

1.0 Energy Security and Resilience

Each Federal Energy solution procurement is a specific solution tailored to the needs of a customer, requiring a specific level of Security (defined as the uninterrupted availability of energy sources at an affordable price) and Resilience (defined as the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents). The requirements of Energy Security and Resilience can be met by contractors who deliver energy solutions with capability in the following four “pillars” of success: (a) Cybersecurity, (b) Industrial Control Systems, (c) DoD Architectural Framework, and (d) Controlled Technical Information. Paragraphs 1.0 through 1.5 of this section should assist contractors to demonstrate within their proposals, how they will deliver capability in the four pillars of success.

1.1 Basic Design and Implementation Standards

Contractor shall meet or exceed all current, applicable codes and criteria of the following:

- 1.1.1 Installation Design Guide available at each individual location
- 1.1.2 American National Standards Institute (ANSI)
- 1.1.3 Department of the Army Regulation (AR) AR 385-40 Accident Reporting and Records
- 1.1.4 Department of the Army Corps of Engineers, Huntsville Division (CEHND) Manual
- 1.1.5 HNC-PR-ED-2000.10 Engineering Guidance Design Manual
- 1.1.6 National Electric Code (NEC)
- 1.1.7 National Electrical Safety Code (NESC)
- 1.1.8 National Fire Protection Association (NFPA) Standards including, but not limited to, NFPA 101- Life Safety Code
- 1.1.9 National Institute of Standards and Technology (NIST)
- 1.1.10 NIST 800-82, Guide to Industrial Control Systems (ICS) Security
- 1.1.11 National Electrical Manufacturers Association (NEMA)
- 1.1.12 Underwriters Laboratory (UL)
- 1.1.13 Institute of Electrical and Electronics Engineers (IEEE)
- 1.1.14 IEEE 1547 Standard for Interconnecting Distributed Resources with Electric Power Systems
- 1.1.15 International Building Code (IBC)
- 1.1.16 International Plumbing Code (IPC)
- 1.1.17 International Mechanical Code (IMC)
- 1.1.18 Unified Facilities Criteria (UFC) UFC 3-410-01FA Heating, Ventilating, and Air-Conditioning (HVAC)
- 1.1.19 UFC 3-470-01 Lonworks Utility Monitoring and Control System (UMCS)
- 1.1.20 UFC 3-530-01 Interior and Exterior Lighting Systems and Controls
- 1.1.21 UFC 4-010-01 DoD Minimum Antiterrorism Standards for Buildings
- 1.1.22 UFC 4-010-03 Security Engineering: Physical Security Measures for High-Risk Personnel (HRP)

- 1.1.23 UFC 4-010-06 Cybersecurity of Facility-Related Control Systems
- 1.1.24 American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE)
- 1.1.25 ASHRAE 62 Ventilation for Acceptable Indoor Air Quality
- 1.1.26 ASHRAE 90.1 Energy Standard for Buildings Except Low-Rise Residential Buildings
- 1.1.27 ASHRAE 189.1 Standard for the Design of High-Performance Green Buildings
- 1.1.28 ASHRAE 189.1 Section 10 Construction and Plans for Operation Subsection 3 Mandatory Provisions (Commissioning /Testing Subsections)
- 1.1.29 Occupational Safety and Health Administration (OSHA) regulations
- 1.1.30 Army Corps of Engineers Safety Manual
- 1.1.31 EM 385-1-1 Safety and Health Requirements
- 1.1.32 29 CFR 1904 Recording and Reporting Occupational Injuries and Illnesses
- 1.1.33 29 CFR 1910 Occupational Safety and Health Standards
- 1.1.34 29 CFR 1926 Safety and Health Regulations for Construction
- 1.1.35 National Historic Preservation Act, as applicable
- 1.1.36 Illuminating Engineering Society of North America (IESNA)
- 1.1.37 American Institute of Architects (AIA) Masterspec
- 1.1.38 Air-Conditioning and Refrigeration Institute (ARI)
- 1.1.39 UFGS 23 09 23 Direct Digital Control for HVAC and Other Local Building Systems
- 1.1.40 UFGS 23 09 23.13 20 BACnet Direct Digital Control Systems for HVAC
- 1.1.41 UFGS 25 10 10 UMCS Front End and Integration
- 1.1.42 UFGS Division 21 Fire Suppression as applicable for conservation measures implemented
- 1.1.43 Cyber Security based upon level of network interconnection of ECMs identified in Feasibility Study and Proposal coordinated with installation Information Assurance personnel

1.2 Information Technology (IT) Standards

- 1.2.1 Contractor shall meet or exceed all current, applicable codes and criteria of the following: and regulations, including but not limited to: Army Regulation (AR) 25-1 Army Information Technology
- 1.2.2 Army Regulation (AR) 25-2 Information Assurance
- 1.2.3 The Federal Information Security Management Act (FISMA)
- 1.2.4 National Security Telecommunications and Information Systems Security (NSTISSP) Policy No. 11 National Information Assurance Acquisition Policy
- 1.2.5 Federal Information Processing Standards
- 1.2.6 Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs)
- 1.2.7 DoD Directive 8500.1 Information Assurance (IA)
- 1.2.8 DoD Instruction 8500.2 IA Implementation

- 1.2.9 DoD Instruction 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) Note: Use latest guidance unless Agency-specific guidelines permit otherwise.
- 1.2.10 DoD Manual 8570.01-M Information Assurance Workforce Improvement Program
- 1.2.11 Air Force Engineering Technical Letter 11 (for Air Force Projects only)
- 1.2.12 Air Force Guidance Memo 2017-32-01 (for Air Force projects only)
- 1.2.13 UFC 4-010-06 Cyber Security for Facilities Related Control Systems
- 1.2.14 NIST 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security
 - 1.2.14.1 Contractor will provide ICS Supplemental Guidance. See Section 1.4 DoD Architectural Framework (DoDAF)

1.3 Operational Technology (OT) Standards

Contractor shall meet or exceed all current, applicable codes and criteria and regulations, including but not limited to of the following :

- 1.3.1 Army Directive 2017-07 Installation Energy and Water Security Policy
- 1.3.2 Defense Federal Acquisition Regulation 252.204.7012
- 1.3.3 Defense Federal Acquisition Regulation Supplement clause 252.227-7013,
- 1.3.4 Rights in Technical Data - Noncommercial Items (48 CFR 252.227-7013)
- 1.3.5 NIST SP 1800 Situational Awareness for Electric Utilities
- 1.3.6 NIST SP 1800-7a Executive Summary
- 1.3.7 NIST SP 1800-7b Approach, Architecture, and Security Characteristics for CIOs, CISOs, and Security Managers
- 1.3.8 NIST SP 1800-7c How-To Guides
- 1.3.9 IEC 61850 (Series) Communication Networks and Systems for Power Utility Automation
- 1.3.10 NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- 1.3.11 NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security
 - 1.3.9.1 Contractor will provide ICS Supplemental Guidance on the application of the security controls and control enhancements, and the environments in which these specialized systems operate. See Section 1.4 DoDAF)
- 1.3.12 NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- 1.3.13 NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- 1.3.14 IEC 62443 Industrial Network and System Security
- 1.3.15 IEEE 242 Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems
- 1.3.16 IEEE 37.1 SCADA and Automation Systems

The following documents enable the application of IEEE 37.1

- 1.3.16.1 EIA/ECA-310 Cabinets, Racks, Panels, and Associated Equipment

- 1.3.16.2 IEC 60529 Degrees of Protection Provided by Enclosures (IP Code)
- 1.3.16.3 IEC 60870-6 Telecontrol Equipment and Systems
- 1.3.16.4 IEC 61131-3 Programmable Controllers – Part 3: Programming Languages
- 1.3.16.5 IEC 654-3 Operating Conditions for Industrial Process Measurement and Control Equipment – Part III: Mechanical Influences
- 1.3.16.6 IEC 61850 (Series) Communication Networks and Systems for Power Utility Automation
- 1.3.16.7 IEEE 525 IEEE Guide for the Design and Installation of Cable Systems in Substations
- 1.3.16.8 IEEE 1379 IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation
- 1.3.16.9 IEEE 1588 IEEE Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- 1.3.16.10 IEEE 1590 IEEE Recommended Practice for the Electrical Protection of Communication Facilities Serving Electric Supply Locations Using Optical Fiber Systems
- 1.3.16.11 IEEE 1613 IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations
- 1.3.16.12 IEEE 1615 IEEE Recommended Practice for Network Communication in Electric Power Substations
- 1.3.16.13 IEEE 1646 IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation
- 1.3.16.14 ANSI S12.10 Acoustics - Measurement of Airborne Noise Emitted by Information Technology and Telecommunications Equipment
- 1.3.16.15 ANSI S1.4 Specification for Sound Level Meters

- 1.3.17 IEEE 1547 Standard for Interconnecting Distributed Resources with Electric Power Systems (Series)
 - 1.3.17.1 IEEE 1547.1 Standard Conformance Test Procedures for Equipment Interconnecting Distributed Resources with Electric Power Systems
 - 1.3.17.2 IEEE 1547.1a Standard Conformance Test Procedures for Equipment Interconnecting Distributed Resources with Electric Power Systems—Amendment 1
 - 1.3.17.3 IEEE 1547.2 IEEE Application Guide for IEEE 1547, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems

- 1.3.17.4 IEEE 1547.3 IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems
- 1.3.17.5 IEEE 1547.4 IEEE Guide for Design, Operation, and Integration of Distributed Resource Island Systems with Electric Power Systems
- 1.3.17.6 IEEE 1547.6 IEEE Recommended Practice for Interconnecting Distributed Resources with Electric Power Systems Distribution Secondary Networks
- 1.3.17.7 IEEE 1547.7 IEEE Guide for Conducting Distribution Impact Studies for Distributed Resource Interconnection

1.4 DoD Architectural Framework (DoDAF)

Contractor shall provide a DoDAF operational view with its intended control system(s) and network. DoDAF may serve as ICS Supplemental Guidance (per NIST SP 800-82) on the application of the security controls and control enhancements, and the environments in which these specialized systems operate. A contractor should deliver a DoDAF view as a conceptual document, at a minimum, with its initial Site Survey or Preliminary Assessment. The contractor shall provide a DoDAF operational view with its intended control system(s) and network, in its Feasibility Study or Investment Grade Audit, prior to an award. A DoDAF operational view template is available in both Visio and PDF upon request from the Project Manager or Contracting Officer.

1.5 Covered Defense Information (DFARS 252.204.7012)

The Contractor shall manage covered defense information to safeguard the security of the data and provide the data to the government allowing for current timely operations to monitor and manage the critical energy infrastructure. Critical energy infrastructure includes all systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters (<http://www.archives.gov/cui/registry/category-list.html>). The management of covered defense information also includes but is not limited to the following:

- 1.5.1 Contractor shall assist the receiving Government customer to maintain or improve the effectiveness of its current mission, by understanding and describing the impact(s) that its proposed energy solutions are likely to have on the mission.
- 1.5.2 Contractor shall establish a system that enables the support of field-based applications that enable scalable peer-to-peer publish/subscribe architecture using distributed logic as well as centralized logic.
- 1.5.3 The Contractor shall update and or modify the collection, management, and transmittal of covered defense information as required to maintain the security of the information from unauthorized access.
- 1.5.4 Contractor should assist the Government in meeting Executive Order 13693, Section 3(a)(i)(A), to utilize remote building energy performance assessment

auditing, in order to improve energy use diagnostics, monitor and measure energy demand, and reduce the cost of on-site audits.