International Nuclear Security for Advanced Reactors (INSTAR)

In order to prevent the theft of nuclear material or sabotage of nuclear facilities, the International Nuclear Security for Advanced Reactors (INSTAR) program partners with the U.S. advanced nuclear reactor industry and embarking nuclear power countries on nuclear security topics to:

- Improve the security of future U.S. advanced reactor exports through early integration of security by design.
- Build nuclear security capacity in countries embarking on new nuclear power programs.
- Strengthen the global nuclear security regime to develop international guidelines and resources on evolving security considerations posed by advanced and small modular reactors (A/SMR).

These partnerships help support the responsible international deployment of U.S. advanced reactor technologies while ensuring technological innovation in meeting global security legal obligations and host country requirements.

Why Should You Partner with INSTAR on Security by Design?

Security is a significant cost driver for nuclear facilities. By working with the U.S. Department of Energy's National Nuclear Security Administration (DOE/ NNSA)'s INSTAR program on SeBD technical partnerships, U.S. companies can optimize internal resources and leverage the unique capabilities and expertise of the National Laboratories. For companies looking to export their technologies, it is most efficient to take international security requirements, guidance, and unique operating environments into consideration early in the design process. By working with INSTAR, vendors can:

- Identify and address nuclear security risks as part of a comprehensive system-level approach along with safety and international safeguards, thereby improving deployment readiness.
- Gain access to world-renowned security experts at the national laboratories, leverage resources, and utilize security tools from DOE.
- Reduce need for potentially costly retrofits and redesigns due to more efficient resource allocations in the security system design, thereby minimizing risk to scope, schedule and budget.
- Be better prepared to initiate dialogues with potential customer countries' regulatory authorities and owner/operators
- Apply a wholistic cybersecurity approach from critical digital assets to a fully risk-informed approach.
- Benefit from a graded approach to security where the level of physical protection should depend on the categories of the nuclear material (theft) or levels of unacceptable consequences (sabotage).

WHAT IS SECURITY BY DESIGN (SeBD)?

SeBD is an approach whereby protection-related elements are considered and incorporated early, frequently, and continuously throughout the design of a new nuclear facility to achieve cost and risk informed results. This can occur during the design, siting, construction, operation, and decommissioning of any nuclear facility.

164 States are party to the Convention on the Physical Protection of Nuclear Material (CPPNM) that establishes the legal obligations for physical protection of nuclear material during transport

130 States are party to the Amendment to the CPPNM that establishes the legal obligation for physical protection of nuclear facilities and nuclear material

10-12 embarking countries expected to have nuclear power by 2035

For more information, contact:
INSinfo@nnsa.doe.gov
https://nuclear-nexus.anl.gov/nexus/

INSTAR
INTERNATIONAL NUCLEAR SECURITY FOR ADVANCED REACTORS

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

Frequently Asked Questions

What is international security and how is it different from safeguards or domestic security?

International nuclear security is built upon the implementation of relevant international legal instruments, national nuclear laws, policies, regulations, and technical protection measures to prevent the theft or sabotage of nuclear material in transit and at nuclear facilities worldwide.

- International nuclear security is a State's responsibility and helps prevent the risk of internal and external malicious actors stealing material or sabotaging the facility.
- In contrast, nuclear safeguards are purely intended to verify that a country is using its facilities solely for peaceful purposes and is not diverting material for nuclear weapons.

How does INSTAR work with vendors to apply SeBD?

INSTAR, a Congressionally mandated program, provides funding to DOE national laboratory experts to partner with vendors under Cooperative Research and Development Agreements (CRADAs) or non-disclosure agreements (NDAs). By working with INSTAR, U.S. companies will be better positioned to engage with global customers. Specific areas of support are customized to the vendor's needs, reactor design concept, and technology readiness level. Some examples include:

- Conducting regulatory analyses and crosswalks to prepare vendors for international design reviews and licensing processes in other countries.
- Applying security analysis software tools for rapid design review of evolving physical security system requirements and technologies.
- Vital area and target set identification to evaluate advanced reactor theft/sabotage targets and vulnerabilities.
- Identifying material control requirements and approaches that harmonize domestic and international requirements and regulations.
- Security economics analysis to perform a cost-benefit analysis of design features.
- Design evaluation process outline (DEPO) training which is a methodology used to define, design, and evaluate physical protection systems.
- Conducting cyber security evaluations and providing design feature recommendations.

How does INSTAR work with DOE's Office of Nuclear Energy (DOE-NE) and Nuclear Regulatory Commission (NRC)?

DOE/NNSA is Congressionally mandated to work closely with DOE-NE and the U.S. NRC to support the development and integration of security by design in U.S. origin technology. INSTAR seeks to move the needle forward on U.S. civil nuclear technology development critical in meeting climate change goals by integrating into the existing processes vendors have underway and not hampering timelines.

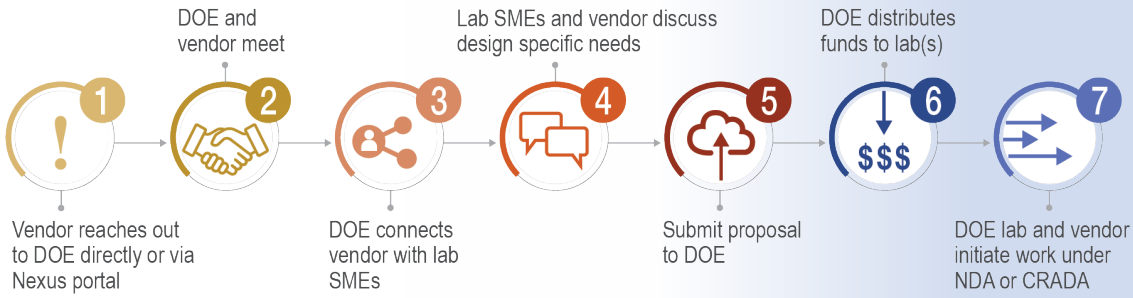
What are some examples of Security by Design?

- Modifying the locations of doors or barriers, camera infrastructure or wall thickness for enhanced detection, delay or response.
- Locating sabotage targets below-grade to improve resilience, thereby reducing the amount of blast-resilient delay barriers needed and improving cost-efficiencies.

How can a vendor engage with INSTAR?

Vendors can reach out to INSTAR directly or via the Nuclear Nexus portal to connect with NNSA and learn more about resources available to support U.S. companies.

INSTAR
INTERNATIONAL NUCLEAR SECURITY FOR ADVANCED REACTORS



For more information, contact:
INSinfo@nnsa.doe.gov
https://nuclear-nexus.anl.gov/nexus/

LLNL-MI-841655 24-FS-03