

Environmental Security Technology Certification Program (ESTCP)

INNOVATIVE TOOLS THAT REDUCE THE TIME AND COST REQUIRED TO OBTAIN AND MAINTAIN AUTHORITY TO OPERATE FOR FACILITY ENERGY AND WATER CONTROL SYSTEMS AND CONNECTED TECHNOLOGY

OBJECTIVE

The DoD Installation Energy Test Bed seeks innovative tools that reduce the time and cost required to obtain and maintain Authority To Operate (ATO) for systems supporting new facility energy and water technologies. Proposed technologies must demonstrate that they help installation personnel reduce the time and cost to complete the Risk Management Framework process and that they satisfy requirements established in 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/tools that enable more efficient execution and/or documentation of portions of the cybersecurity process, such as aiding the incorporation of cybersecurity in FRCS design, the testing and validation of FRCS, or the continuous monitoring of FRCS.

Demonstration projects with the following characteristics are preferable:

- High likelihood of supporting reciprocity¹ between Services
- High calculable time and cost savings, as a direct result of the technology
- Minimal design and engineering required for deployment of the technology after the demonstration
- 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 and maintaining ATO for new facility energy and water control systems and devices.

BACKGROUND

Many new facility energy and water technologies are not able to provide 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

¹ 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.

as intended and be cost-effective, they must have access to DoD networks 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 cybersecurity reciprocity for purposes of reducing 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 service's/agency's Platform Enclave (Transport Backbone) and applying appropriate security control mitigations to ensure the AO from one service will honor the authorization from another service with a different enclave configuration (e.g. Navy PSNet and AF COINE).

Additional information on the RMF process and related references can be found on the SERDP & ESTCP website at:

<https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity>

POINT OF CONTACT

Mr. Tim Tetreault

Program Manager for Installation Energy & Water (EW)

Environmental Security Technology Certification Program (ESTCP)

4800 Mark Center Drive, Suite 16F16

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](#).