affairs
Walter Ludwig, Department of Defense
Randy Smidt, Department of Defense, Army
Dan Magro, Department of Defense, Navy
Leslie Martin, Department of Defense, Airforce
Chau H. Tran, Department of Justice
Ileana Speer, Department of Justice

AFCEC Escalation Rate Guidance

Escalation Rates - Supplement to the ESPC Playbook

As a supplement to the AF ESPC Playbook, the following will be the guidance for ESCOs calculating escalation rates in ESPC projects.

Escalation Rates:

Based on guidance from FEMP and Exeter Associates, the escalation rates for the ESPC going forward will be the Nominal Escalation Rate for each utility as calculated by National Institute for Standards and Technology (NIST) software program called the Energy Escalation Rate Calculator, or EERC. EERC 2.0-17 (use most current version) is available for download from the FEMP website.

http://www.energy.gov/eere/femp/energy-escalation-rate-calculator-download.

The inflation rate used for calculating escalation rates in ESPCs will be in in accordance with the directives of 10 CFR 436, Subpart A "Federal Energy Management and Planning Programs, Methodology and Procedures for Life Cycle Cost Analyses". The inflation figure should represent "estimated increases in the general level of prices consistent with projections of inflation in the most recent Economic Report of the President's Council of Economic Advisors." The inflation rate used for calculating the ESPC escalation rates will be the projected rates of general inflation published in the most recent Report of the President's Council of Economic Advisors. For the EERC 2.0-17, the default figure is 2.2%.

Individual escalation rates must be used for each commodity. Users of the EERC tool only specify 100% for a single fuel type:

1. Identify the state in which their prospective project will take place.
2. Select industrial sector for AF installations.
3. The expected start date (award year).
4. Duration of the project.

With that, the tool will determine an escalation rate for each fuel type.

ESPC Technology Categories and Associated ECMs

This attachment lists the technology categories (TCs) authorized under this master indefinite IDIQ contract, and provides ECM examples for each TC. This list is not intended to be inclusive of all potential ECMs authorized under each TC.

TC.1 Boiler Plant Improvements -ECMs such as, but not limited to:

1. Boiler control, including new controls and retrofits to existing controls
2. Replacement of existing boilers with high efficiency boilers
3. Boiler decentralization

TC.2 Chiller Plant Improvements -ECMs such as, but not limited to:

1. Chiller retrofits or replacements
2. Chiller plant pumping, piping, and controls retrofits and replacements

TC.3 Building Automation Systems (BAS)/Energy Management Control Systems (EMCS) -ECMs such as, but not limited to:

1. Heating, Ventilating, and Air Conditioning (HVAC) upgrade from pneumatics to Direct Digital Control
2. Upgrade or replacement of existing EMCS systems

Note: Must comply with Air Force Guidance Memorandum (AFGM) Civil Engineer Control Systems Cybersecurity (2 Feb 2017). The AFGM supersedes ETL 11-1, Civil Engineer Industrial Control System Information Assurance Compliance (30 Mar 2011). However, the AFGM (12 pages) does not address all items included in ETL 11-1 (32 pages). Therefore, those ETL 11-1 items not addressed in the AFGM, are still in effect.

TC.4 Heating, Ventilating, and Air Conditioning (HVAC, not including boilers, chillers, and Building Automation System/Energy Monitoring/Management Control System (EMCS)) -ECMs such as, but not limited to:

1. Packaged air conditioning unit replacements
2. HVAC damper and controller repair or replacement
3. Window air conditioning replacement with high efficiency units
4. Cooling tower retrofits or replacements
5. Economizer installation
6. Fans and pump replacement or impeller trimming
7. Thermal energy storage
8. Variable air volume retrofit

TC.5 Lighting Improvements -ECMs such as, but not limited to:

1. Interior and exterior lighting retrofits and replacements
2. Intelligent lighting controls
3. Occupancy sensors
4. Light Emitting Diode technologies
5. Daylighting
6. Spectrally enhanced lighting
7. Fiber optic lighting technologies

TC.6 Building Envelope Modifications -ECMs such as, but not limited to:

1. Insulation installation
2. Weatherization
3. Window replacement
4. Reflective solar window tinting

TC.7 Chilled Water, Hot Water, and Steam Distribution Systems -ECMs such as, but not limited to:

1. Piping insulation installation
2. Hot water heater repair and replacement
3. Steam trap repair and replacement
4. Repair or replacement of existing condensate return systems and installation of new condensate return systems

TC.8 Electric Motors and Drives -ECMs such as, but not limited to:

1. Motor replacement with high efficiency motors
2. Variable speed motors or drives

TC.9 Refrigeration -ECMs such as, but not limited to:

1. Replacement of ice/refrigeration equipment with high efficiency units

TC.10 Distributed Generation -ECMs such as, but not limited to:

1. Cogeneration systems installation
2. Microturbines installation
3. Fuel cells installation

TC.11 Renewable Energy Systems -ECMs such as, but not limited to:

1. Photovoltaic system installation
2. Solar hot water system installation
3. Solar ventilation preheating system installation

4. Wind energy system installation
5. Passive solar heating installation
6. Landfill gas, waste water treatment plant digester gas, and coalbed methane power plant installation
7. Wood waste and other organic waste stream heating or power plant installation
8. Replacement of air conditioning and heating units with ground coupled heat pump systems

TC.12 Energy/Utility Distribution Systems -ECMs such as, but not limited to:

1. Transformers installation
2. Power quality upgrades
3. Power factor correction
4. Gas distribution systems installation

TC.13 Water and Sewer Conservation Systems -ECMs such as, but not limited to:

1. Low-flow faucets and showerheads
2. Low-flow plumbing equipment
3. Water efficient irrigation
4. On-site sewer treatment systems

TC.14 Electrical Peak Shaving/Load Shifting -ECMs such as, but not limited to:

1. Thermal energy storage
2. Gas cooling

TC.15 Energy Cost Reduction Through Rate Adjustments -ECMs such as, but not limited to:

1. Change to more favorable rate schedule
2. Lower energy cost supplier(s) (where applicable)
3. Energy service billing and meter auditing recommendations

Note: Not applicable to AF projects

TC.16 Energy Related Process Improvements -ECMs such as, but not limited to:

1. Production and/or manufacturing improvements
2. Recycling and other waste stream reductions
3. Industrial process improvement

TC.17 Commissioning -ECMs such as but not limited to:

1. Retro-commissioning services
2. Continuous commissioning services

TC.18 Advanced Metering Systems

Note: Must comply with AF Advanced Meter Reading System (AMRS) policy

TC.19 Appliance/Plug-load reductions -ECMs such as but not limited to:

1. Replace air-cooled ice/refrigeration equipment
2. Replace refrigerators
3. De-lamp vending machines
4. Plug timers
5. Energy Star® products

TC.20 Future ECMs -(not currently authorized):

1. Non-Building Applications

Federal Energy Management Program

1 Acq Planning
2 **ESCO Select.**
3 Proj. Dev.
4 Implementation
5 Performance

PA Review Checklist
ESPC Process Doc. P2-09
r. 3-7-16
Responsibility: PF

PRELIMINARY ASSESSMENT (PA) REVIEW CHECKLIST

Project Name _____

Project Number _____

Agency _____

Evaluator _____

Date of Review _____

ENERGY (and water) CONSERVATION MEASURES (ECMs):

- ☐ Existing equipment and systems and proposed measures are reasonably defined.
- ☐ The package of ECMs is as comprehensive as desired (encompasses a wide range of opportunities – energy, water, and O&M savings, renewable energy, site infrastructure needs, etc.)
- ☐ Each ECM is suitable for its intended purpose and consistent with government needs/requirements
- ☐ Bases for all savings streams are well described (energy, water, interactive effects, O&M, rate change...)
- ☐ Methods and analyses used to calculate baseline energy/water use and savings are sound
- ☐ Magnitude of baselines and savings for each ECM and each form of energy are in line with expectations
- ☐ Operational conditions (set points, operating hours, foot-candles, etc.) described before and after upgrade.
- ☐ Operating hours and other assumptions are consistent with site operations and documented
- ☐ O&M cost savings are considered per site requirements and there is confidence in their accrual
- ☐ Cost savings for each ECM and form of energy are consistent with energy savings and unit costs

RISK, RESPONSIBILITY, and PERFORMANCE:

Financial Factors: (construction costs, M&V confidence, energy-related savings, delays, facility changes, interest rates)

- Risks for the financial components of the Risk, Responsibility, and Performance Matrix (RRPM) have been clearly described and allocated
- Potential shortfalls in any responsibility have been considered along with resolution strategies.
- Strategies for addressing each risk are effective and acceptable

Operational Factors: (operating hours, loads, weather, user participation)

- Risks for the operational components of the RRPM have been clearly described and allocated
- Potential shortfalls in any responsibility have been considered along with resolution strategies
- Strategies for addressing each risk are effective and acceptable

Performance Factors (the ESCO is ultimately responsible for performance**): (equipment performance, operations, maintenance, repair & replacement)**

- Risks for the performance components of the RRPM have been clearly described and allocated
- Potential shortfalls in any responsibility have been considered along with resolution strategies. It should clarify what will happen if inadequate equipment performance, operations, maintenance, or repair & replacement impacts performance.
- Methods for validating performance and standards of service clearly hold the ESCO responsible for performance (this is required) and other areas where desired
- Day-to-day and periodic O&M strategies match site needs and provide effective, workable solutions
- Where the agency agrees to perform day-to-day O&M and/or R&R, strategies are defined that 1) clearly describe agency tasks and recordkeeping requirements, 2) hold the ESCO accountable for the O&M and/or R&R (e.g., ESCO defines and oversees or performs), and 3) describe how it will be reflected in the annual verification report.
- Strategies for addressing each risk are effective and acceptable

Management Approach:

- Key players, expertise, responsibilities, and the project organization needed to effectively develop and implement the project are identified and described
- Interaction plan with government to collectively build project is described

- Project Management Plan provides a framework for the efficient development of a proposal, implementation of the project, and long term project support to meet the government's objectives

M&V APPROACH:

- An M&V approach (A, B, C, D, from FEMP M&V Guidelines) is defined for each measure
- Annual verification and measurement activities are mentioned.
- M&V strategies manage risk well and are acceptable to agency

PRICE:

- ECM prices (refer to TO-2*) are approximately in line with expectations (benchmarks, rules of thumb, history). A reasonableness check is suitable for the PA (project facilitators may have benchmark ranges for direct costs of common ECMs such as lighting, variable-speed drives, and chillers).
- Contractor and other costs are within range of expectations and/or reasonable (refer to TO-2 and TO-3)
- TO-1: All annual payments are less than guaranteed annual savings (required)
- TO-1: Guaranteed annual cost savings are consistent with estimated annual cost savings
- TO-3: Interest payment for each year is consistent with project interest rate and loan balance

OVERALL:

(Y/N) Does this project meet much of the agency needs and all requirements? Or can it be easily modified to meet the needs?

(Y/N) Is this an appropriate project to pursue under a performance contract?

(Y/N) Is this a reasonable technical and financial deal for the government?

(Y/N) Is this a contractor with whom you can have a good long-term working relationship?

(Y/N) Have agency risks been evaluated and minimized?

(Y/N) Are all buildings included in the scope appropriate given facility master plan?

(Y/N) Are the overall percentages of energy and cost savings from the project reasonable?

* TO - Task Order Schedule

FEMP Federal Energy Management Program

① Acq Planning
② **ESCO Select.**
③ Proj. Dev.
④ Implementation
⑤ Performance

PA Review Template
ESPC Process Doc. P2-10
r. 3-8-16
Responsibility: NA

PRELIMINARY ASSESSMENT REVIEW TEMPLATE FOR FEDERAL ESPCS

Area Reviewed	Notes/Comments	Assessment*
• **Contract Requirements Met: (see Section H.5 of DOE ESPC IDIQ)**		
• **Scope – Energy Conservation Measures**		
*List each ECM** identified in the Preliminary Assessment. Make review comments as to whether each is reasonable, acceptable, and well described. Is overall package of ECMs comprehensive and does it provide a robust solution toward the agency's energy reduction goals and other needs?*	Recommended ECMs: ECM 1: ECM 2: Potential ECMs: ECM 1: ECM 2: Overall:	
• **RRPM Financial Factors:**		
• **RRPM Operational Factors:**		
• **RRPM Performance Factors:**		
• **Management Approach:**		
• **M&V Options/Approaches**		
Identify the M&V option for each of the ECMs and determine whether the offered strategy is appropriate for the ECM and whether the M&V option costs reflect a reasonable balance between cost and savings uncertainty.	ECM 1 M&V Option: ECM 2 M&V Option: ECM 3 M&V Option:	
• **TO Schedules**		
Note guaranteed cost savings and annual payments. Are payments less than guarantees and is contract within term? Note other terms & conditions or areas requiring discussion.		

A – Acceptable, M – Minimal changes needed, S – Significant changes required, U – Unacceptable
** Energy Conservation Measure*

INVESTMENT-GRADE AUDIT: REVIEW CHECKLIST

Project Name FEMP ID# Agency Project Facilitator Date of Review

_____

_____

_____

Overall

- ☐ IGA content consistent with Agency requirements
- ☐ All buildings included in the scope are appropriate given facility master plan
- ☐ Overall percentage energy and cost savings are reasonable
- ☐ Rebates and incentives were adequately pursued by ESCO
- ☐ Risks of emerging/underutilized technologies properly identified and brought to Agency's attention as necessary
- ☐ Where Agency accepting O&M responsibilities, reviewer has assessed the likelihood of problems and their potential impacts, and has brought these to the Agency's attention
- ☐ Risk, Responsibility, and Performance Matrix consistent with Agency expectations
- ☐ M&V strategies and costs provide good balance between cost and Agency risk
- ☐ Reviewer has assessed the overall reliance on Option A methods to ensure appropriate, given risks.
- ☐ Reviewer has examined percentage of project savings from electricity, gas, other fuels, water, and O&M, to identify where M&V should be focused
- ☐ Reviewer's written comments provided to Agency, and all comments, analysis, and supporting work archived and recallable upon request

For each form of energy and water (duplicate for each type of energy):

- ☐ Energy type: _____
- ☐ Baseline unit rate adequately documented.
- ☐ If blended rates are used, the methodology for calculating them is valid.
- ☐ Escalation rate adequately documented and consistent with FEMP guidance.

For each ECM (duplicate for each ECM):

Technical Category: _____

- ECM Name: _____
- FPE notified of need for technology expert review, if necessary
- ECM suitable for intended purpose and consistent with agency requirements
- Construction cost consistent with similar ECMs in recent projects
- Proposed construction schedule reasonable and consistent with previous projects
- Commissioning plan is adequate
- Methodology used to calculate baseline energy use adequate and supported by the included measured data
- Operating hour and other assumptions are reasonable and well-documented
- Energy savings estimate consistent with similar ECMs in recent projects, and is adequately documented
- Interactive effects with other ECMs considered in the calculations
- Assessed the need for expert review of building models (DOE-2, EnergyPlus, etc.) and obtained secondary reviews as necessary
- Simulation models adequately calibrated
- Sampling of equipment to calculate baseline performed correctly
- Energy cost savings calculation consistent with energy savings estimate and baseline energy unit prices.
- Energy-related O&M cost savings reasonable, well-documented and consistent with FEMP guidance, and supported by customer evaluation
- Added O&M costs for additional equipment adequately documented, and included in cash flow
- For ECMs with expected useful life less than project term, replacement plan is documented
- Post-installation M&V activities appropriate and adequate to determine potential to provide savings
- Annual M&V activities adequate and consistent with current FEMP guidance
- Planned measurements during post-acceptance M&V confirm performance as opposed to confirming operation
- Any sampling performed during M&V is adequate and consistent with FEMP guidelines
- Where M&V method depends on customer-maintained equipment, reviewer comments address the potential risks and/or recommend backup plan
- Where ECMs or M&V depend on connection to military LAN, reviewer comments address potential risks

TO Schedules

TO-1

- Implementation period savings and payments consistent with Agency expectations and FEMP guidance
- Estimated annual cost savings traceable to and consistent with ECM-level calculations
- Guaranteed cost savings consistent with estimated annual cost savings
- Annual contractor payments consistent with guaranteed cost savings, and are less than guaranteed savings in each contract year

TO-2

- Implementation expense of each ECM traceable to pricing calculations in body of IGA
- M&V expense for each ECM adequately documented

TO-3

- Implementation price consistent with total on schedule TO-2
- Performance period service prices adequately documented and consistent with previous projects of this size
- Interest payments for each year consistent with project interest rate and loan balance
- Loan balance correct for each year

TO-4

- Energy baseline and savings for each ECM and each form of energy consistent with calculations provided in the IGA
- Energy cost savings for each ECM and each form of energy consistent with energy savings and energy unit costs
- Other energy-related O&M costs for each ECM consistent with documentation in IGA

TO-5

- Cancellation ceiling for each year is consistent with remaining principle per Schedule TO-3 and agreed upon cancellation penalty ceiling

Summary of Key Issues/Findings (List main areas of concern identified in review)

ESPC M&V Best Practices for ESCOs

An ESCO M&V plan for ESPC projects includes the following best practices:

1. Metered consumption data is required for the M&V baseline. Estimating baseline consumption is unacceptable.
2. If the installation cannot provide measured consumption data from existing meters, the ESCO shall install meters to capture the data to build the baseline. It is the ESCO's responsibility to take whatever action necessary for the ECMs proposed to establish the baseline data.
3. The AF requires a minimum of 2/3 (67%) of the energy savings to be validated with metered data using Option B (sub-meters) or Option C (whole-building meters), with the preference being Option C.
4. A minimum of 12 months of metered data is usually required to establish the baseline per FEMP guidelines for M&V. AFCEC will accept less than 12 months (for example, 6 months) of metered data if the appropriate season(s) for heating &/or cooling (depending on type of ECM) is included in metered data, and if data sufficiently correlates (prefer $R^2 > 0.8$) with weather or other factors. AFCEC approval is based on a case by case analysis, per ECM.
5. The installation shall not provide funds to support metering requirements. Metering costs are to be included in the ESPC.
6. The AF does not accept M&V plans that transition from Option C (after a minimal number of years) to Option A or B during an ESPC performance period, without AFCEC/CND approval.
7. Option B measures consumption of the selected ECM using sub-meters, such as electrical or natural gas. It is not an estimate from the building automation system (BAS) or a calculation using other parameters.
8. Good candidates for M&V Option C are buildings in which all ECMs combined in an individual building produce savings predicted to be greater than 10% of the individual building's overall baseline consumption. Buildings that are identified as candidates for Option C shall have all ECMs performed within that building by M&V performance verification as Option C.
9. When there are multiple ECMs in a building where Options A and B are proposed, AFCEC recommends that the ESCO use M&V **Option C** and aggregate all savings from those ECMs as a whole, and do a onetime comparison to the facility meter for verification.

In summary, for M&V requirements, a minimum of 2/3 of the guaranteed savings for any ESPC project must be validated with meter readings confirming the **actual savings**. If all ECMs combined in an individual building produce savings predicted to be greater than 10% of the individual building's overall baseline consumption per FEMP Guidelines for M&V, use **Option C**.

Measurement of the 2/3 guaranteed energy savings is the minimum for M&V at TO award. During negotiations it is recommended to start at a higher goal such as metering 80% . The higher the percentage, the better, and Option C is considerably less expensive than multiple Option "A" or "B" solutions for each individual ECM. Option C provides a more precise measurement of overall savings and verification that the savings have been achieved.

The COR is required to witness the annual M&V performed by the ESCO. With regard to M&V witnessing, Option C is the most efficient method to verify savings because Option C is the most accurate while also being the easiest and quickest to witness.

AFCEC

UFC 3-530-01 Change 3 on TLED Requirements

15Mar2017

UFC 3-530-01 Change 3, dated 01-June-2016, TLEDs

AF has now determined that TLEDs are now authorized with the following stipulations:

1. They must not require any electrical/mechanical modifications to the existing fixture with the exception of changing out ballasts if necessary (by-passing the ballast is prohibited).
2. If ballasts are replaced as part of the project, the new ballasts must also be able to meet the advanced control requirements for each space IAW ASHRAE 90.1; however, installing controls is not necessary if not currently cost justifiable. Future energy/lighting projects can install advanced controls to achieve further energy reduction when they become cost justifiable without also having to replace the TLED and/or ballast again.
3. Specific TLED lamps that are selected must meet all the parameters and performance requirements listed in the UFC paragraph 2-8.4 Light Source Retrofit.

Best Practices for ESPC Portfolio Review

Preface

This report is a product of the Federal ESPC Steering Committee Working Group. The information provided within this document serves to highlight best practices for review of a portfolio of federal Energy Savings Performance Contract (ESPC) projects. The document aims to outline potential elements of a systematic approach to evaluating the performance of an agency's ESPC portfolio as a whole, in addition to the performance of individual projects within the portfolio. Agencies may consider utilizing the approaches outlined within this document in combination with the agency's determined policy for review of ESPC project portfolios.

Contents

Definitions

Energy Savings Performance Contract (ESPC): A multiyear, firm fixed-price contract between a Federal agency and an energy service company (ESCO) solely for the purpose of achieving energy savings and benefits ancillary to that purpose, with a term not to exceed 25 years for the provision of supplies or the performance of services for the design, acquisition, installation, testing, measurement and verification, and, where appropriate, operation, maintenance, repair, and replacement, of an identified energy conservation measure, water conservation measure, or series of energy conservation measures or water conservation measures at one or more locations.
Energy Conservation Measure (ECM): Measures that are (1) applied to a Federal building; (2) improve energy efficiency; (3) are life cycle cost effective; and (4) that involve energy conservation, cogeneration facilities, renewable energy sources, improvements in operations and maintenance, or retrofit activities.

Measurement and Verification (M&V): the process of measuring and verifying energy, water, and related cost savings.

Performance Period: The period after government acceptance of the ESPC project where by the energy service company (ESCO) delivers the savings and equipment performance, as contracted, and conducts the annual measurement and verification (M&V) activities described in the M&V plan. Through witnessing of the ESCO's annual M&V activities and review of the ESCO's annual M&V report, the government ensures that savings guarantees are met. The government also performs the operation and maintenance functions specified in the contract during this period.

Guaranteed Savings: The value of energy and energy-related cost savings contractually agreed upon to be delivered by the ESCO from the measures implemented under an ESPC project. In Federal ESPCs, guaranteed energy and energy-related cost savings are established on an annual basis.

Verified Savings: The value of energy and energy-related cost savings delivered by the ESCO from the measures implemented under an ESPC project as determined under the contractually agreed upon Measurement and Verification (M&V) plan. In Federal ESPCs, verified energy and energy-related cost savings are determined on an annual basis.

Risk, Responsibility, and Performance Matrix (RRPM): A document that assigns the risk, responsibility, and performance of various responsibilities of an ESCO's proposed approach under an ESPC.

Escalation Rate: The rate of change in price for a particular good or service. Under an ESPC, an escalation rate is used to determine annual contractor payments, which are based on projected annual energy cost savings.

1. Introduction

Energy Savings Performance Contracts (ESPCs), have become an effective tool for financing energy projects in both federal and non-federal facilities. The U.S. Department of Energy's (DOE) Federal Energy Management Program (FEMP) has been providing project support and training to federal agencies since 1996. As federal agencies have implemented projects, their acquisition teams and FEMP have taken note of lessons learned and best practices, which over time have been incorporated into the DOE Indefinite-Delivery, Indefinite-Quantity (IDIQ) ESPCs, FEMP ESPC training, and FEMP project assistance.

This document highlights current best practices that agencies may consider using in combination with an agency's determined policy in reviewing their portfolio of ESPC projects. This best practices document is not all encompassing and does not replace other FEMP services that include evaluation and discussion of best practices, such as services from FEMP Federal Project Executives (FPEs) and Project Facilitators (PFs).

Agencies may use this document in addition to all of FEMP's ESPC resources in awarding and maintaining high-quality and high-value ESPC task orders (TOs). FEMP ESPC guidance, contract document templates and examples, and other informational resources are available at http://www1.eere.energy.gov/femp/financing/espcs_resources.html.

This portfolio review best practices document aims to outline elements of a systematic approach to evaluating the performance of an agency's ESPC portfolio as a whole, in addition to the performance of individual projects within the portfolio, by assessing:

- Achievement of annual guaranteed savings in accordance with contract terms,
- Identification of impacts to a project's savings and required corrective actions,
- Considerations for contract modification to address site changes affecting ECM performance, and
- Documentation of agency completion of contract responsibilities and oversight

This document presents factors that agencies may consider and evaluate as part of a performance contracting portfolio review to determine if additional resources and/or project modifications are required based on their agency and/or organizational policies. Agencies should consult with the CO and agency counsel on matters of modifications to ESPC contracts. Users should take into account the performance and net benefits of the entire portfolio when determining if project level actions are warranted to a given performance aspect of an ESPC project.

Section 10 of this document contains an example of a form for documenting a portfolio review summary of findings and the planned action for each topic covered in this best practices document. In addition, Appendix A contains a template for structuring a portfolio report consistent with the review approach outlined in this document.

Agencies are encouraged to reach out to FEMP with any questions pertaining to this guidance.

2. Portfolio Summary

A comprehensive portfolio-level review would consist of gathering the contractual status of all previously awarded ESPC projects, identifying those that are (1) under construction, (2) in the

performance period ("M&V Phase"), (3) have completed their contract term, (4) or were terminated or canceled before the end of the contract term. Additionally, collection of current and historical performance of all awarded ESPC projects should include a calculation of the cumulative guaranteed and verified savings, both at the individual project and portfolio-wide levels. Guaranteed and verified savings are provided in an annual measurement and verification (M&V) report from the Energy Services Company (ESCO) responsible for each ESPC project. Viewing the cumulative savings across the history of ESPC projects and the portfolio will provide an opportunity to assess the broader overall benefits of the agency's performance contracting efforts and aid in identifying trends in the performance or management of projects on a historical basis.

3. Project Performance

At a minimum, portfolio review will require a compilation of the current performance findings for all projects actively in the performance period. This will include collecting the guaranteed and verified savings data from the most recent M&V reports from the ESCOs. Additionally, each project should be assessed for the following:

1. Does the verified savings meet or exceed the guaranteed savings in accordance with the M&V Plan for the project?
2. For cases where the verified savings has not met the guaranteed savings and the ESCO is responsible for the shortfall:
    a. Has the ESCO identified and implemented a corrective action to restore savings?
    b. Was/will the invoice payment to the ESCO adjusted to offset the lost savings?
3. Has the ESCO documented instances where agency action has impacted energy and energy-related cost savings?
    a. Example: Agency removes building with ECMs, or fails to perform agreed upon maintenance, thus impacting energy and energy-related cost savings.
    b. **NOTE:** ESCOs may not capture agency impacts to savings within the "verified savings" value that is reported, as such impacts are typically outside of agreed upon terms within M&V plan and Risk, Responsibility and Performance Matrix (RRPM).
4. For cases where the agency has negatively impacted the energy and energy-related cost savings:
    a. Does the agency have a corrective action to restore the savings?
    b. If savings will not be restored, the agency should consult the project Contracting Officer and agency counsel about taking action to modify or terminate the ESPC.
5. Annual Operation and Maintenance (O&M):
    a. Where provided by the ESCO, is the ESCO performing O&M as set forth under the contract? If not, has this been communicated to the ESCO? Has a corrective action been developed and implemented by the ESCO?
    b. Where provided by the agency, is the agency performing O&M as set forth under the contract? If not, has the agency developed and implemented a corrective action?

4. Life of Contract Management

As part of an effective approach to administration and management of the ESPC portfolio, the agency should evaluate its "life of contract" approach with respect to each project and the personnel supporting the agency's performance contracting efforts. Detailed FEMP guidance on developing a life of contract plan for each project in your ESPC portfolio can be found at: http://energy.gov/eere/femp/downloads/doe-espc-life-contract-plan-template. As part of a portfolio

review, elements to be assessed and questions to be considered would include:

1. Is the staff administering contracts (Contracting Officer, Contracting Officer Representative, Site Energy Manager) sufficiently trained in ESPCs? If not, plan for taking FEMP's ESPC contract administration courses.
2. Has the Contracting Officer designated a primary contact that is responsible for maintaining continuity of documentation and awareness of the ESPC project throughout the performance period?
3. Is the project audit-ready? Review a checklist of contract documents on file for each project.
4. Confirm that agency staff are witnessing annual ESCO M&V activities and verifying compliance with the contract's M&V plan.
5. Confirm that agency staff are reviewing annual M&V report and providing notification to the Contracting Office that the report was received, reviewed and approved and noting any ESCO shortfalls to the guarantee that require invoice adjustment.
6. Are ESCO payments being made in a timely manner?

5. Interest Rates

Since federal performance contracts may have a maximum contract period of 25 years and ESPCs are frequently structured with terms of 17-20 years, market interest rates may vary significantly over the performance period of any contract or task order. When the interest rate on a contract is significantly higher than the current market rates and sufficient time remains on the contract, the Contracting Officer may wish to explore with the ESCO whether debt modification is appropriate and whether the ESCO is willing to explore modifications to the ESPC agreement to benefit both parties. Keep in mind that ESCO and financier costs associated with restructuring the debt would likely be incurred and need to be considered as part of an assessment of potential savings from a restructuring effort.

In considering the impact of debt modifications on ESPCs, it is important to recognize that ESPC financing arrangements are between the ESCO and a third-party financier – the Government is not a contractual party. Responsibility therefore rests with the ESCO to initiate communication with its financier regarding a debt modification. FEMP guidance related to the topic of refinancing, restructuring, or modifying loan agreements entered into by an ESCO under a federal ESPC can be found on the DOE FEMP website at the following link: http://energy.gov/sites/prod/files/2013/10/f3/1_4_idiqrefinance.pdf

6. Utility Rates

Federal agencies may rely on estimated energy and water tariffs in determining projected energy savings. To the extent that future energy or water rates are known at the time of contract formation, the calculation of ESPC payments should rely on known values. If future energy or water rates over the term of an ESPC are unknown at the time of contract formation, federal agencies are authorized to rely on estimated values in determining the energy or water tariffs. For additional guidance on ESPC utility rate estimations see Federal ESPC FAQ on Scope of 42 U.S.C. § 8287, *et seq*. and FEMP's guidance on utility rate estimations and weather normalization in an ESPC.

FEMP's Energy Escalation Rate Calculator (EERC), a cost calculator for estimating escalation rates in performance contracts, was developed under a FEMP contract with the National Institute of Standards and Technology (NIST) to develop life-cycle costing tools for the purposes of federal energy management. EERC incorporates the projections for changes in future energy costs in various regions of

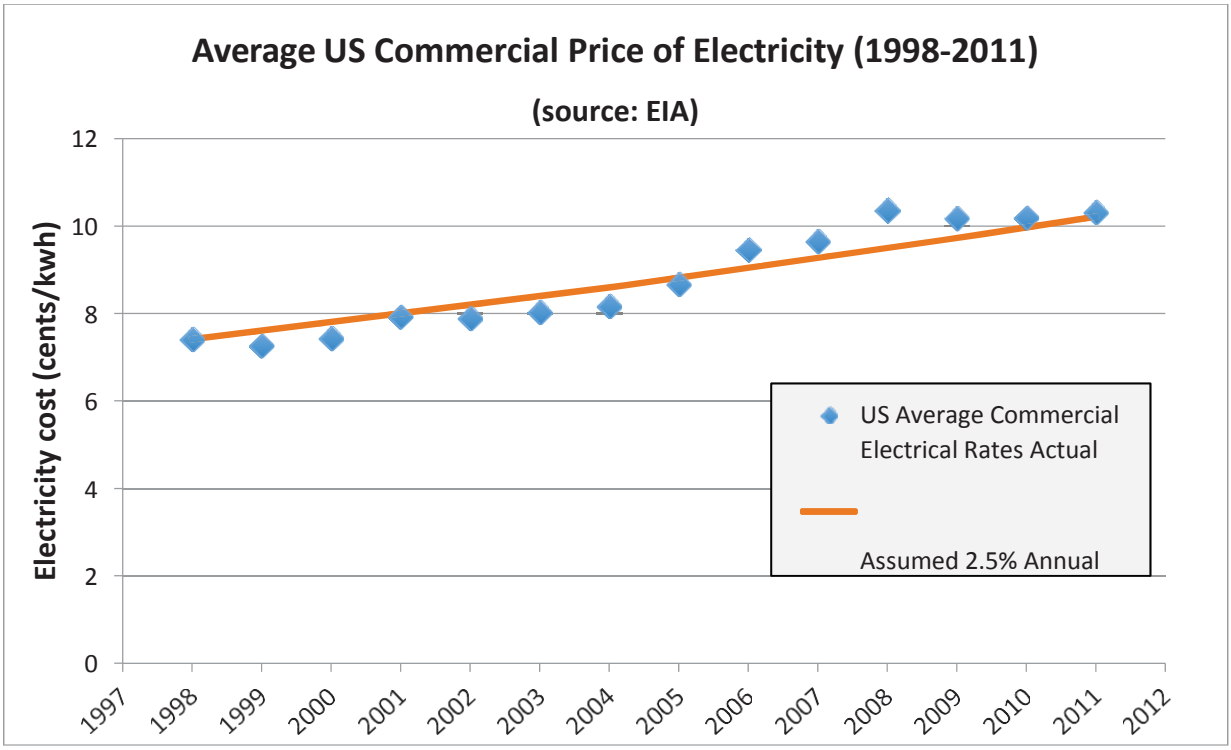
the country based on energy price projections from the Energy Information Administration (EIA). It also incorporates a long-term inflation rate that is annually calculated by NIST. A 2015 study by Lawrence Berkley National Laboratory[1] found that EIA's analysis of its historical predictions show a systematic under prediction of energy prices and thus the EERC tool likely has a tendency to under-predict escalations.

Performance contracting escalation rate assumptions, including those generated by the EERC tool, are typically applied as a consistent year-over-year percentage increase. As seen in the plot of average US commercial electricity rates in the chart below, a project with an assumed electric utility rate escalation of 2.5% annually would appear to have over-estimated electricity rates in 5 of the first 7 years of the contract. Conversely, electricity rates would appear to have been underestimated for 5 out of the last 6 years of the contract. The actual electrical utility rate increased by an average of 2.5% over the 13-year period. This example illustrates the importance of agencies being authorized to estimate future energy prices; otherwise there would be a significant increase in the burden to administer performance contracts with little benefit.

Some ECMs may warrant additional monitoring, such as combined heat and power (CHP) and biomass generation with the capability of fuel switching (i.e. the site already has the ability with existing capacity to choose between fuel types and/or equipment to meet site energy needs). Additional monitoring may be required to determine the most cost effective operation of the equipment based on current fuel prices. Consider the following two examples:

1. Based on current natural gas rates it may be determined that it is more economical to run a boiler on natural gas than the originally intended biomass.
2. Based on current electricity prices it may be determined that it is more economical to purchase grid electricity than to utilize on-site generation via a CHP ECM.

[1] P. Coleman, 2015, Escalation Rates in Energy Savings Performance Contracts, https://buildings.lbl.gov/sites/all/files/lbnl1004319.pdf



7. Contract Modification or Termination due to ECM Performance

ESPCs are commonly structured as long term task orders, often exceeding 17 years in length and thus may be affected by site changes. Changes to site conditions such as equipment removal, replacements, demolitions or other changes in usage of ECMs installed as part of the performance contract will require assessment by the agency to determine whether a modification, termination, or cancelation of the task order is warranted.

Underperforming ECMs

For ECMs that (1) produce savings that fall short of guaranteed savings and (2) will not have corrective action implemented to restore savings to levels that eliminate the shortfall, the agency CO may determine that a contracting action is required to modify or terminate the contract with respect to those ECM's responsible for the shortfall in savings.

FEMP's M&V reporting template provides a best practice for reporting impacts to savings (positive and negative) as part of Tables E3 and E4 of the Annual M&V Reporting template (http://energy.gov/sites/prod/files/2016/01/f28/mv_guide_4_0.pdf - See Appendix E-1)

Removed or Decommissioned ECMs

In rare circumstances, mission needs may require the demolition or decommissioning of a building or buildings where an ESPC has been implemented or necessitate the removal of ECM equipment by the government. In cases such as these, it is suggested that the agency Contracting Officer promptly initiate a contracting action to modify or terminate the portion of the contract pertaining to such ECMs that are no longer in place or are no longer functional.

In taking action to modify, terminate, or cancel all or part of an ESPC, agencies should consult the project Contracting Officer and agency counsel.

8. Savings Beyond Contractual Agreements

Net cost savings to the government in federal ESPC projects are generally believed to be small, given that most of the guaranteed energy and energy-related cost savings accruing over the life of the contract are paid to the ESCO. However, this belief is based on the assumption that the guaranteed savings are more or less equal to the actual avoided costs associated with the project. ORNL's report "Beyond Guaranteed Savings: Additional Cost Savings Associated with ESPC Projects" (http://info.ornl.gov/sites/publications/Files/Pub41816.pdf) outlines four principal sources of cost savings that are not captured in the calculation of the guaranteed savings:

1. The ESCO does not guarantee all of the savings it estimates;
2. The useful life of the equipment extends beyond the performance period of the ESPC;
3. National Institutes for Standards and Technology (NIST)/Energy Information Administration projections for energy price escalation have been very conservative with respect to actual price increases; and
4. The baseline case that forms the basis of the guaranteed savings calculation assumes that the baseline equipment would maintain the same efficiency and require the same level of maintenance for a period of time equal to the performance period of the ESPC.

As part of a comprehensive portfolio review, an agency may wish to consider some of the factors outlined in the ORNL paper when evaluating the full benefit of an agency's ESPC efforts.

9. Future ESPC Opportunities

As part of ongoing ESPC planning, an annual review of the EISA 432 Compliance Tracking System (CTS) data can aid in determining new opportunities for ESPCs. CTS data is available at http://energy.gov/eere/femp/eisa-federal-covered-facility-management-and-benchmarking-data

Questions and elements to consider in expanding the agency's ESPC portfolio include:

1. Have sites already identified potential cost effective energy/water conservation projects?
2. Review opportunities for bundling multiple sites under a single task order award.
3. Use FEMP's ESCO Selector tool and explore a new ESPC. Available at http://hyperion.ornl.gov/noo/
4. Consider ESPC ENABLE which is designed to permit a standardized and streamlined procurement process for small federal projects to install targeted energy conservation measures (ECMs) in six months or less. ESPC ENABLE can also help agencies address buildings within a site that have not been addressed under previous ESPC efforts at the site.

10. Portfolio Review Findings and Plan of Action

The final step of the agency's portfolio review should be to document each of the elements considered across the entire review along with a summary of findings and plan of action for each of the major categories and elements outlined in this best practices document. The following table offers a sample format for documentation.

Portfolio Review Findings and Plan of Action		
Portfolio Performance		
Element Reviewed	Findings	Plan of Action
Cumulative savings vs. guaranteed		
Savings beyond the contract		
Project Performance		
Element Reviewed	Findings	Plan of Action
a. ESCO Shortfalls	General:	General:
	Site 1:	Site 1:
	Site 2:	Site 2:
b. Agency Impacts		
c. O&M Issues		
Life of Contract		
Element Reviewed	Findings	Plan of Action
a. Staff Training		
b. Primary Contact assigned per project		
c. Project Documentation in order		
d. M&V Witnessing occurring		
e. M&V Report Review occurring		
f. Timely ESCO Payments		
Interest Rates		
Element Reviewed	Findings	Plan of Action
a. Interest Rate Assessment		
Utility Rates		
Element Reviewed	Findings	Plan of Action
a. Utility Rate Assessment		
Contract Mods/Terminations		
Element Reviewed	Findings	Plan of Action
a. Assessment of Needed Contract Modification		

APPENDIX A

The following is a portfolio report template for structuring performance contracting project data in a manner aligned with the review approach outlined in this best practices document.

Performance Contracting Portfolio Report TEMPLATE

Agency:

Report Date:

1. Portfolio Summary

	# of Projects	Investment ($)	Cumulative Guaranteed Cost Savings To Date ($)	Cumulative Reported Energy and Energy-related Cost Savings To Date ($)	Reported Savings as % of Guaranteed Savings	Cumulative Energy Savings To Date (MMBTU)
All Projects						
Active (Pre-Performance Period)			N/A	N/A	N/A	N/A
Active (In Performance Period)						
Completed (ran full contract term)						
Terminated (early buyout)						

2. Active Project Performance Summary
(Utilize latest years M&V report data)

Number of Active Projects in Performance Period (in M&V)	Total Guaranteed Savings from Latest M&V Reports	Total Reported Verified Savings from Latest M&V Reports (per M&V plan)	Total Agency Impacts to Energy and Energy-Related Cost Savings Identified Outside of Reported Verified Savings	Net Surplus or (Deficit) to Guaranteed Savings (Verified- Total Agency $ Impact)

3. Project Contract Summary

Project #	Mod to project #	Project Name/Site	Status	Investment ($)	Award Date	Contract Term (yrs)	Financing Rate (%)
			Example: "In Construction"				
			Example: "In M&V"				
			Example: "Terminated"				

4. Project Performance (Project in Performance Period/M&V)

Project #	Project Name/Site	Guaranteed Savings met per M&V plan (Y/N)	Agency Impacts to Energy and Energy-Related Cost Savings (Y/N)	Evidence of Agency M&V Witnessing (Y/N)	Evidence of Annual M&V Report Review (Y/N)	Notes

5. Shortfall/Agency Impact Details

Project #	Project Name/Site	Shortfall/ Impact ($)	Responsibility	Payment reduced to ESCO?	Resolution Path (see key below)	Notes
			Example: "ESCO"		*Example:* "3."	
			Example: "Agency"		*Example:* "4."	

Shortfall Resolution Key

1. ESCO Responsible, permanent shortfall
2. ESCO Responsible, ESCO has plan to restore savings
3. ESCO Responsible, ESCO plan to restore savings unclear
4. Agency Responsible, Taking corrective action to restore savings
5. Agency Responsible, Status of corrective action unknown
6. Agency Responsible, ECM(s) removed, taking action to modify contract
7. Agency Responsible, ECM(s) removed, agency determined that no contract modification will be taken
8. Agency Responsible, ECM(s) removed, agency action unknown

6. Life of Contract Findings

Include text that will highlight any key performance issues or findings from agency programs or efforts to assess annual performance of projects though contact and/or feedback directly with the project site.

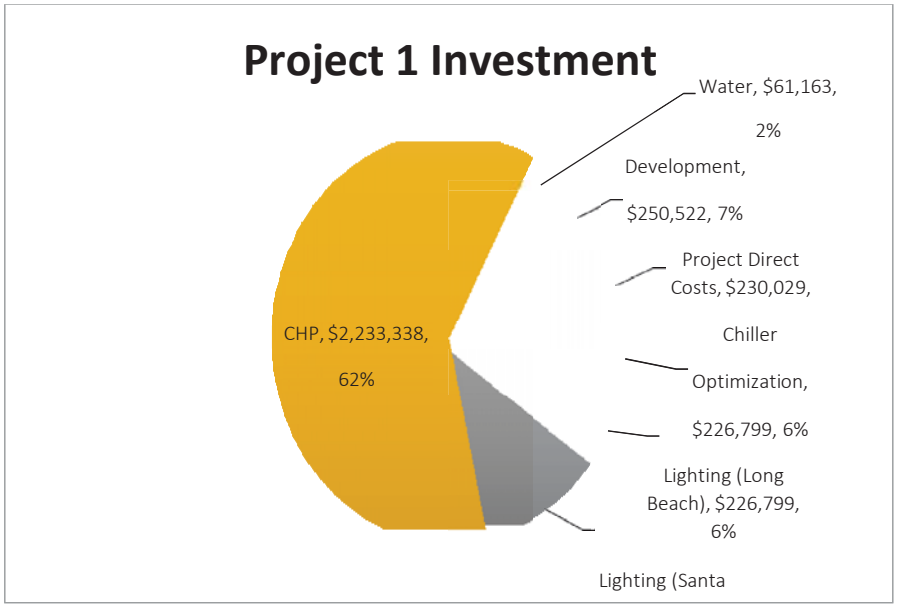
7. Project Level Details

(*For Each Project in Performance Period)*

Project 1:
Date Awarded: X/X/XX
Investment: $
Contract Term: X Years (Performance Period)
Financing Rate: X%
Current Status: Year X of 17
ESCO:

Project Investment by Energy Conservation Measure:

(EXAMPLE)



Escalation Rates:

Utility	Escalation Rate	Rates Utilized in Latest M&V report
Electricity		
Natural Gas		
Water/Sewer		
O&M		

Project Performance:

(For each year of performance to date)

Performance Year	Performance Period	Guaranteed Savings ($)	Verified Savings ($)	Variance	Cumulative Variance
Year 1	d/m/y – d/m/y	$	$		
Year 2	d/m/y – d/m/y	$	$		
Year 3	d/m/y – d/m/y	$	$		
Year 4	d/m/y – d/m/y	$	$		

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

AFGM2017-32-01

2 February 2017

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: AF/A4C
1800 Air Force Pentagon Washington
DC 20330-1800

SUBJECT: Air Force Guidance Memorandum, *Civil Engineer Control Systems Cybersecurity*

ACCESSIBILITY: Publication is available for downloading on the e-Publishing web site at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum (AFGM) immediately establishes cybersecurity policy for civil engineer (CE)-owned or operated control systems (CS). This Memorandum details the unique operational characteristics of Air Force (AF) CS, outlines roles and responsibilities for managing risk under the Risk Management Framework, and implements guidance and policy for securing and mitigating risk to AF CE CS.

This Guidance Memorandum supersedes *Engineering Technical Letter 11-1* and applies to all military and civilian Air Force personnel, the Air Force Reserve and the Air National Guard. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force (AF) publications, the information herein prevails, IAW AFI 33-360, *Publications and Forms Management*.

Ensure all records created as a result of processes prescribed in this publication are maintained IAW AFMAN 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). This Memorandum becomes void after one year from the date of this Memorandum, or upon the publication of a new Instruction permanently establishing this guidance, whichever is earlier.

JOHN B. COOPER, Lieutenant General, USAF
DCS/Logistics, Engineering & Force Protection

2 Attachments:

1. Control Systems Background
2. Cybersecurity Policy for Civil Engineer Control Systems

BREAKING BARRIERS...SINCE 1947

Attachment 1

CONTROL SYSTEMS BACKGROUND

A1.1. Control Systems Overview.

A1.1.1. Control systems are integrated hardware and software designed to monitor, or monitor and control, the operation of equipment, infrastructure, or associated devices. Control Air Force Civil Engineering systems consist of a combination of technology (computers, human-machine interfaces (HMI)) and control components (electrical switches, mechanical actuators, environmental sensors) that act together upon underlying mechanical or electrical equipment to achieve a physical objective (the transport of matter or energy, control of a dynamic process, or maintenance of a secure and comfortable work environment, etc.) Generally, these special-purpose systems regulate the flow of electricity, fluids, gases, air, traffic, and even people.

CS are comprised of several sub-groups of systems including building automation systems and industrial control systems (ICS). Various categories of ICS include supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLC), intelligent HMI modules, and other dedicated CS configurations often found in the industrial sector and support critical infrastructure.

A1.1.1.1. SCADA systems are highly distributed systems used to monitor and control geographically-dispersed assets where centralized data acquisition, control, and status reporting are critical to system operation. SCADA systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.

A1.1.1.2. DCS are used to control industrial processes such as electrical power generation, oil refineries, water/wastewater treatment, manufacturing production, and materiel distribution. DCS are integrated control architectures that provide supervisory-level control and integration over subsystems responsible for local process control.

A1.1.1.3. PLC are proprietary processor-based, solid-state devices found in almost all industrial equipment and processes to provide logic algorithms for connected input and output devices. They can vary in sophistication from simple, stand-alone microcontrollers to sophisticated, multi-processor controllers that provide advanced motion control, network capability, error detection, diagnostics, process recovery, and fail-safe redundancy. While PLC are components of DCS and SCADA systems, they are often the solitary control device for smaller CS configurations used to provide operational control of separate processes.

A1.1.1.4. A list of AF CE-owned CS can be referred to in section A1.2.

A1.1.2. Throughout the Air Force, CS are typically used to monitor and/or control electricity; facility heating, ventilation, and air conditioning (HVAC); interior and exterior lighting; water and wastewater; natural gas distribution; certain intrusion detection systems and fire/life safety systems (such as fire alarm reporting systems and fire suppression systems). CS are a critical part of automation and are used extensively to optimize resources supporting nearly all aspects of Air Force core mission areas.

A1.1.3. Historically, CE CS were neither automated nor networked. Devices used for monitoring or control had no computing resources, and those that were digitized typically used proprietary protocols and PLCs rather than full computer control. As controllers became interconnected, they were not designed with traditional IT system and security considerations, as they were expected to operate as isolated systems running on their own dedicated network with proprietary communication protocols and specialized hardware and software. This intentional separation from AF-wide traditional IT (e.g., e-mail, web access, networked printing, or remote access) allowed CS to be easily connected, open and accessible, highly stable, and readily serviced.

Today, however, CS are designed using standard platforms, operating systems, network protocols, and access controls commonly found in traditional IT systems. The ever- increasing connectedness of CS allows for greater operational capabilities, efficiencies, and automation. However, this integration also introduces new vulnerabilities that expose both the CS and the underlying network to threats.

A1.1.4. Special precautions must be taken when introducing IT security controls and solutions to CS environments because of the unique ways CS communicate and operate. Interconnections between CS and organizational networks/business systems are a particular point of focus for security and should be carefully considered. In all cases, security solutions must be tailored to the specific CS environment and verified to ensure their impact to the CS is not detrimental to a CS's operation.

A1.1.5. CS can have long life spans (often exceeding 20 years) and can be comprised of technology that suffers rapid obsolescence. This longevity introduces several issues. Most importantly, older hardware and software may no longer be supported by the manufacturer. Companies can go out of business or terminate their support for an installed product. Because of this, patches and forward support for compatibility with new operating systems may no longer be available as new vulnerabilities are discovered.

A1.1.6. In the traditional IT domain, where data is the preeminent priority, cyber defenders often focus on preventing the disclosure of information to unauthorized individuals or processes. Consequently, confidentiality tends to be the most important attribute among the three properties of the confidentiality – integrity – availability (CIA) triad. However, with CS, it is paramount to actively manage or monitor physical processes and maintain high availability and positive control of the system. Therefore, availability and integrity of the CS take precedent over confidentiality. It is this difference in cybersecurity priorities that impacts what security controls and procedures are appropriate to implement for CS compared with those of traditional IT.

A1.1.7. The goal of securing CS components is to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the CS as much as possible. Therefore, security controls such as intrusion detection software, antivirus software and file integrity checking software should be utilized to the fullest extent technically feasible. However, it is also recognized that CS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT processes. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.

A1.1.8. CS and their real-time operating systems are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems are often lacking resources common on modern IT systems. Many systems may not have desired features including encryption capabilities, error logging, and password protection.

Indiscriminate use of IT security practices in CS may cause availability and timing disruptions. There may not be computing resources available on CS components to retrofit these systems with current security capabilities. Adding resources or features may not be possible.

A1.2. Scope. AF CE-owned CS include, but are not limited to, the following types of systems (including all points, devices, control panels, means of connectivity, software, controllers, computer workstations, servers, etc.):

A1.2.1. SCADA Systems

A1.2.1.1. Protective relays (microprocessor-based)
A1.2.1.2. Cathodic protection systems
A1.2.1.3. Natural gas distribution systems
A1.2.1.4. Power generation systems, including renewable systems
A1.2.1.5. Water/wastewater distribution systems
A1.2.1.6. Water/waste treatment systems

A1.2.2. Building Automation Systems (BAS)
A1.2.2.1. Energy Management Control Systems (EMCS)
A1.2.2.2. Advanced Meter Reading Systems (AMRS)
A1.2.2.3. Interior/exterior lighting controls

A1.2.3. Fire/Life Safety systems
A1.2.3.1. Fire Alarm Reporting Systems (FARS)
A1.2.3.2. Fire Suppression Systems (FSS)
A1.2.3.3. Facility Mass Notifications Systems

A1.2.4. Utility Monitoring and Control Systems (UMCS)
A1.2.4.1. Electrical distribution systems
A1.2.4.2. Generator monitoring systems

A1.2.5. Airfield Control Systems
A1.2.5.1. Airfield Lighting Control Systems (ALCS)
A1.2.5.2. Aircraft Arresting Systems (AAS)
A1.2.5.3. Runway Ice Detection Systems (RIDS)
A1.2.5.4. Bird abatement systems
A1.2.5.5. Ramp lighting control systems

A1.2.6. Vehicle Traffic controls
A1.2.6.1. Drop-arm barriers
A1.2.6.2. Pop-up barriers
A1.2.6.3. Traffic signal systems

A1.2.7. CE-maintained Intrusion Detection Systems

Attachment 2

CYBERSECURITY POLICY FOR CIVIL ENGINEER CONTROL SYSTEMS

A2.1. Applicability. Due to the unique nature of CS, there is a need for specific control system guidance and policies to help secure, maintain, and provide mission assurance of the critical infrastructure and missions these systems support.

A CS is considered operational technology (OT), which is IT adapted to directly monitor and/or control physical devices, processes and events where availability is the primary operational concern. Accordingly, OT is more sensitive to the application of cybersecurity measures and controls that can affect its availability. The Authorizing Official (AO) assigned to the CS boundary is responsible for managing the risk for OT and may tailor controls to balance security and availability.

Air Force CE CS consist of OT classified as either Real Property Installed Equipment (RPIE) or Non-RPIE Equipment. Figure 1 represents the elements that comprise CS in addition to OT's affiliation with the Platform IT (PIT) category of Air Force IT, defined further in AFI 17-101. Referencing AFI 17-101, Platforms and Non-RPIE Equipment would generally be classified as types of "PIT Systems" or "PIT Subsystems."

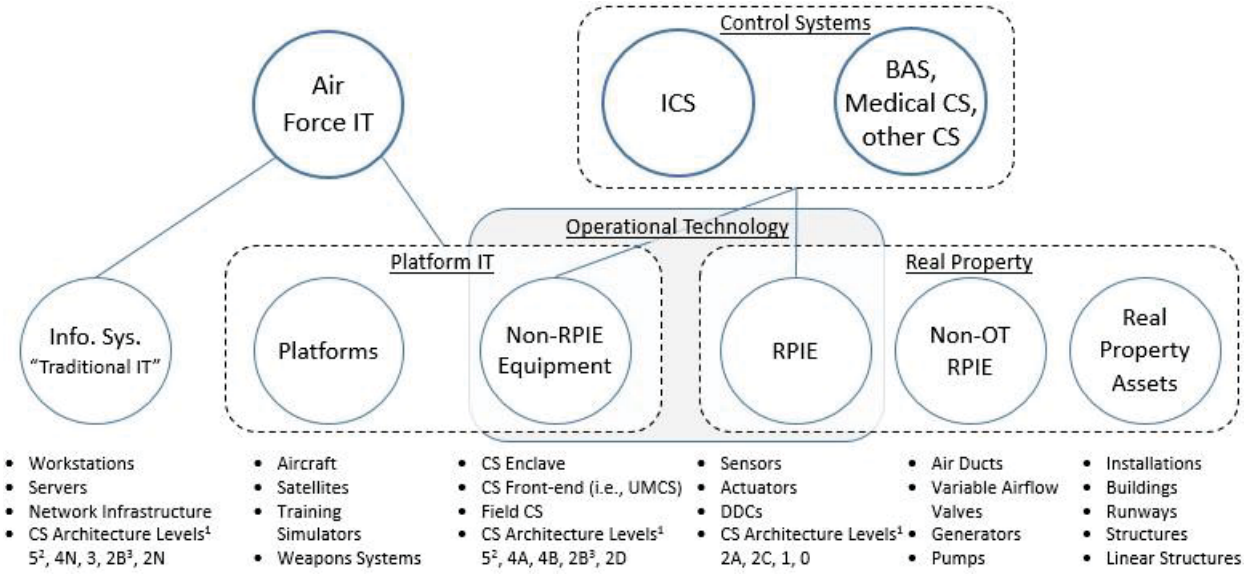


Figure 1: Categorization of AF IT and CS

Attachment 2 outlines some of the defensive cybersecurity policies to be adhered to throughout the life cycle of CS operating on AF installations. These policies are not meant to supersede any established Federal, Department of Defense (DoD) or AF policy, but instead are intended to supplement existing policy (such as DoDI 8500.01) and DoD's Risk Management Framework (RMF) (outlined in DoDI 8510.01) by providing guidance on security measures.

[1] From Unified Facilities Criteria 4-010-06, *Cybersecurity of Facility-Related Control Systems*, Appendix E

[2] Equipment in CS Architecture Level 5 is considered Non-RPIE Equipment when installed as part of a CS enclave. [3] CS Architecture Level 2B is considered an Information System as a Base Area Network (BAN) access switch and Non-RPIE Equipment when part of a CS in Levels 0-2.

A2.2. Standard Level of Cybersecurity Service. At a minimum, the standard cybersecurity level of service for base CE organizations is to be compliant with this AFGM for the CE-owned, operated, or managed on-base assets supporting identified Defense Critical Infrastructure (DCI) missions and capabilities. These procedures and guidelines should also be followed in a prioritized manner for the remaining infrastructure under CE's ICS PIT AO boundary (introduced in section A2.4.1).

A2.3. Installations' CS Inventory. Installations will conduct and maintain accurate inventories of all CS under the purview of CE. The installations' CS inventory should provide thorough awareness of existing systems, their interconnections, and their link to the mission or function they serve. For more information on the recommended content and CS inventory specificity, see NIST SP 800-82.

A2.3.1. The CS inventory at installations shall include both hardware (physical devices and systems) and software (communications platforms and applications) down to Topology Tier Level 2 at a minimum. A diagram of CS topology, its associated levels and components are defined and exemplified in Unified Facilities Criteria 4-010-06, *Cybersecurity of Facility-Related Control Systems*, Appendix E.

A2.3.2. The inventory shall include descriptions of CS-supported assets and infrastructure, and whether the CS supports DCI as determined by A3OA or locally-derived mission critical capabilities. Actual names of critical infrastructure, Task Critical Assets (TCA), or Defense Critical Assets (DCA) should not be listed in an unclassified environment. TCA and DCA are defined as part of the Defense Critical Infrastructure Program (DCIP) detailed in DoD Manual 3020.45, Volume 1.

A2.4. Risk Management Framework. The AF CE community shall adhere to the NIST ICS guidelines (NIST SP 800-82), DoD RMF guidance outlined in DoDI 8510.01, and subsequent AF RMF policy (AFI 17-101) to the greatest extent possible in order to sufficiently manage the life cycle cybersecurity risk of CS.

A2.4.1. RMF Roles and Responsibilities. The transition from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to RMF warrants changes in workflow, roles and responsibilities to accompany the shift from compliance-based accreditation to a risk-based approach to securing assets. To comply with RMF, the AF Chief, Information Dominance and Chief Information Officer (SAF/CIO A6) has appointed the Deputy Director of Civil Engineers (A4C-2) as the AO for CE ICS PIT. Upon appointment by the AF Chief Information Security Officer, the Air Force Civil Engineer Center (AFCEC) Operations Directorate Director will be the Security Control Assessor (SCA) for CE ICS PIT.

During the phase-in period to RMF, the role of Information System Security Manger (ISSM) will be temporarily assumed by AFCEC. The roles of the Information System Owner (ISO) and the Program Manager (PM) for CE CS will be performed, in the short- term, by the owning base's Deputy Base Civil Engineer (BCE). Funding for contract support to assume these roles and responsibilities is currently in the process of being approved through the FY18 budgeting process. The specific roles and responsibilities for performing continuous monitoring, as required by RMF, are forthcoming. See section A2.17 for further details regarding FY18 funding and the transition plan to meet CS cybersecurity protocol expectations.

A2.4.2. Preliminary Baseline Classification. For assistance with determining the Potential Impact Values for the RMF "Step 1 - Categorize System" process, please reference the *EI&E PIT Control System Master List* located on the RMF Knowledge Service portal. The list provides a baseline confidentiality – integrity – availability impact rating for various AF control systems. This baseline rating is considered the minimum impact value for a given system based on its mission criticality.

A2.5. Acquisitions. Because a CS is related to the facility being constructed and tailored to the mission it supports, acquisition and procurement of CS is currently a decentralized process in the AF. Until there is a centralized CS Program Management Office (PMO) able to adequately conduct CS lifecycle management, the CE community needs to collaborate with the Acquisitions community to accurately define security requirements and prioritize CS acquisitions with cybersecurity measures already incorporated into the design of the asset. Additionally, it is recommended to incorporate the best practices from the Department of Homeland Security (DHS)'s *Cyber Security Procurement Language for Control Systems* document into all future procurement and maintenance contracts.

A2.6. Segregated CS Network Environment. The AFCEC Operations Directorate's Civil Engineer Maintenance Inspection Repair Team (CEMIRT) Division will assist Base CE squadrons to establish an accredited CS enclave in order to segregate CS and CS traffic from the base area network (BAN). The enclave configuration will provide a defendable and monitored space protecting both the CS from network vulnerabilities and the network from CS vulnerabilities. CS should be operated either as stand-alone systems (no network connectivity), on an air-gapped network, or on a CS enclave. CS should not be directly connected to the Internet through either static or dial-up connections except as described in sections A2.9 and A2.16.

A2.7. Information Protection and Mission Assurance. A modified list of cybersecurity best practices to follow and frequently review is listed below. Additionally, the technical references listed in section A2.19 provide comprehensive procedures to follow for information protection and mission assurance.

A2.7.1. Apply security techniques such as encryption and/or cryptographic hashes to CS data storage and communications where determined appropriate.

A2.7.2. Frequent backups of CS data should be conducted, maintained, and properly stored. It is recommended to store copies of data and "golden image" configuration backups in a secure location for business continuity and disaster recovery.

A2.7.3. When a CS is no longer required, the ISO should take appropriate action to ensure the system and its data is properly disposed IAW established procedures detailed in NIST SP 800-53r4 and NIST SP 800-82r2.

A2.7.4. Ensure response plans (Incident Response/Business Continuity) and recovery plans (Incident Recovery/Disaster Recovery) are in place and managed IAW NIST SP 800-82.

A2.7.4.1. Response and recovery plans should contain specific tactics, techniques, and procedures (TTP) for when adversarial activity is detected. Such a plan may include disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100 percent password reset. The plan may also define escalation triggers and actions, including incident response, investigation, and public affairs activities.

See *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures for Department of Defense Industrial Control Systems* for examples of applicable TTPs to be considered for use or tailoring to base-specific conditions.

A2.7.4.2. Response and recovery plans should frequently be tested and reviewed. Personnel should be aware of their roles and responsibilities in case of an incident.

A2.7.4.3. Have a restoration plan in place, including having "gold disks" ready to restore systems to known good states.

A2.8. Access Control.

A2.8.1. Abide by strict access control protocols to prevent unauthorized physical access to all components of the CS (focusing on control nodes) and the unauthorized introduction of new hardware, infrastructure, and communications interfaces where feasible.

A2.8.2. Adhere to strict access control protocols for logical access to systems – limit to authorized users on an as-needed basis with permissions pertinent to the users' role.

A2.8.3. Enforce separate authentication mechanisms and credentials for users of the CS network and the BAN (i.e., CS network accounts do not use BAN user accounts).

A2.9. Connectivity. All non-BAN connectivity to CS (including, but not limited to, dial-up, Internet, Bluetooth, wireless, and cellular) are considered external connections. These connections bring substantial vulnerabilities warranting additional scrutiny and cybersecurity safeguards.

A2.9.1. Any data transmitted by commercial wireless devices, services, and technologies will implement end-to-end data encryption over an assured channel (AC). The security level of data encryption shall be dictated by the sensitivity of the data and validated under the "Cryptographic Module Validation Program," specified in FIPS PUB 140-2. Per DoDD 8100.02, individual exceptions to unclassified wireless encryption may be granted on a case-by-case basis after an operational risk assessment is conducted and approval is granted by the AO.

A2.9.2. CS with dial-up modem connections to the Defense Switched Network (DSN), such as direct subscriber lines (DSL), require AF Enterprise AO approval and ATC prior to use. The DSN is a primary information transfer network for the Defense Information Systems Network (DISN) and provides the worldwide non-secure voice, secure voice, data, facsimile, and video teleconferencing services for the DoD and other Federal agencies. All dial-up modem requests shall be submitted through *eMASS* for CE's ICS PIT AO and the AF Enterprise AO approval. Until approved, all dial-up modem connections are immediately prohibited.

A2.9.3. A DoD Chief Information Officer (CIO) waiver is required before procuring any of the following commercial services: Internet Service Provider (ISP), networking, system hosting, satellite and cloud computing. The DoD CIO grants DoD Information Network (DODIN) (formally Global Information Grid (GIG)) waivers to use non-DISN commercial IT services when in the best interest of DoD and when Defense Information Systems Agency (DISA) services cannot support mission requirements. Requests are evaluated from a Joint Information Enterprise (JIE) perspective for efforts such as cybersecurity, information sharing, budgeting, interoperability and mission scope.

A2.9.4. Use of a commercial ISP is not authorized unless a DODIN waiver has been approved for this service. Immediately cease all unapproved commercial ISP connections. Seek a DODIN waiver from the DoD CIO. Neither the Installation Commander, Mission Support Group Commander, nor CE's ICS PIT AO have the authority to approve commercial ISP connections. Unauthorized Commercial ISP connections result in a Denial of Authorization to Operate (DATO).

A2.9.4.1. Visit the DISA website for the DODIN Waiver Process.

A2.10. Solid State Devices and Removable Media. As recommended by NIST SP 800-82, no removable media is to be connected to a CS or CS enclave other than as described in section A2.15.4. Provisions should be made to prohibit the connection of unauthorized items, including vendor-owned devices. Make any necessary adjustments to the Service Level Support Agreement or service contract with the system maintainer or vendor.

A2.10.1. In the instance Solid State Hard Drives, Thumb Drives, Dongles, DVDs, CDs, and other removable media and storage devices are connected to a CS or CS enclave, ensure compliance with requirements outlined in USCYBERCOM CTO 10-084 and AF Network Operations Center NETOPS Tasking Order 2008-323-001.

A2.11. Switches. The use of switches within the CS should be kept to a minimum and should use managed switches to restrict port access to the CS. These devices have Security Technical Implementation Guides applicable to them, and their configurations will be assessed during the RMF lifecycle. The use of hubs is not permitted. In instances where replacing unmanaged switches becomes an enormous cost and labor burden, the best practice is to replace unmanaged switches with managed switches at the end of the asset's life cycle, however operating unmanaged switches will be taken into account by the SCA and AO.

All switches should have physical security measures. Ensure switches are stored in a locked, secure area/cabinet, and add necessary tamper-proof features to restrict access to these devices.

A2.12. Handheld Personal Devices. The use of a Personal Data Assistant (PDA) to access, monitor or control CE-owned CS is not authorized. The discovery of such a connection can result in issuance of a DATO and thus disconnection from the AF Information Network (AFIN).

A2.13. Device Security.

A2.13.1. Operating Systems. NIST SP 800-82 notes that CS operating systems and control networks are often quite different from their IT counterparts, requiring different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers, not IT personnel. Assumptions that differences are not significant can have disastrous consequences on system operations.

A2.13.1.1. To the greatest extent practicable given acceptable levels of risk and final approval by the Lifecycle System Owners, AF CS' operating systems should be upgraded and maintained to the most current operating system and patch levels approved by the Air Force for the workstation baseline.

A2.13.1.2. In instances when the CS operating system cannot be upgraded for technical or operational reasons, the risk, mitigating actions, and a Plan of Actions and Milestones must be documented and approved through the RMF process by the appropriate approval roles.

A2.13.2. Anti-Virus. Use security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware on CS.

A2.13.2.1. Antivirus tools only function effectively when installed, configured, run full-time, and are maintained properly against the state of known attack methods and payloads. However, while antivirus tools are common security practice in IT computer systems, their use with CS may require adopting special practices including compatibility checks, change management issues, and performance impact metrics.

These special practices should be utilized whenever new signatures or new versions of anti-virus software are installed.

A2.13.2.2. Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general purpose SCADA and backup servers generally can be secured just like enterprise IT equipment: install push- or auto- updated antivirus and patch management software with updates distributed via an antivirus server and patch management server located inside the CS network and auto-updated from the BAN.

A2.13.2.3. Follow vendor recommendations on all other servers and computers (DCS, PLC, instruments) that have time-dependent code, modified or extended operating systems or any other change that makes it different from a standard device. Expect the vendor to make periodic maintenance releases that include security patches.

A2.13.3. Ports / Services. Because the specific function of dedicated CS devices should be determined and documented, it is relatively easy to identify those ports and input/output devices that are unnecessary.

A2.13.3.1. Disable all unused ports and services on CS devices after testing to ensure this will not impact the CS operation.

A2.13.3.2. Ensure that unused ports and services remain disabled.

A2.13.3.3. Uninstall any programs, applications and services not strictly necessary for operation of the control system.

A2.14. Configuration / Patch Management. An essential aspect of life cycle cybersecurity management is patch management to mitigate known vulnerabilities of CE-owned CS.

A2.14.1. Appropriate configuration change processes and procedures should be instituted and followed to ensure any changes to the baseline configuration are approved and coordinated with the ISO and Mission Owner (MO). The ISO should track any system modifications and document them in the installation's CS inventory IAW NIST SP 800-53.

A2.14.2. Ideally, in order to evaluate the operational impact of installation new software prior to being applied to an operational environment, system patches and upgrades should first be assessed in a testing environment, on a backup/redundant system, or on an offline system. Then, the operational risk to the availability of the system should be weighed against the unpatched security risk to the system by the appropriate approval authority for the system or subsystem.

A2.14.3. While recognizing that an enterprise-wide CS cyber test range does not exist yet, it is recommended to work with the system vendor or manufacturer through hardware and software maintenance agreements to provide operational testing and evaluation. Bases are not expected to procure separate testbed environments for every CS.

A2.14.4. Systems should be patched or updated only with digitally-signed or hashed software from trusted authoritative sources.

A2.14.5. Procedures for on-site maintenance and patches for CS are outlined in sections A2.15.4 and A2.15.5.

A2.14.6. For further guidance on patch management, refer to *NSA Guidelines for Configuration / Patch Management in Industrial Control Systems*.

A2.15. On-site Maintenance. System maintenance practices to be followed are listed below. Further details of these practices can be found in NIST SP 800-82.

A2.15.1. To the greatest extent possible, maintenance and support should be performed on- site only (not remotely).

A2.15.2. Plan for or enforce having (if a plan exists) only government-owned computers connect to CS and CS enclaves (for maintenance or other authorized uses).

A2.15.3. Government-owned maintenance assets will be maintained by CE and must remain in government control. These maintenance assets must adhere to the following restrictions:

A2.15.3.1. Maintain the cybersecurity practices and procedures also required for NIPRNet machines.

A2.15.3.2. Uninstall any programs, applications, and services not strictly necessary.

A2.15.3.3. Disable any Wi-Fi, cameras, or microphones, preferably at the hardware or physical level.

A2.15.3.4. As stated in NIST SP 800-46 procedures, when existing contracts do not allow for maintenance using government-owned assets, ensure assets used by vendors and service personnel are thoroughly scanned for viruses and malware and have anti- virus software enabled before the asset is allowed to connect to a CS enclave or related infrastructure.

A2.15.3.5. For future CS maintenance-related contracts, incorporate contracting language ensuring the use of government-owned assets for CS maintenance.

Suggested CS contracting language is detailed in DHS's *Cyber Security Procurement Language for Control Systems*.

A2.15.4. CS that support Tier 1 TCAs should be on air-gapped networks and not directly connected to either a CS enclave, the NIPRNet, or the Internet. On-site maintenance and patches for DCI-supporting CS will be accomplished using the following procedures:

A2.15.4.1. Download digitally-signed or hashed software from trusted authoritative sources to a CD/DVD.

A2.15.4.2. Scan the CD/DVD on a computer having classified scanning signatures to ensure it is malware-free.

A2.15.4.3. Insert the CD/DVD into a government-owned maintenance computer (per section A2.15.3) to connect to the stand-alone system or air-gapped CS network.

A2.15.4.4. After patching or upgrading the system, destroy the CD/DVD media to ensure it cannot be used in another device.

A2.15.5. CS that do not support DCI, whether stand-alone or connected to a CS enclave, can be maintained according to defined base maintenance, configuration, and patch management processes.

A2.15.6. Ensure CS maintenance and repair is performed and logged in a timely manner with approved tools IAW this AFGM and existing policy.

A2.16. Remote Maintenance. When on-site maintenance and support (per section A2.15) absolutely cannot be accommodated for existing contractual or cost-effective reasons, remote maintenance access to CS is allowed as an option of last resort only for CS not supporting DCI. If remote access is employed, bases must adhere to the following recommendations and restrictions:

A2.16.1. Follow security measures recommended in NIST SP 800-46, NIST SP 800-82, and DHS/CPNI's *Configuring and Managing Remote Access for Industrial Control Systems* such as requiring encryption and token-based, multi-factor authentication.

A2.16.2. Remote access to the CS or CS enclave should be of limited duration – allowed only for the time necessary to accomplish the established maintenance task. The allotted time, initial time of access, and reason for access should be coordinated between the base and vendor in order for remote access to be enabled and monitored.

A2.16.3. Any remote access to the CS or CS enclave outside of the pre-arranged window should be blocked by disabling the modem or by other technical means.

A2.16.4. All remote access events should be logged and monitored. Access and events should be reviewed on a regular schedule. Additionally, the legitimacy and necessity of access should be verified.

A2.16.5. Remote access to CS is to be phased out. On-site maintenance requirements, cybersecurity procedures and Service Level Support Agreements are to be written into new, renewed or updated maintenance and support contracts.

A2.16.6. Other remote access to the CS or CS enclave not meeting these specifications is prohibited.

A2.16.7. Remote access to CS supporting DCI is prohibited.

A2.17. Transition Plan. Funding for contract support to assume these roles and responsibilities is currently in the process of being approved through the FY18 budgeting process.

A2.17.1. To alleviate the burden and to support compliance with these RMF and cybersecurity requirements, funding for contract support is in the approval process for FY18 to provide CE CS cybersecurity expertise at the base level in a prioritized manner. These full-time cybersecurity professionals will be dedicated to managing the CS cybersecurity efforts for the CE functional community, including conducting and maintaining accurate inventories, conducting mission support analysis, managing and configuring the type-accredited CS enclaves, conducting self-assessments of security controls and performing cybersecurity maintenance and lifecycle management of CE-owned CS.

A2.17.2. Inventories and the full implementation of cybersecurity controls on critical infrastructure-related CS need to be completed and in place by the end of FY19. Until bases receive dedicated manpower, bases are expected to plan for and comply with the remainder of guidance contained in this AFGM to the greatest extent possible given availability of resources and expertise.

A2.17.3. At this time, the exact roles and responsibilities for a Cybersecurity Defense Service Provider (CDSP) to provide defensive cyber operations and continuous monitoring for CE-owned CS and CS enclaves have not yet been determined.

A2.17.4. Further training material and templates are forthcoming to assist in base execution of this AFGM's requirements.

A2.18. Technical Support. For specific CS-related technical support and guidance, AFCEC's CEMIRT Division supports the accreditation of CE CS and guidance for implementing the enclave for CE-owned CS. CEMIRT can be reached by phone at DSN 523-6989/6929 or by e- mail at afcec.comi.icshelpdesk@us.af.mil, afcec.comi.ics@us.af.mil.

A2.19. Technical References. For specific technical guidance on the policies outlined above and on additional CE CS security controls, consult the following references which detail procedures on cybersecurity best practices and on system classification for tailoring security controls.

A2.19.1. NIST SP 800-82 A2.19.2.

NIST SP 800-53

A2.19.3. NIST Framework for Industrial Control System Cybersecurity

A2.19.4. NSA Information Assurance Directorate Guidance for Industrial Control Systems

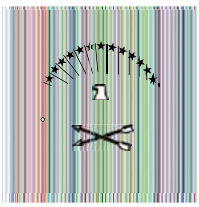
A2.19.5. *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures for Department of Defense Industrial Control Systems*

A2.19.6. Federal Information Processing Standards Publications (FIPS PUBS)

A2.19.7. CNSSI No. 1253, *Security Control Overlays for Industrial Control Systems*

A2.19.8. DHS ICS-CERT Standards and References

A2.19.9. Air Force Control Systems Community



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE CIVIL ENGINEER SUPPORT AGENCY

30 MAR 2011

FROM: HQ AFCESA/CEO
139 Barnes Drive Suite 1 Tyndall AFB
FL 32403-5319

SUBJECT: Engineering Technical Letter (ETL) 11-1: Civil Engineer Industrial Control System Information Assurance Compliance

1. **Purpose.** This ETL provides technical guidance and criteria for information assurance (IA) of civil engineering (CE) industrial control systems (ICS). This ETL applies to all ICSs that utilize any means of connectivity to monitor and control industrial processes, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC), which are often found in industrial equipment and critical infrastructures.

Note: The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this ETL does not imply endorsement by the Air Force.

2. **Application.** This ETL supersedes ETL 09-11, *Civil Engineering Industrial Control System Information Assurance Compliance*, dated October 26, 2009. Requirements in this ETL are mandatory. The interpreting authority for this ETL is the Air Force Civil Engineer Support Agency, Operations and Programs Support Division, Engineer Support Branch (HQ AFCESA/CEOA).

2.1. Authority: Air Force instruction (AFI) 32-1063, *Electric Power Systems*.

2.2. Effective Date: Immediately.

2.3. Intended Users:
- Major command (MAJCOM) engineers
- Base civil engineers (BCE)
- ICS information assurance managers (IAM)

2.4. Coordination:
- MAJCOM engineers responsible for CE ICSs
- The Air Force Civil Engineer, Resources Division, Information Technology Branch (HQ AF/A7CRT)
- Air Force Network Integration Center, Information Assurance Directorate (AFNIC/EV) and Air Force certifying authority (CA)
- Chief, Cyberspace Surety Division (SAF/A6OI), on behalf of Director, Cyberspace Operations (SAF/A6O) and Air Force senior information assurance officer (SIAO)

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

3. Referenced Publications.

3.1. Air Force (departmental publications available at http://www.e-publishing.af.mil/):

- Air Force policy directive (AFPD) 16-14, *Information Protection*
- AFI 31-401, *Information Security Program Management*
- AFI 31-501, *Personnel Security Program Management*
- AFI 32-1063, *Electric Power Systems*
- AFI 33-112, *Information Technology Hardware Asset Management*
- AFI 33-114, *Software Management*
- AFI 33-115V1, *Network Operations (NETOPS)*
- AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*
- AFI 33-200, *Information Assurance (IA) Management*
- AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*
- AFI 33-230, *Information Assurance Assessment and Assistance Program*
- AFNIC EV 2010-08, *Guide for Submission of Platform Information Technology (PIT) Determination Concurrence Requests*, 18 August 2010
- *Information Technology Investment Policy Guidance Memorandum*, 9 June 2008, HQ USAF/A7C

3.2. United States Code (U.S.C.):

- Title 40 U.S.C. 1401(3), The Clinger-Cohen Act of 1996

3.3. Code of Federal Regulations (CFR):

- Title 47, CFR, Part 15, *Radio Frequency Devices*, http://www.gpo.gov/

3.4. Department of Defense (DOD):

- DOD 8570.01-M, *Information Assurance Workforce Improvement Program*, incorporating Change 2, 20 April 2010, http://www.dtic.mil/whs/
- DOD Directive (DODD) 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf
- DODD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)*, 14 April 2004, http://www.dtic.mil/whs/directives/corres/dir.html
- DODD 8500.01E, *Information Assurance (IA)*, 24 October 2002, http://www.dtic.mil/whs/directives/corres/dir.html
- DOD Instruction (DODI) 5000.02, *Operation of the Defense Acquisition System*, 8 December 2008, http://www.dtic.mil/whs/directives/
- DODI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003, http://www.dtic.mil/whs/directives/corres/ins1.html
- DODI 8510.01, *DOD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007 http://www.dtic.mil/whs/directives/corres/ins1.html

3.5. National Institute of Standards and Technology (NIST):

- Federal Information Processing Standards Publication (FIPS PUB) 140-2, *Security Requirements for Cryptographic Modules*, 25 May 2001, http://csrc.nist.gov/
- FIPS PUB 197, *Advanced Encryption Standard (AES)*, 26 November 2001 http://csrc.nist.gov/
- NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, August 2009, http://csrc.nist.gov/publications/nistpubs/
- NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, Final Public Draft, September 2008, http://csrc.nist.gov/publications/drafts/
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Revision 1, February 2006, http://csrc.nist.gov/publications/nistpubs/

3.6. Other Government References:

- Committee on National Security Systems Instruction (CNSSI) No. 4012, *National Information Assurance Training Standard for Senior System Managers*, June 2004, Committee on National Security Systems, http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf
- Federal Information Security Management Act (FISMA) of 2002, Section 301: Information Security, http://iase.disa.mil/fisma/index.html
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4015, *National Training Standard for System Certifiers*, December 2000, Committee on National Security Systems, http://www.cnss.gov/Assets/pdf/nstissi_4015.pdf
- Office of Management and Budget (OMB) Circular A-76, *Performance of Commercial Activities*, 29 May 2003, http://www.whitehouse.gov/
- OMB Circular A-130, *Management of Federal Information Resources*, 28 November 2000, http://www.whitehouse.gov/
- National Telecommunications and Information Administration, *Manual of Regulations and Procedures for Federal Radio Frequency Management*, September 2010 Revision of the 2008 Edition, http://www.ntia.doc.gov/

4. Acronyms and Terms. See Attachment 2.

5. Background.

5.1. ICS Overview.

5.1.1. Industrial control system (ICS) is a general term for several types of control systems, including SCADA systems, DCSs, and other control system configurations such as skid-mounted or panel-mounted PLCs often found in the industrial sector and critical infrastructure. ICSs are typically used in infrastructure/utility/industrial systems such as electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper,

food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods).

5.1.1.1. SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square miles, where centralized data acquisition and control are critical to system operation. SCADA systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.

5.1.1.2. DCSs are used to control industrial processes such as electrical power generation, oil refineries, water/wastewater treatment, and manufacturing production. DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple integrated subsystems responsible for controlling the details of a localized process.

5.1.1.3. PLCs are computer-based, solid-state devices controlling almost all industrial equipment and processes. While PLCs are control system components used throughout DCS and SCADA systems, PLCs are often the primary components in smaller control system configurations used to provide operational control of separate processes.

5.1.2. For Air Force CE, real property ICSs include, but are not limited to, the following types of systems (including all points, devices, control panels, means of connectivity, software, controllers, computer workstations, servers, etc.):

- Supervisory control and data acquisition (SCADA) systems
  - Fuel distribution systems
  - Protective relays
  - Cathodic protection systems
  - Power generation systems, including renewable systems
  - Natural gas distribution systems
- Energy management and control systems (EMCS)
- Automated meter reading (AMR)/utility systems, including water metering systems
- Fire alarm/fire suppression/mass notification systems
- Utility monitoring and control (UMAC) systems
  - Electrical distribution systems
  - Generator monitoring systems
  - Water system controls
  - Natural gas distribution systems
- Airfield control systems
  - Lighting system controls
  - Aircraft arresting system (AAS) controls
- Traffic signal controls and vehicle barriers

- CE-maintained intrusion detection systems (IDS) (by CE/Security Forces memorandum of agreement only). **Note:** IDSs are not considered real property installed equipment.

5.1.3. Initially, many CE ICSs had little resemblance to traditional information technology (IT) systems in that ICSs were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICSs are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems, and network protocols, ICSs are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICSs from the outside world than predecessor systems, creating a greater need to secure these new systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

5.1.4. Many ICS characteristics differ from those of traditional IT systems, including different risks and priorities. Some of these ICS characteristics include significant risk to the health and safety of human lives and serious damage to the environment. ICSs have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT support personnel. Furthermore, the goals of safety and efficiency can sometimes conflict with security in the design and operation of control systems. For example, requiring password authentication and authorization should not hamper or interfere with emergency actions for the ICS. For additional information concerning the distinct differences between ICSs and typical IT systems, see NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, section 3.1.

5.2. Information Assurance (IA) of ICSs.

5.2.1. The Air Force Chief Information Officer (CIO) has issued policy guidance for the identification and IA of all legacy and future information systems (IS). For the CE community, these systems include the ICSs identified in paragraph 5.1.2 whether or not they are physically connected to the base local area network (LAN) or Air Force Global Information Grid (AF-GIG). ICSs that do **not** have a direct connection to the AF-GIG (see Attachment 2 for definition) are considered platform IT (PIT) systems. If a connection to the AF-GIG exists, that connection is considered a PIT interconnection (PITI).

5.2.2. Platform IT (PIT) Systems.

5.2.2.1. A PIT system is considered a special purpose system using computing resources (i.e., hardware, firmware, and [optionally] software) that are physically embedded in, dedicated to, or essential in real time to the mission performance of the system. A PIT system performs only (i.e., is dedicated to) the information processing assigned to the PIT system by its hosting special purpose system. Examples include, but are not limited to, SCADA-type systems, certain medical devices, training simulators, and diagnostic test and maintenance equipment.

Note: PIT point-to-point interconnections using an Air Force installation's backbone infrastructure for the purpose of connecting to remote sensors or to another PIT capability (within the same base/enclave) are not considered to be PITIs as long as they are logically or physically separated/isolated from the base common user infrastructure and systems (see AFNIC EV 2010-08, *Guide for Submission of Platform Information Technology (PIT) Determination Concurrence Requests*). See section 8.1.6 of this ETL for additional guidance on virtual local area networks (VLAN).

5.2.2.2. ICS PIT Certification and Accreditation (C&A). ICS PIT C&A is required for any new or existing ICS. ICS PIT C&A is not to be confused with the Air Force Certification and Accreditation Program (AFCAP) that utilizes the Defense Information Assurance Certification and Accreditation Process (DIACAP). The ICS PIT C&A process is illustrated in Attachment 1, with step-by-step instructions provided in section 7. New system acquisitions must incorporate security and IA requirements into the design specifications, and systems already in operation require IA controls as prescribed in current policy and guidance. PIT systems require IA risk assessment (RA) and periodic review as directed by the PIT designated accrediting authority (DAA).

5.2.3. Platform IT Interconnections (PITIs).

5.2.3.1. A PITI is the interface/connection between a PIT and the AF-GIG or any other DOD communications network. Examples of PITIs that require security considerations include, but are not limited to, PIT communications interfaces for data exchanges with the AF-GIG for mission planning or execution, remote administration, remote sensing, remote alerting (including one-way communication), and remote upgrade, query, or reconfiguration.

5.2.3.2. PITI C&A.

5.2.3.2.1. When a PIT system requires connection to the AF-GIG or any other DOD network to exchange information as part of the mission of the ICS, the IA requirements for the exchange must be explicitly addressed as part of the interconnection. These interconnections are subject to the AFCAP and

DIACAP as outlined in AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, and DODI 8510.01, *DOD Information Assurance Certification and Accreditation Process (DIACAP)*, respectively.

5.2.3.2.2. PITI C&A requires documenting any additional measures required by the AF-GIG to extend IA services or to protect the PIT from interconnection risk. The IA controls and level of robustness must be selected as applicable and shall consider the mission assurance category (MAC) and confidentiality level of both the PIT and its interconnecting means. IA controls provide a common management language for establishing IA needs, promoting consistency for testing and validating the implemented IA solutions, reducing complexity when managing changes to the validated baseline, providing a common pivot point when negotiating interconnections, and increasing accuracy for reporting IA readiness.

Note: IA controls listed in DODI 8500.2, *Information Assurance (IA) Implementation*, and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Appendix I ("Industrial Control Systems"), are designed to complement each other in addressing the uniqueness of PIT or PITI. When IA controls conflict, the MAC of the interconnected system will drive the security objectives of the PIT or PITI ICS.

Note: All IT is subject to IA policy, but PIT is excluded from the AFCAP; however, **PITIs** are specifically subject to the AFCAP, per AFI 33-210.

5.2.4. Figure 1 shows the applicability of IA policy for PIT systems and IA policy and the AFCAP for PITIs to the AF-GIG.

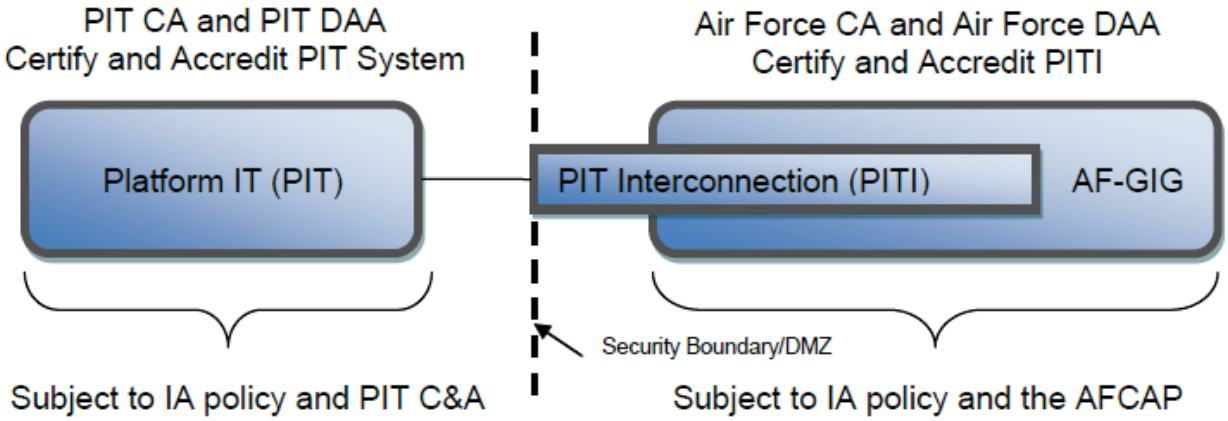


Figure 1. AFCAP Applicability (AFI 33-210)

6. Designated Personnel: General Roles, Responsibilities, and Qualifications.

6.1. Within CE are base-level ICS IAMs, MAJCOM ICS functional area managers (FAM), the ICS program manager (PM), the ICS PIT certifying authority (CA), the ICS portfolio manager (PfM), and the ICS PIT DAA. Their general roles, responsibilities, and qualifications are as follows:

6.1.1. Base-level ICS IAM. The BCE shall appoint, in writing, a primary and alternate ICS IAM for the civil engineer group (CEG) or civil engineer squadron (CES). The ICS IAMs are responsible for ensuring that base CE ICSs are certified and accredited in accordance with DOD and Air Force IA directives and instructions.

6.1.1.1. The primary ICS IAM must have Information Assurance Technical (IAT) Level II or Information Assurance Management (IAM) Level I certification in accordance with DOD 8570.01-M, *Information Assurance Workforce Improvement Program*, within six months of BCE appointment. (**Note:** Security+ certification satisfies either IAT Level II or IAM Level I certification.) If the CEG or CES has IT support personnel, it is recommended that the BCE assign an IT system administrator as the primary ICS IAM. Many Air Force CE IT specialists have IAT Level I or higher certification. In addition to the primary ICS IAM, an alternate ICS IAM must be appointed to assist the primary with the functional and technical aspects of ICSs. The alternate ICS IAM must be a qualified ICS operator/technician, and IAT/IAM certification is desired but not required. The alternate ICS IAM's primary role is to provide the necessary technical support/expertise to the primary ICS IAM to achieve ICS IA certification and accreditation. These two individuals will leverage each other's expertise to achieve IA of our ICSs.

6.1.1.2. The primary ICS IAM shall:

- Approve and manage all access privileges to ICS software and systems; validate all access privileges annually; and re-evaluate frequency requirements every three years or at any mission change, system change, or other significant change to operating requirements.
- Ensure appropriate access privileges for all individuals based on their training, qualification, and functional duties.
- Manage CE ICS access by ensuring that accounts are deactivated or activated in a controlled manner. Personnel designated to make configuration decisions and responsible for IA controls for both PIT and PITI shall be certified to IAT Level II or IAM Level I in accordance with DOD 8570.01-M.
- Have full administrative rights to install software updates/patches.
- Have access to review, modify, and edit the Enterprise Information Technology Data Repository (EITDR) entries as approved by the ICS FAM.

- Document and track system configurations for each CE-owned, -operated, and -maintained ICS throughout the system life cycle, including any Air Force CE ICSs operated and maintained by contractors. For each ICS, the ICS IAMs will assemble a PIT determination package in accordance with section 7.1.1 of this ETL and forward the package to the respective ICS FAM.
- Provide an annual report entitled "Industrial Control System Security Status Report" to the MAJCOM ICS FAM. The report will include a summary of current systems and system changes and will indicate compliance/non-compliance with IA security requirements. This report is due to the ICS FAM in October of each year.

6.1.1.3. The alternate ICS IAM shall:

- Document and track system configurations for each CE-owned, -operated, and -maintained ICS throughout the system life cycle, including any Air Force CE ICSs operated and maintained by contractors. For each ICS, the ICS IAMs will assemble a PIT determination package in accordance with section 7.1.1 of this ETL and forward the package to the respective ICS FAM.
- Provide an annual report entitled "Industrial Control System Security Status Report" to the MAJCOM ICS FAM. The report will include a summary of current systems and system changes and will indicate compliance/non-compliance with IA security requirements. This report is due to the ICS FAM in October of each year.

6.1.2. MAJCOM ICS FAM. The ICS FAM is designated in writing by the MAJCOM A7O (Operations) or equivalent. The ICS FAM is responsible for collecting the base-level PIT determination packages, reviewing them for completeness, and sending them to the ICS PM. In addition, the ICS FAM will submit an annual report entitled "Industrial Control System Security Status Report" to the ICS PfM. This report will contain a summary of current systems and system changes and will indicate compliance/non-compliance with IA security requirements. This report is due in November of each year. The ICS FAM may have access to create, modify, or delete EITDR entries as approved by the ICS PM or ICS PfM.

6.1.3. ICS PM. The ICS PM is designated in writing by HQ AFCESA/CEO. The ICS PM is responsible for ensuring appropriate scheduling of all IA aspects of the program to meet the ultimate goals of IA compliance. The ICS PM is also responsible to ensure that the following tasks are accomplished:

- Review and submit ICS PIT packages to Air Force CA for a PIT determination statement.
- Complete initial EITDR entries for CE ICS PITs.
- Provide updates to MAJCOM FAMs on the status of C&A activities of their respective systems.
- Establish a PIT integrated product team (IPT) of engineers, testers, etc.

- Coordinate and oversee execution of IA RAs.
- Ensure that all IA testing requirements are performed.

6.1.4. ICS PIT CA. The PIT CA is the technical authority for the IA aspects of a PIT system within their control. The PIT CA is responsible for ensuring clear definition of the IA requirements at the earliest stage possible. The PIT CA is then responsible for ensuring the implementation of the IA requirements to the extent possible based on program or system cost, schedule, and technical trade- offs. One of the primary functions of the PIT CA is to review the RA completed by the IPT. The ultimate goal of the RA is to mitigate or reduce remaining risks to an acceptable level. The PIT CA should agree with the RAs and help structure any mitigations for those risks not considered low. The PIT CA has the responsibility to advise the PIT DAA in making a final IA RA of the system. The PIT CA is designated in writing by the Air Force SIAO. The Air Force SIAO has designated HQ AFCESA/CEO as the ICS PIT CA.

6.1.4.1. The ICS PIT CA may have the following roles and responsibilities:

- Act as the focal point for the CE ICS IA compliance program and ETL.
- Coordinate CE ICS IA-related tasks with ICS PfM/ICS PIT DAA.
- Review and approve CE ICS IA strategy and implementation.
- Act as the technical authority for ICS-related IA issues.
- Certify the ICS IA design and implementation.
- Advise the ICS PIT DAA on IA-related issues.

6.1.4.2. Technical aspects of an ICS that may be reviewed include the following:

- ICS IA requirements
- Threat assessments
- Accreditation boundary/demilitarized zone (DMZ)
- Topology, block, and data flow diagrams
- Software, hardware, and firmware analysis
- Network connection compliance analysis
- Integrity analysis of integrated products
- Risk/vulnerability assessment results/findings
- Mitigation recommendations/techniques/shortfalls

6.1.4.3. Air Force SIAO-Directed Training, Certification, and Reporting Requirements:

- Maintain compliance with training and certification criteria outlined in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4015, *National Training Standard for System Certifiers*, and DOD 8570.01-M.

- Submit monthly reports to SAF/A6OI providing the status of all HQ AF/A7 CE ICS certified over the specified period at af.infoassurance@pentagon.af.mil.

6.1.5. ICS PfM. The ICS PfM has oversight responsibility for IT initiatives and systems for which they have lead funding responsibility. The ICS PfM is required to certify to the Air Force CIO annually, based on the ICS security status reports received from the ICS FAMs, that the provided IT portfolio management information is complete, accurate, and in accordance with current Air Force IT portfolio management direction as provided in budgetary documents (policy, annual planning and programming guidance, program objective memorandum preparation instructions, etc.). The ICS PM assists the ICS PfM by ensuring that all ICSs are registered in the EITDR. The ICS PfM resides at HQ AF/A7CRT and is responsible for CE portfolio management and annual reviews to maximize the value of IT investments and minimize the risk.

6.1.6. ICS PIT DAA. The PIT DAA is designated in writing by the Air Force CIO. The PIT DAA has a level of authority commensurate with accepting, in writing, the risk of operating all PIT systems under their jurisdiction. The PIT DAA must be independent of any particular program, but has the authority to influence programs from a global perspective. The PIT DAA consults with the PIT CA in making decisions but is not bound by the recommendation of the PIT CA. The PIT DAA takes into account the command's technical and programmatic needs in rendering a decision. The Air Force CIO has designated HQ AF/A7C-2 as the CE ICS PIT DAA. See Attachment 3.

6.1.6.1. ICS PIT DAA Responsibilities. The PIT DAA may have the following responsibilities:

- Ensure that IA requirements are identified and integrated into the systems engineering and acquisition processes as appropriate.
- Review/approve the accreditation decision package that includes an IA RA and mitigation approach.
- Accredit/deny systems for test or operation.
- Submit the system accreditation package to the Air Force DAA for network connection to the AF-GIG (if required) and acknowledge any PITIs in their accreditation decisions.

6.1.6.2. ICS PIT DAA Decisions. The PIT DAA may grant the following accreditation decisions to PIT ICSs under their purview:

1. Interim Authority to Test (IATT): Special case for authorizing testing in an operational environment or with live data for a specified time period. An IATT is for testing purposes only.
2. Interim Authority to Operate (IATO): A temporary authorization to operate under the conditions or constraints enumerated in the accreditation decision. An IATO is normally granted for up to

180 days. The DAA may not grant consecutive IATOs totaling more than 360 days.

3. Authority to Operate (ATO): Accreditation by the DAA for the system to operate without restriction. All IA risks are considered low or mitigations are in place, and the DAA agrees that any residual risk is acceptable under the circumstances. An ATO is required prior to initial operating capability (IOC). An ATO may be granted up to three years.
4. Denial of Authorization to Operate: A DAA decision that the information system cannot operate because of inadequate IA design, failure to adequately implement assigned IA requirements, or lack of adequate security.

6.1.6.3. Air Force CIO-Directed Training, Certification, and Reporting Requirements:

- Complete training and maintain appropriate IA certification in accordance with DOD 8570.01-M, Chapter 5, and Committee on National Security Systems Instruction (CNSSI) No. 4012, *National Information Assurance Training Standard for Senior System Managers*, prior to appointment. Proof of training (e.g., certificate) will be included as an artifact to the PIT accreditation decision package.
- Submit semi-annual reports to SAF/A6OI providing the status of all CE PIT ICSs accredited over the specified period at af.infoassurance@pentagon.af.mil.

7. CE ICS C&A Process. The C&A process for PIT systems, with or without interconnections, commences at issuance of this ETL. The C&A process is divided into three phases: Phase 1, ICS PIT Determination; Phase 2, ICS PIT C&A; and Phase 3, PITI AFCAP. Figure 2 summarizes the CE ICS C&A process flow chart provided in Attachment 1.

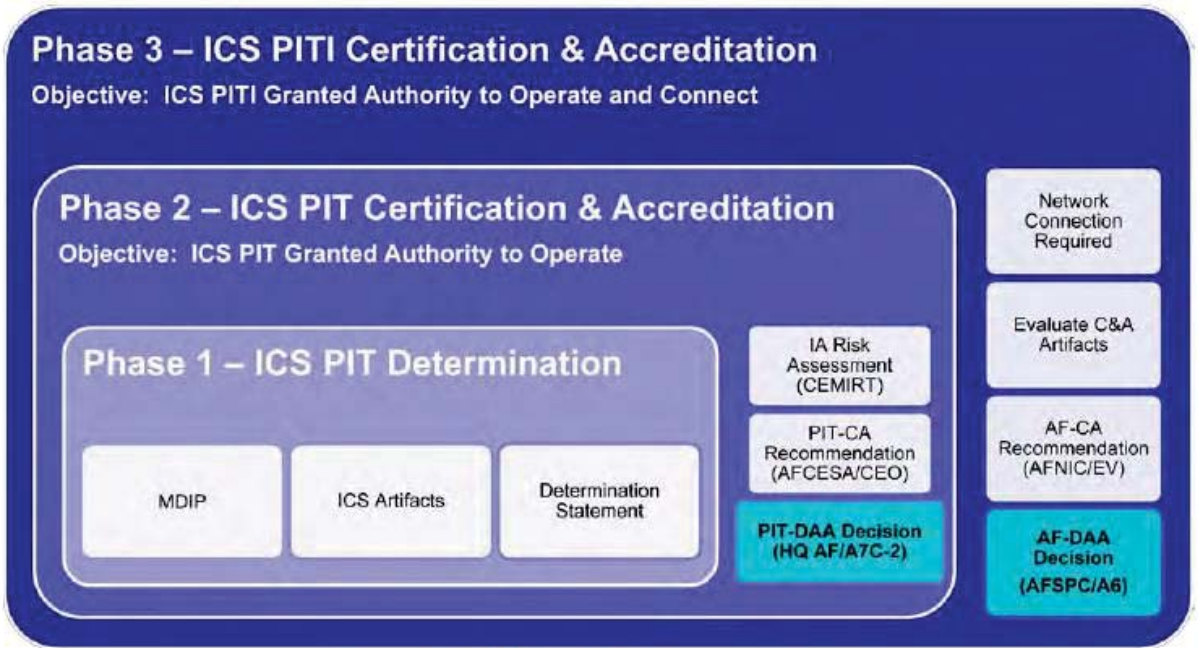


Figure 2. CE ICS C&A Process Overview

7.1. Phase 1: PIT Determination.

7.1.1. ICS IAMs shall document system configurations for each CE-owned, -operated and -maintained ICS, including any ICS operated and maintained by contractors. For each ICS, the ICS IAM will assemble a PIT determination package composed of the following information and forward that package to the respective ICS FAM.

7.1.1.1. Provide a single line block diagram of each type of ICS architecture. These diagrams should show the ICS network topology (i.e., its interconnections, data flow, components, and external connections).

- System connectivity
  - How the data flows
  - Where the data is coming in and out
  - Connection type(s) – wireless radio frequency (RF), Cat5, fiber, modem, etc.
  - Firewall location(s), if applicable
- System interconnectivity (i.e., other systems to which the ICS is connected, whether PIT, PITI, commercial Internet service provider, World Wide Web (WWW), GIG, LAN, etc.)
- Key components, including:
  - Make and model
  - IP address, if applicable
- Accreditation boundary (or boundaries), DMZ, or security boundary. The ICS security boundary shall be identified and well defined on all single line diagrams and network topologies for each ICS. The ICS

security boundary is the demarcation of connection to the AF-GIG or other DOD network.

- Firewalls, if applicable
  - Vendor, make, model, software version
- Cyber intrusion prevention/detection, if applicable
  - Vendor, make, model, software version
- IP addresses, if applicable. Do not use Xs. Network and ranges must be expressed correctly.

Note: The diagram must allow the Air Force CA to clearly understand and identify the hardware, software, and other IT components as well as the mission the platform supports.

7.1.1.2. Complete the Modified DIACAP Implementation Plan (MDIP) template for each ICS (see paragraph 5.1.2 for a list of common ICSs). Include any ICS architecture and installation specifications for each type of ICS architecture.

Note: ICS architecture and installation instructions are typically provided by the vendor and can be supported through vendor-specific literature, white papers, and/or configuration guides.

7.1.1.3. Complete the PIT determination checklist. This data is required by the ICS PM for input into the EITDR.

7.1.1.4. Describe the ICS in narrative form, and describe how, in real time, the ICS supports the operation and functionality of the special purpose system.

7.1.1.5. Submit the above information to the ICS FAM via a digitally signed and encrypted e-mail message.

7.1.2. ICS FAMs should submit the packages to the ICS PM via an encrypted and digitally signed e-mail message.

7.1.3. The ICS PM reviews the PIT(I) determination packages for completeness and submits them to the Air Force CA for a PIT(I) determination. The ICS PM will request in writing an Air Force CA evaluation to determine if the ICS is PIT(I). If the ICS requires the use of interconnections not connected to the AF-GIG, the ICS PM must state the justification for requesting exemption from the AFCAP, including rationale for the ICS as PIT.

7.1.4. The Air Force CA will evaluate the package and determine if the ICS is PIT. If the Air Force CA determines that the submission represents PIT, the PIT determination letter will indicate concurrence that the ICS meets the criteria for designation as PIT and is exempt from the formal AFCAP. Non-concurrence by the Air Force CA means the system is not a PIT system or the system has an

interconnection to the AF-GIG. The AFCAP will be required for those systems and interconnections in accordance with AFI 33-210.

7.1.5. The ICS PM shall receive the PIT(I) determination letter from the Air Force CA, review for changes to the original ICS architecture, recommend best security practices using, as a minimum, NIST SP 800-53, Appendix I, and provide additional instructions for Phase 2 of the CE ICS C&A process. The ICS PM will also provide system security and IA strategies.

7.1.5.1. If the ICS PM does not agree with the Air Force CA's PIT determination, the ICS PIT CA may appeal Air Force CA's determination to the Air Force SIAO for reconsideration. The Air Force SIAO's decision is final. If the ICS PM does not wish to appeal Air Force CA's determination, then the ICS PM will update the PIT package indicating PITI reclassification to the ICS PfM and to the ICS FAM.

7.1.5.2. The ICS PM will forward to the ICS FAM the Air Force CA PIT(I) determination statement, proposed security requirements, and IA controls required for each approved PIT(I) ICS. The ICS PM will enter the system into the EITDR with assistance from the ICS PfM.

7.1.6. Upon receipt of the PIT(I) determination statement, the ICS FAM will notify the respective ICS IAMs of the Air Force CA's determination and any required security actions. Transition to Phase 2 of the CE ICS C&A process is now authorized.

7.2. Phase 2: ICS PIT C&A.

7.2.1. The ICS PM will provide the ICS PIT CA with an overview of, and any changes to, the CE ICS C&A process. PIT CA approval of the RA strategy, templates, tools, and test team activation is required prior to scheduling and supporting site visits at active and reserve bases. The Civil Engineer Maintenance, Inspection, and Repair Team (CEMIRT) currently provides, among other areas of expertise, ICS technical support to the ICS PIT IPT. That support is expanding to include CEMIRT RA teams to help base ICS IAMs assess ICS threats, vulnerabilities, and risks. CEMIRT will also identify, implement, and/or recommend risk mitigation strategies, techniques, and/or solutions. The CEMIRT RA team will generate an IA RA and mitigation report within two weeks after the RA. CEMIRT will not coordinate and schedule site visits until all site-specific PIT determination statements are received from the Air Force CA, thus preventing multiple site visits.

7.2.2. The ICS PM goal will be to review and validate the IA RA and mitigation report and assemble the accreditation decision package (ADP) for the PIT CA within 30 calendar days of receipt.

7.2.3. The PIT CA will review the ADP and submit a recommendation to the PIT DAA for consideration.

7.2.4. The PIT DAA will issue an ATO once all compliance actions are certified by the PIT CA. An IATO may be issued at the PIT DAA's discretion prior to a formal ATO to reduce or eliminate known risks/vulnerabilities. If the PIT DAA issues an IATO or ATO, the ICS FAM and ICS IAM will be provided with a copy of the C&A approval, and the ICS IAM is responsible for continuously monitoring the approved PIT configuration as defined in the PIT package for security compliance of the ICS and for making EITDR updates as necessary or as prescribed by the ICS FAM. Changes in submitted topology or component configuration shall be staffed to the ICS PM for approval prior to implementation.

7.3. Phase 3: ICS PITI C&A.

7.3.1. If the PIT system has a previously identified interconnection to the AF-GIG, the formal AFCAP commences. The AFCAP will not begin until the PIT receives an IATO or ATO. The ICS PM will submit the entire package, with the proposed system design or legacy system interface description, along with the ICS PIT DAA signed ATO letter, to the Air Force CA.

7.3.2. Using the ICS system configuration submittals from the ICS FAM, the ICS PM and ICS PfM have the responsibility to work together and submit the package for C&A in accordance with AFI 33-210. If the ICS requires an on-site evaluation to validate IA controls, an IATT will be requested and submitted as part of the C&A package.

7.3.3. If the Air Force DAA/CA issues ATO and authority to connect (ATC) for the PITI, the ICS PM shall work with the ICS FAM and ICS IAM to implement any additional security actions to meet established AFCAP requirements (i.e., continuous monitoring and annual FISMA reporting requirements). The ICS IAM is responsible for maintaining accreditation and security for each ICS PITI. If the Air Force DAA and/or the Air Force CA disapproves interconnect, instructions/directions/rationale will be provided to the ICS PIT DAA and ICS PIT CA for corrective action.

8. Technical Requirements. This section outlines hardware and operational requirements for existing and new PIT ICSs and for existing PITI ICSs to operate while awaiting C&A and/or AFCAP approval.

8.1. Base-level ICS IAMs shall ensure that ICSs comply with the requirements in the following paragraphs. The MAJCOM ICS FAM is responsible for technical oversight of the requirements in this section of the ETL and shall consult with the HQ AFCESA ICS PM for clarification or interpretation of these requirements.

Note: ICSs on OCONUS military installations (outside the continental United States and its possessions [US&P]) or military installations not owned or operated by the DOD are installed and maintained under the rules and regulations of the host nation government. Personnel granted access to these systems shall comply with host nation and Air Force minimum training and experience requirements. Waivers to this policy require approval from the BCE, installation commander, MAJCOM CE, HQ AFCESA/CC, and the host nation governing body.

Note: For certification of supporting ICSs under host nation control and/or ownership, identify the ICS and forward technical information through the ICS FAM to the ICS PM for further guidance.

8.1.1. Because of inherent security risks, all commercial wireless networking devices are considered “external” connections to both PIT and PITI systems and warrant additional scrutiny before being implemented into the ICS architecture.

8.1.1.1. At a minimum, any data transmitted by commercial wireless devices, services, and technologies will implement data encryption from end to end over an assured channel (AC) (see clarification in Note below) and shall be validated under the Cryptographic Module Validation Program as meeting requirements, per Federal Information Processing Standards Publication (FIPS PUB) 140-2, *Security Requirements for Cryptographic Modules*, Overall Level 1 or Level 2, as dictated by the sensitivity of the data. Historically, ICS devices were not designed with encryption capabilities. In cases where commercial wireless must be employed but the ICS device(s) cannot provide FIPS PUB 140-2 encryption capabilities, the architecture must be carefully designed to provide an AC and additional defense-in-depth risk mitigation strategies to complement the IA controls to achieve an adequate level of security. The minimum acceptable cryptographic standard is the Advanced Encryption Standard (AES) using a cryptographic key length of 128 bits as outlined in FIPS PUB 197, *Advanced Encryption Standard (AES).*

Note: To clarify, an AC is a network communication link protected by a security protocol providing authentication, confidentiality, and data integrity, and employs US government-approved cryptographic technologies whenever cryptographic means are used. Examples of protocols and mechanisms sufficient to meet the requirements of authentication, confidentiality, and data integrity protection for an AC are Internet Protocol Security (IPSec); Secure Sockets Layer (SSL) v3; Transport Layer Security (TLS); and systems using National Security Agency (NSA) -approved high assurance guards with link encryption methodology.

Exception: Fire alarm reporting systems do not require data encryption for signaling to/from the fire alarm control panel (FACP). See paragraph 8.1.5.3 for requirements for sensitive compartmented information facilities (SCIF).

8.1.1.2. Substituting wireless for wired technology introduces numerous vulnerabilities into the network, which may be unacceptable or not cost-effective to mitigate. Convenience and/or minimal cost savings shall not be the sole justification for the use of wireless technologies.

8.1.1.3. Adding commercial wireless technologies to an existing approved network configuration boundary is considered a major configuration change and requires a review of security controls and the accreditation decision.

Note: Data hashing, regardless of the method, is not a form of encryption.

8.1.2. Telephone Modems.

8.1.2.1. PIT systems with modem connections to the Defense Switched Network (DSN) require PITI C&A (i.e., AFCAP) on those connections.

8.1.2.2. All telephone modems shall be a secure, dial-back (call-back) type. These exceptions apply:

- Dial-out modems for voice annunciation only are not required to be of the dial-back type.
- Conventional modems over DSN lines are permitted for control of AASs.

8.1.2.3. All telephone modems shall be configured to communicate with on-base or DSN numbers only.

8.1.2.4. Submit a request to the Network Operations and Security Center (NOSC) administrator to block all incoming commercial callers to specific modem control numbers that access ICSs and to block modem dial-out numbers from going off base.

8.1.2.5. The base-level ICS IAM shall provide these numbers to the voice protection system (VPS) personnel at the NOSC.

Note: If the PIT is connecting to one or more phone lines, the phone lines must be identified to the respective NOSC (East, West, Air National Guard). The voice protection team at the NOSC will assist in locking down the point of telephone service (POTS) line to further secure the PIT.

8.1.2.6. Establish audit procedures to record and archive modem usage, blocked calls, and rule violations. This audit record is an IA control and shall be accomplished annually or more often if situations dictate. These records shall be available for a minimum of six years.

8.1.3. ICS passwords shall be as follows:

8.1.3.1. Top-level access portions of the ICS, such as system host or client stations or computers, must comply with the following IA password safeguards.

8.1.3.1.1. Passwords shall not be factory default settings.

8.1.3.1.2. Passwords shall be at least 15 characters in length (for new system acquisitions) or the maximum supportable, using the following criteria:

- Do not use a password that has been used in the past.
- Use a minimum of two numbers, two special characters (e.g., $, %), two capital letters, and two lower-case letters. If special characters are not supported by the ICS, use the broadest combination of password features supported.
- Do not create a password that includes a phone number, home address, birth date, or personal specific dates.
- Do not use a word listed in a dictionary.
- Do not use simple or default passwords (e.g., 1234, data).

8.1.3.1.3. Passwords on all systems shall be changed every 90 days.

8.1.3.1.4. Password control shall incorporate a lock-out requirement.

8.1.3.2. Password-capable field devices (i.e., remote terminal units or field control devices) shall have their passwords changed from manufacturer defaults, and thereafter, as directed by the ICS IAM. The ICS IAM shall provide written certification to the MAJCOM ICS FAM that all password-capable field device passwords have been changed from manufacturer defaults. This certification shall be included as an artifact for final accreditation as PIT or PITI.

8.1.4. Radios used on any wireless ICS within the US&P that will transmit/receive within the Federal or military spectrum require frequency approval from base-level spectrum managers. A DD Form 1494, *Application for Equipment Frequency Allocation*, commonly referred to as the J-12 process, shall be approved before a spectrum allocation is issued. If the ICS uses an unlicensed frequency that complies with Federal Communications Commission (FCC) Part 15B (see Title 47 CFR, Part 15, *Radio Frequency Devices*), notify the base-level spectrum manager of the use of this unlicensed frequency. If a wireless solution is proposed for use outside the US&P, the MAJCOM ICS FAM shall contact the MAJCOM spectrum manager for host nation approval.

8.1.4.1. Develop contingency plans to manually control ICSs when RF interference disrupts monitoring or control.

Note: Non-licensed device operations must accept any interference from any Federal or non-Federal authorized radio station, other non-licensed devices, or industrial, scientific, and medical (ISM) equipment. The agency operating a non-licensed device that causes interference to an authorized radio station shall promptly take steps to eliminate the interference. Upon notification by the base spectrum manager that the device is causing interference, the operator of the non-licensed device shall cease all radiations from the device. Operations shall not resume until the condition causing the interference has been corrected.

Note: Non-licensed devices, since they operate on a non-interference basis, may not provide sufficient reliability for critical radio communications functions affecting human life or property; however, non-licensed devices may provide valuable and unique supplemental or expendable radio communications services where needed. To ensure adequate regulatory protection, Federal entities should rely only on devices with frequency assignments in the Federal or military spectrum and in the government master file as principal radio communication systems for safeguarding human life or property.

8.1.4.2. Any wireless transmission in the 2.4 gigahertz (GHz) unlicensed frequency range that is not a Combat Information Transport System Program Management Office (CITS PMO) -installed access point should be coordinated with the CITS lead command, AFNIC (afnic.ecnn@us.af.mil, (618) 229-5666), for possible interference.

8.1.5. Fire Alarm Reporting Systems.

8.1.5.1. Manually connect/disconnect remote system access (RSA) on all FACPs and/or servers (e.g., D-21) when RSA actions are needed/complete. Section 8.1.2 of this ETL identifies modem connection requirements.

8.1.5.2. Communications modems shall comply with section 8.1.2.

8.1.5.3. Fire alarm reporting from any SCIF to FACPs shall be wired (e.g., copper, fiber) systems, not wireless, and require an (air gap) isolation device if the available notification appliance device is a speaker. Fire alarm reporting signals sent from the SCIF FACP to the central monitoring station must be encrypted.

8.1.6. Virtual Local Area Networks (VLANs).

8.1.6.1. VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through the use of managed Ethernet switches. A managed switch provides all the features of an unmanaged switch, plus the ability to configure the switch to allow greater control over how the data

travels over the network and who has access to it. Each VLAN consists of a single broadcast domain that isolates traffic from other VLANs. Just as replacing hubs with switches reduces collisions, using VLANs limits the broadcast traffic, as well as allowing logical subnets to span multiple physical locations. There are two categories of VLANs:

- Static, often referred to as port-based, in which switch ports are assigned to a VLAN so that it is transparent to the end user.
- Dynamic, in which an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

8.1.6.2. Although more than one IP subnet may coexist on the same VLAN, the general recommendation is to use a one-to-one relationship between subnets and VLANs. This practice requires the use of a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can be used to route between multiple logical networks.

8.1.6.3. VLANs are not typically deployed to address host or network vulnerabilities in the way that firewalls or IDSs are deployed; however, when properly configured, VLANs do allow switches to enforce security policies and segregate traffic at the Ethernet layer. Properly segmented networks can also mitigate the risks of broadcast storms that may result from port scanning or worm activity.

8.1.6.4. Switches have been susceptible to attacks such as media access control (MaC) address spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. VLAN hopping, the ability for an attack to inject frames to unauthorized ports, has been demonstrated using switch spoofing and double tagging. These attacks cannot be conducted remotely and require local physical access to the switch. A variety of features such as MaC address filtering, port-based authentication using IEEE 802.1x, and specific vendor-recommended practices can be used to mitigate these attacks, depending on the device and implementation.

8.1.6.5. VLANs have been deployed effectively in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches. ICSs connected to a VLAN shall incorporate the following:

8.1.6.5.1. Firewalls separating base network traffic from external base traffic and the ICS VLAN. The configuration of the ICS VLAN must ensure that no ICS traffic exits the base firewall.

8.1.6.5.2. Hypertext Transfer Protocol Secure (HTTPS) for remote control of the ICS from the LAN. If Web services are provided to Nonsecure

Internet Protocol Router Network (NIPRNet) systems, implementation of an AC is required.

8.1.7. Replace any unmanaged switch with a managed switch. While awaiting replacement, add physical security measures, house unmanaged switches in a locked secure area, and/or add tamper-proof features. The ICS PM shall approve interim measures.

9. Additional Guidance.

9.1. Privatized ICSs.

9.1.1. For the purposes of this ETL, privatization is defined as the transfer of ownership and operations of Air Force utility systems and associated industrial monitoring/control systems to the private sector. The private sector includes all privately owned and publicly owned entities.

9.1.2. DOD and Air Force directives and instructions pertaining to IA and DIACAP requirements apply only to DOD-owned systems, including outsourced services such as operation and maintenance (O&M) by a private entity (e.g., Office of Management and Budget (OMB) Circular A-76, *Performance of Commercial Activities*, outsourced CE O&M or AF Form 9, *Request for Purchase*, service contract). A privatized utility is no longer a DOD-owned asset, including the privatized ICS that monitors and controls the privatized utility distribution system. Therefore, this formal real estate transaction relieves the US government from any and all planning, financing, designing, constructing, operating, and maintaining responsibilities of this utility infrastructure and associated monitoring and control system.

9.1.3. RF spectrum utilization by a privately owned or publicly owned entity while in garrison requires base or regional spectrum management notification and/or approval.

9.2. Outsourced O&M of ICSs. The following information applies to any OMB Circular A-76 outsourced CE O&M of ICSs, including AF Form 9 service contracts. DOD IA requirements apply to government-owned PIT and PITI ICSs that are operated and maintained by a private entity. Specific guidance for outsourced IT processes is located below and in section 6.9 of DODI 8510.01.

9.2.1. Outsourced IT-based processes that may also support non-DOD users or processes must still be certified and accredited by DOD entities. IA requirements for DOD information in an outsourced environment are determined by the information's MAC and classification or sensitivity and need to know, just as for other DOD ISs. However, the following also apply:

9.2.2. Technical security of the outsourced environment is the responsibility of the service provider.

9.2.3. Outsourced applications that are accessed by DOD users from DOD enclaves are subject to DOD enclave boundary defense IA controls for incoming traffic (e.g., ports and protocols and mobile code).

9.2.4. Responsibility for procedural and administrative security is shared between the service provider and the supported DOD entity contracting for the service.

9.2.5. The security responsibilities of the service provider down to the control level are made explicit in the contract, along with any other performance and service level parameters by which the DOD shall measure the IA profile of the outsourced IT-based process for the purpose of C&A.

9.2.6. Any baseline IA controls not explicit in the contract or otherwise covered by a service level agreement are categorized as NC. All such NC IA controls must be documented in an IT security plan of action and milestones (POA&M) that explains the acceptability of the risk of operating the outsourced IT-based process with the control in an NC status.

9.2.7. The security roles and responsibilities are to be made explicit in the acquisition, along with the performance and service level parameters by which the DOD shall measure the IA profile of the outsourced IT-based process. The PM for an outsourced IT-based process should carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied in the acquisition to protect DOD information in the service provider's operating environment and interconnected DOD ISs.

9.3. Type Accreditation. DODI 8510.01 defines type accreditation as "the official authorization to employ identical copies of a system in specified environments." This form of C&A allows a single DIACAP package to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. Automated information system (AIS) applications accreditations are type accreditations. Stand-alone IS and DMZ accreditations may also be type accreditations.

9.3.1. HQ AFCESA believes the majority of Air Force ICSs vary greatly in system hardware and software configurations, and consequently, a type accreditation is not warranted.

9.3.2. See AFI 33-210, section 3.14, for additional requirements regarding type accreditations.

9.4. Air Force Civil Engineer IT Investment Policy. In accordance with HQ USAF/A7C's *Information Technology Investment Policy Guidance Memorandum*, dated 9 June 2008, all IT investments with functionality supporting a

CE capability must be approved by the A7C IT governance structure prior to any development or sustainment activities or funds being committed or obligated. HQ AF/A7CRT, as the CE CIO, is the office of primary responsibility (OPR) for all CE IT investment processes, including IT portfolio management. The main purpose for the A7C IT governance structure is to analyze, control, select, and evaluate IT investments across the enterprise by standardizing capabilities, reducing duplication, and maximizing functionality across existing IT resources.

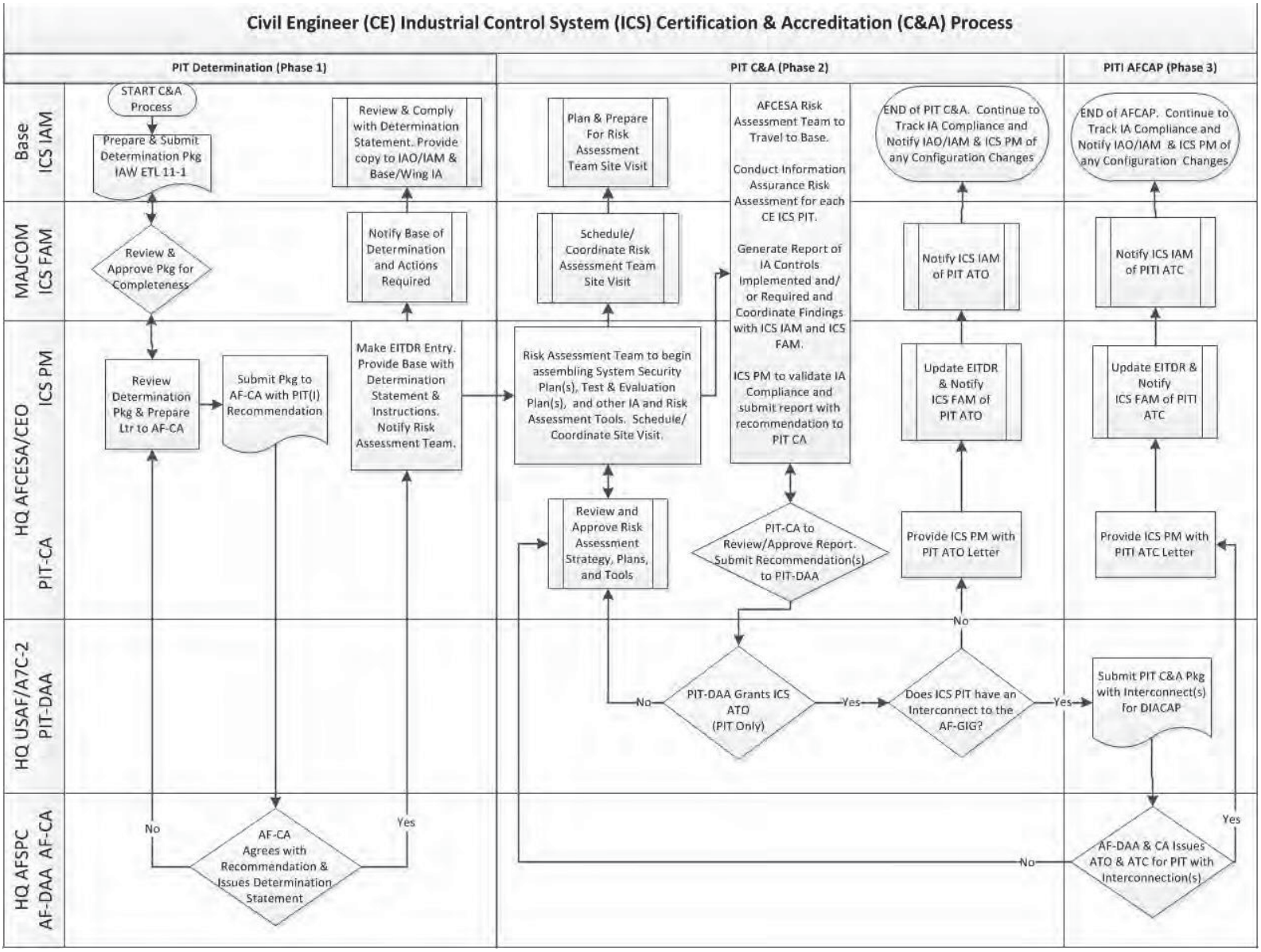
10. Points of Contact. The HQ AFCESA ICS PM has interpretive authority for the ICS IA and security issues contained in this ETL. The authority having jurisdiction over the content of this ETL is HQ AFCESA/CEOA.

10.1. HQ AFCESA ICS PM. To reach the ICS PM, e-mail AFCESAReachBackCenter@tyndall.af.mil, call DSN 523-6995 or commercial (850) 283-6995, or mail to 139 Barnes Drive, Suite 1, Tyndall AFB, FL 32403-5319. Subject line: ATTN HQ AFCESA ICS PM.

10.2. HQ AFCESA/CEOA. To reach HQ AFCESA/CEOA, e-mail AFCESAReachBackCenter@tyndall.af.mil or afcesa@aetc.af.smil.mil, call DSN 523-6995 or commercial (850) 283-6995, or mail to 139 Barnes Drive, Suite 1, Tyndall AFB, FL 32403-5319.

DAVID J. ANASON, Lt Col, USAF
Chief, Operations and Programs Support Division

4 Atchs
1. CE ICS C&A Process
2. Acronyms and Terms
3. CE ICS PIT DAA Appointment
4. Distribution List


Civil Engineer (CE) Industrial Control System (ICS) Certification & Accreditation (C&A) Process
PIT Determination (Phase 1)
PIT C&A (Phase 2)
PITI AFCAP (Phase 3)
Base ICS IAM
MAJCOM ICS FAM
HQ AFCESA/CEO ICS PM PIT-CA
HQ USAF/A7C-2 PIT-DAA
HQ AFSPC AF-DAA AF-CA
START C&A Process
Prepare & Submit Determination Pkg IAW ETL 11-1
Review & Approve Pkg for Completeness
Review Determination Pkg & Prepare Ltr to AF-CA
Submit Pkg to AF-CA with PIT(I) Recommendation
AF-CA Agrees with Recommendation & Issues Determination Statement
No
Yes
Make EITDR Entry. Provide Base with Determination Statement & Instructions. Notify Risk Assessment Team.
Notify Base of Determination and Actions Required
Review & Comply with Determination Statement. Provide copy to IAO/IAM & Base/Wing IA
Plan & Prepare For Risk Assessment Team Site Visit
Schedule/ Coordinate Risk Assessment Team Site Visit
Risk Assessment Team to begin assembling System Security Plan(s), Test & Evaluation Plan(s), and other IA and Risk Assessment Tools. Schedule/ Coordinate Site Visit.
Review and Approve Risk Assessment Strategy, Plans, and Tools
AFCESA Risk Assessment Team to Travel to Base.
Conduct Information Assurance Risk Assessment for each CE ICS PIT.
Generate Report of IA Controls Implemented and/ or Required and Coordinate Findings with ICS IAM and ICS FAM.
ICS PM to validate IA Compliance and submit report with recommendation to PIT CA
PIT-CA to Review/Approve Report. Submit Recommendation(s) to PIT-DAA
PIT-DAA Grants ICS ATO (PIT Only)
No
Yes
Does ICS PIT have an Interconnect to the AF-GIG?
No
Yes
Provide ICS PM with PIT ATO Letter
Update EITDR & Notify ICS FAM of PIT ATO
Notify ICS IAM of PIT ATO
END of PIT C&A. Continue to Track IA Compliance and Notify IAO/IAM & ICS PM of any Configuration Changes
Submit PIT C&A Pkg with Interconnect(s) for DIACAP
AF-DAA & CA Issues ATO & ATC for PIT with Interconnection(s)
No
Yes
Provide ICS PM with PITI ATC Letter
Update EITDR & Notify ICS FAM of PITI ATC
Notify ICS IAM of PITI ATC
END of AFCAP. Continue to Track IA Compliance and Notify IAO/IAM & ICS PM of any Configuration Changes

ACRONYMS AND TERMS

Acronyms

AAS	- aircraft arresting system
AC	- assured channel
ADP	- accreditation decision package
AES	- Advanced Encryption Standard
AF-CA	- Air Force certifying authority
AFCAP	- Air Force Certification and Accreditation Program
AF-DAA	- Air Force designated accrediting authority
AF-GIG	- Air Force Global Information Grid
AFI	- Air Force instruction
AFNIC	- Air Force Network Integration Center
AFNIC/EV	- Air Force Network Integration Center, Information Assurance Directorate
AFPD	- Air Force policy directive
AIS	- automated information system
AMR	- automated meter reading
ATC	- authority to connect
ATO	- authority to operate
BCE	- base civil engineer
CA	- certifying authority
C&A	- certification and accreditation
CA	- certifying authority
CCA	- Clinger-Cohen Act
CE	- civil engineering
CEG	- civil engineer group
CEMIRT	- Civil Engineer Maintenance, Inspection, and Repair Team
CES	- civil engineer squadron
CFR	- Code of Federal Regulations
CIO	- chief information officer
CITS PMO	- Combat Information Transport System Program Management Office
Config	- configuration
DAA	- designated accrediting authority
DCS	- distributed control system
DIACAP	- DOD Information Assurance Certification and Accreditation Process
DMZ	- demilitarized zone
DOD	- Department of Defense
DODD	- Department of Defense Directive
DODI	- Department of Defense Instruction
DSN	- Defense Switched Network
EITDR	- Enterprise Information Technology Data Repository
EMCS	- energy management and control system
ETL	- Engineering Technical Letter

FACP	- fire alarm control panel
FAM	- functional area manager
FCC	- Federal Communications Commission
FIPS PUB	- Federal Information Processing Standard Publication
FISMA	- Federal Information Security Management Act
GHz	- gigahertz
GIG	- Global Information Grid
HQ AF/A7C-2	- The Air Force Deputy Civil Engineer
HQ AF/A7CRT	- The Air Force Civil Engineer, Resources Division, Information Technology Branch
HQ AFCESA	- Air Force Civil Engineer Support Agency
HQ AFCESA/CC	- Air Force Civil Engineer Support Agency Commander
HQ AFCESA/CEO	- Air Force Civil Engineer Support Agency, Operations and Programs Support Division
HQ AFCESA/CEOA	- Air Force Civil Engineer Support Agency, Operations and Programs Support Division, Engineer Support Branch
HTTPS	- Hypertext Transfer Protocol Secure (combination of the Hypertext Transfer Protocol and a cryptographic protocol)
IA	- information assurance
IAM	- information assurance manager or management
IAO	- information assurance officer
IAS	- information assurance strategy
IAT	- information assurance technical
IATO	- interim authority to operate
IATT	- interim authority to test
IAW	- in accordance with
ICS	- industrial control system
IDS	- intrusion detection system
IOC	- initial operating capability
IP	- Internet Protocol
IPSec	- Internet Protocol Security
IPT	- integrated product team
IS	- information system
ISM	- industrial, scientific, and medical
IT	- information technology
LAN	- local area network
Ltr	- letter
MAC	- mission assurance category
MaC	- media access control
MAJCOM	- major command
MDIP	- Modified DIACAP Implementation Plan
NIPRNet	- Nonsecure Internet Protocol Router Network
NIST	- National Institute of Standards and Technology
NIST SP	- NIST Special Publication
NOSC	- Network Operations and Security Center
NSA	- National Security Agency
NSTISSI	- National Security Telecommunications and information Systems Security Instruction

OCONUS	- outside the continental United States
O&M	- operation and maintenance
OMB	- Office of Management and Budget
OPR	- office of primary responsibility
PfM	- portfolio manager
PIT	- platform information technology
PIT-CA	- platform information technology certifying authority
PIT-DAA	- platform information technology designated accrediting authority
PITI	- platform information technology interconnection
Pkg	- package
PLC	- programmable logic controller
PM	- program manager
POA&M	- plan of action and milestones
POC	- point of contact
POTS	- point of telephone service
RA	- risk assessment
Rep	- representative
RF	- radio frequency
RSA	- remote system access
SCADA	- supervisory control and data acquisition
SCIF	- sensitive compartmented information facility
SIAO	- senior information assurance officer
SSL	- Secure Sockets Layer
TLS	- Transport Layer Security
UMAC	- utility monitoring and control
US&P	- United States and its possessions
U.S.C.	- United States Code
VLAN	- virtual local area network
VPS	- voice protection system
WWW	- World Wide Web

Terms

Accreditation – A management decision by a senior agency official to authorize operation of a PIT-designated system based on the results of a certification analysis and other relevant considerations. The PIT DAA can grant system accreditation but cannot grant connection approval to the AF-GIG. Only the Air Force DAA may grant an ATC. The current Air Force DAA is AFSPC/A6.

Certification – A comprehensive analysis of the technical and non-technical aspects of an information system in its operational environment to determine compliance to stated security requirements and controls. The current Air Force CA is AFNIC.

Computing Environment – A computing environment has a server with multiple stations working from it. The stations can be standard computers, remote sensors, satellite feeds, etc.

Computer Network – The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as

LANs, or long-haul data transport capabilities, such as wide area and backbone networks.

Demilitarized Zone (DMZ) – A secure interface between systems or components of systems or a perimeter network that adds an extra layer of protection between internal and external networks by enforcing the internal network's IA policy for external information exchange. A DMZ, also called a "screened subnet," provides external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks.

Enclave – A collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security.

Global Information Grid (GIG) – The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG includes stand-alone, self contained, or embedded IT that is not, and will not be, connected to the enterprise network. (DODD 8000.01)

Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA Control – An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DOD information system to achieve and appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130. (DODI 8500.2)

Information System (IS) – A discrete set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (**Note:** Includes AIS applications, enclaves, outsourced IT-based processes, and PITIs.)

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes equipment used by the executive agency directly or used by a contractor under a contract with the executive agency, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware, and similar

procedures, services (including support services), and related resources. Notwithstanding the preceding, the term "information technology" does not include any equipment that is required by a Federal contractor incidental to a Federal contract.

Mobile Code – Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

Privileged User – An authorized user who has access to system control, monitoring, or administration functions.

Type Accreditation – DODI 8510.01 defines type accreditation as "the official authorization to employ identical copies of a system in specified environments." This form of C&A allows a single DIACAP package (i.e., System Identification Profile, DIACAP Implementation Plan, supporting documentation for certification, DIACAP Scorecard, and IT security POA&M [if required]) to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. AIS applications accreditations are type accreditations. Stand-alone IS and DMZ accreditations may also be type accreditations.

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

FEB 25 2011

MEMORANDUM FOR AF/A7C

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Appointment of Platform Information Technology (PIT) Designated Accrediting Authority (DAA)

1. In accordance with AF Policy Directive, *Information Assurance Program*, I hereby appoint the Air Force Deputy Civil Engineer (HQ USAF/A7C-2), the PIT DAA for all Civil Engineering Industrial Control systems (ICS) designated as PIT. AF/A7C has met the criteria, training, and certification requirements outlined in DoDI 8510.01E, *Information Assurance*, paragraph 4.25 and DoD 8570.1-M, *Information Assurance Workforce Improvement Program*, chapter 5. All Civil Engineering ICS categorized as PIT Interconnections (PITI) must obtain accreditation and connection approval from the Air Force Designated Accrediting Authority (AFSPC/A6) prior to connecting to the Air Force provisioned portion of the Global Information Grid (AF GIG).

2. The AF/A7C-2, as PIT DAA for Civil Engineering ICS, will maintain compliance with:

a. DoD approved DAA training either through the DISA Online DAA Training Course

b. Committee on National Security System Instruction 4012, *National Information Assurance Training Standard for Senior System Managers*

c. Statutory requirements (FISMA, Clinger Cohen Act, Federal Information Processing Standards, etc.), DoD and Air Force information assurance policies.

3. SAF/CIO A6 maintains authority to revoke this appointment based on lack of due diligence, non-compliance with aforementioned policies, and other security related infractions. AF/A7C will provide semi-annual reports to SAF/A6OI (af.infoassurance@pentagon.af.mil) providing status on all Civil Engineering PIT ICS accredited over the specified period. Direct any questions or comments to the SAF/CIO A6 point of contact, Ken Brodie, SAF/A6OI, DSN 425-1526, kenneth.brodie@pentagon.af.mil.

W.T. Lord

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

cc: AFSPC/CV/A6
AFNIC/EV

DISTRIBUTION LIST

SPECIAL INTEREST ORGANIZATIONS

Information Handling Services (1)
15 Inverness Way East
Englewood, CO 80150

Construction Criteria Database (1)
National Institute of Bldg Sciences
Washington, DC 20005