

Environmental Security Technology Certification Program (ESTCP)

Installation Energy and Water Solicitation

INNOVATIVE APPROACHES TO OBTAINING AUTHORITY TO OPERATE FOR FACILITY-RELATED CONTROL SYSTEMS

OBJECTIVE

The DoD Installation Energy Test Bed seeks innovative approaches to obtaining Authority To Operate (ATO) for common current and future network-reliant facility energy control systems and devices. Demonstrations must satisfy the requirements established in the Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, and DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) and any applicable Service-specific requirements. DoD seeks solutions that result in Type Authorization¹ (TA) and Reciprocity² and/or can be easily replicated by installation personnel responsible for this activity.

Demonstration projects with the following characteristics are preferable:

- High likelihood of achieving reciprocity between Services
- High calculable energy savings, in addition to cost savings, as a direct result of the technology
- Minimal design and engineering required for deployment of the technology after the demonstration (e.g., development of pre-filled standard RMF TA submittal templates)
- Identification of common and mismatched security controls across different Platform Enclaves
- Development of cost factors and metrics to demonstrate scalability of the solution
- Low cost to implement after the demonstration
- Cost sharing

Project teams are encouraged to include representatives from each of the Services to ensure broad acceptance of demonstrated approaches and technologies. The demonstration program is for technologies and methods with completed proof-of-principle work. The impact of the demonstration should be to reduce the time and cost of gaining ATO for legacy and new facility energy control systems and devices and to validate the energy and cost savings achieved by allowing network connectivity of legacy systems.

¹ Type Authorization-An official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation.

² Reciprocity-Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. Can apply to both TA and non-TA systems.

BACKGROUND

Many currently-installed facility energy control systems and devices are not providing their full benefit (operational efficiency or energy and cost savings) to DoD due to restrictions on network connectivity stemming from cybersecurity concerns. Additionally, new facility energy and water technologies increasingly incorporate “smart” components and control systems that rely on network connectivity to send and receive data and control signals. For these technologies to operate as intended and be cost-effective, they must have access to DoD network with minimal additional installation, operation and maintenance costs. Currently, the process to gain ATO, a requirement for network connected systems and devices, can be cost-prohibitive and time consuming, which limits DoD’s ability to benefit from these advanced technologies.

Platform IT (PIT), which is identified in the RMF process, is a category of both IT hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. PIT is further categorized as PIT products, PIT subsystems, or PIT systems. PIT differs from “traditional” IT in that it is integral to – and dedicated to the operation of – a specific platform. Although the term PIT is used only by DoD, the concept of categorizing components and systems dedicated to the operation of a specific platform is not.

DoDI 8510.01 provides for a Type Authorization and Reciprocity. The type authorization is used to deploy identical copies of an IS or PIT system in specified environments. This method allows a single security authorization package to be developed for an archetype (common) version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting Platform Enclave³. Cybersecurity reciprocity reduces time and resources wasted on redundant test, assessment and documentation efforts and is best achieved through transparency (i.e., making sufficient evidence regarding the security posture of an IS or PIT system available, so that an Authorizing Official (AO) from another organization can use that evidence to make credible, risk-based decisions regarding the acceptance and use of that system or the information it processes, stores, or transmits).

A key challenge for Reciprocity is identifying the risks associated with the services/agencies Platform Enclave (Transport Backbone) and applying equivalent security controls mitigations to ensure the AO from one service will accept the TA from another service with a different PE configuration (e.g. Navy PSNet and AF CELAN). Implementing the DoDIN Joint Information Environment (JIE) should alleviate some of these issues, but the demonstration project should identify common security controls and solutions and gaps or mismatched controls that will need customized responses.

Additional information on the RMF process and related references can be found on the [SERDP-ESTCP website](#).

³ Platform Enclave-Those components of the control system that are standard IT components and can be secured in a standard manner independent of the type of control system. These components serve only the control system and include the IP network, network management and security devices (e.g., switches, routers), software, computers and/or other devices which provide management and security of the network.

Point of Contact

Mr. Tim Tetreault

Program Manager for Energy & Water (EW)

Environmental Security Technology Certification Program (ESTCP)

4800 Mark Center Drive, Suite 17D03

Alexandria, VA 22350-3605

Phone: 571-372-6397

E-Mail: timothy.j.tetreault.civ@mail.mil

For pre-proposal submission due dates, instructions, and additional solicitation information, visit the [ESTCP website](#).