Independent Review of the United States Department of Energy's Use of Artificial Intelligence for Physical Security

September 2023

Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

ACRONYMS ii

MESSAGE FROM THE SECRETARY iii

EXECUTIVE SUMMARY v

1.0 BACKGROUND 1

2.0 SCOPE AND METHODOLOGY 2

3.0 RESULTS 3

4.0 CONCLUSION 7

REFERENCES 8

ACRONYMS

AI	Artificial Intelligence
DARPA	Defense Advanced Research Projects Agency
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
HEWD	House Energy and Water Development
NDAA	National Defense Authorization Act
PII	Personally Identifiable Information
PSO	Program Secretarial Office
S&S	Safeguards and Security

Message from the Secretary

The U.S. Department of Energy (DOE) Office of Enterprise Assessments (EA) conducted a review of the Department's requirements for and implementation of commercially available artificial intelligence (AI) technologies to detect, track, classify, and identify external physical security threats as required by House Report 117-98 and House Report 117-118.

Pursuant to statutory requirements, this report is being provided to the following Members of Congress:

- **The Honorable Kay Granger**
  Chairwoman, House Committee on Appropriations

- **The Honorable Rosa DeLauro**
  Ranking Member, House Committee on Appropriations

- **The Honorable Chuck Fleischmann**
  Chairman, Subcommittee on Energy and Water Development
  House Committee on Appropriations

- **The Honorable Marcy Kaptur**
  Ranking Member, Subcommittee on Energy and Water Development
  House Committee on Appropriations

- **The Honorable Patty Murray**
  Chair, Senate Committee on Appropriations

- **The Honorable Susan Collins**
  Vice Chair, Senate Committee on Appropriations

- **The Honorable Dianne Feinstein**
  Chair, Subcommittee on Energy and Water Development
  Senate Committee on Appropriations

- **The Honorable John Kennedy**
  Ranking Member, Subcommittee on Energy and Water Development
  Senate Committee on Appropriations

- **The Honorable Mike Rogers**
  Chairman, House Committee on Armed Services

- **The Honorable Adam Smith**
  Ranking Member, House Committee on Armed Services

- **The Honorable Doug Lamborn**
  Chairman, Subcommittee on Strategic Forces
  House Committee on Armed Services

- **The Honorable Seth Moulton**
  Ranking Member, Subcommittee on Strategic Forces
  House Committee on Armed Services

- **The Honorable Jack Reed**
  Chairman, Senate Committee on Armed Services

- **The Honorable Roger Wicker**
  Ranking Member, Senate Committee on Armed Services

- **The Honorable Angus King**
  Chairman, Subcommittee on Strategic Forces
  Senate Committee on Armed Services

- **The Honorable Deb Fischer**
  Ranking Member, Subcommittee on Strategic Forces
  Senate Committee on Armed Services

If you have any questions or need additional information, please contact me or Ms. Katie Donley, Budget Director, Office of the Chief Financial Officer, at 202-586-0176; or Ms. Becca Ward, Deputy Assistant Secretary for Senate Affairs or Ms. Janie Thompson, Deputy Assistant Secretary for House Affairs, Office of Congressional and Intergovernmental Affairs, at 202-586-5450.

Sincerely,

Jennifer Granholm

Independent Review of the United States Department of Energy's Use of Artificial Intelligence for Physical Security

EXECUTIVE SUMMARY

In response to Congressional direction, the U.S. Department of Energy (DOE) reviewed the requirements for and implementation of commercially available artificial intelligence (AI) technologies to detect, track, classify, and identify external physical security threats. The review considered various AI technologies, such as computer vision and sensor fusion; the potential risks and vulnerabilities introduced through commercial AI technologies in security applications; and considerations for piloting these technologies.

DOE directs its sites to use technology in a cost-effective manner, integrate technologies with response force tactics, and employ appropriate sensor technology to address applicable environmental conditions. Multiple sites operating under DOE's Office of Science, Office of Nuclear Energy, Office of Environmental Management, and National Nuclear Security Administration have implemented AI-based technology. Evaluated and deployed AI technologies include computer vision, such as video analytic platforms; facial recognition; and rapid video forensics and sensor fusion technologies, such as fiber-optic vibration detection and gunshot detection.

DOE Program Secretarial Offices (PSO), Field Offices, and management and operating contractors acknowledge the risks of using commercially available AI in physical security applications. These risks include but are not limited to legal liabilities, unintended biases, vulnerabilities in managing and controlling personal information and privacy, a lack of data set integrity and comprehensiveness, auditing limitations, and inadequate cost-benefit analyses. These concerns have contributed to caution in DOE more aggressively pursuing more advanced technologies and solutions.

DOE does not explicitly require using AI in physical security applications; however, there are overarching requirements to use technology in a cost-effective manner. Accordingly, under the auspices of the Program Secretarial Offices, many DOE sites are evaluating, piloting, and deploying AI technologies to meet security requirements. While the security industry and DOE recognize the inherent vulnerabilities and risks associated with using AI in physical security applications, as AI technologies mature, the risks of use and the cost of the applications will decrease, offering DOE and its management and operating contractors more opportunities to leverage AI technologies as cost-effective methods to reduce labor costs while continuing to manage the physical security threats to some of the Nation's most significant assets.

Independent Review of the United States Department of Energy's Use of Artificial Intelligence for Physical Security

1.0 LEGISLATIVE LANGUAGE

In the draft House Energy and Water Development (HEWD) fiscal year 2022 appropriations bill, the HEWD Committee referenced recent advancements in commercially available AI technologies, including computer vision and sensor fusion capabilities. The draft bill noted that these innovative capabilities might make it possible to detect, track, classify, and identify threats and provide an effective method to meet force protection and physical security requirements. The draft bill also stated that other government agencies use these technologies to demonstrate security improvements, augment the cognitive ability of human operators, lower staffing burdens, and reduce costs. The HEWD committee directed the Secretary of Energy to review the requirements for and use of commercially available AI technologies across the DOE complex.

This report fulfills the Committee on Appropriations requirement in House Report 117-98, which accompanied the Energy and Water Development and Related agencies Appropriations Bill for FY 2022. The requirement states:

The Committee notes recent advances in commercially available technologies, including artificial intelligence, computer vision, and sensor fusion capabilities, may make it possible to deploy innovative technologies to detect, track and identify threats at scale to help meet force protection and physical security requirements. The Committee is aware that such initiatives are underway in federal agencies such as the Department of Defense and Customs and Border Protection. The Department is directed to conduct a review of its security requirements across the entire complex to assess how the use of artificial intelligence and commercially available technologies could improve security while reducing overall costs. The Department shall provide to the Committee not later than 180 days after enactment of this Act a report detailing its findings. The report shall include information on if and how the Department is already using artificial intelligence or commercially available technologies, include a recommendation for a pilot project at one or more sites within the complex, and include cost estimates and comparisons to security costs.

This report also addresses the requirement in House Report 117-118, which accompanied the National Defense Authorization Act for FY 2022. The requirement states:

Leveraging Artificial Intelligence and Innovative Commercially Available Technology to Secure Department of Energy Installations. The committee notes that recent advances in commercially available technologies, including artificial intelligence, computer vision, and sensor fusion capabilities, have made it possible to deploy innovative technology to detect, track, classify, and identify threats at scale to meet force protection and installation security requirements. These efforts have demonstrated improvements in security, while augmenting the cognitive ability of human operators and drastically lowering both the manpower burden and fully burdened cost to secure critical infrastructure. The committee is aware that such initiatives are occurring with other government agencies, including the Department of Defense and Department of Homeland Security Customs and Border Protection. The committee directs the Secretary of Energy to conduct a review of its security requirements across the entire complex, including Department of Energy laboratories, Environmental Management facilities, and National Nuclear Security Administration labs, plants, and sites, to assess how and if the use of artificial intelligence and commercially available technology could improve security efficiencies while possibly reducing security

overall costs and mission impacts from security controls. Additionally, the review should include an evaluation of risks and vulnerabilities potentially introduced through commercial artificial intelligence capabilities. The Department shall provide a briefing to the House and Senate Armed Services Committees detailing its findings not later than August 1, 2022. The report shall include recommendations on the feasibility of a pilot program at one or more sites within the complex to field commercially available capabilities, as required by section 3307 of title 41, United States Code, to assess these capabilities to enhance security and reduce overall security costs.

2.0 SCOPE AND METHODOLOGY

2.1 Scope

This review aims to address the committee's direction as follows:

(1) Examine DOE's requirements for the use of AI for physical security.

(2) Identify commercially available AI technologies evaluated and deployed at DOE sites to detect, track, classify, and identify external physical security threats.

(3) Describe the potential risks and vulnerabilities associated with using AI in physical security applications.

(4) Provide considerations for Departmental entities in piloting commercially available AI.

The AI technologies that DOE is researching and developing and partnership programs, as well as technologies that focus on threats such as insiders or cybersecurity, were outside the scope of this review.

2.2 Methodology

The review used surveys, interviews, benchmarking, and evaluation of commercially available solutions.

2.2.1 Artificial Intelligence

The term AI has a range of meanings in current scientific literature and government publications. For this review, the team used the definition codified in the National Defense Authorization Act (NDAA) of 2021: "The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."

In addition to the NDAA's definition of AI, the review used the Defense Advanced Research Projects Agency (DARPA)-developed taxonomy of AI development waves:

(1) The first wave is a technology that uses expert knowledge or criteria developed in law or other authoritative sources, encoded into a computer algorithm, and referred to as an expert system. First-wave systems compare sensor inputs to human-defined parameters that yield an autonomous decision. An example is video analytic software that reads shipping container numbers as they process through a port and alerts a human user if a container number is not on a human-entered manifest list.

(2) The second wave is technology based on machine learning or statistical learning, and these systems perceive and learn. Second-wave systems adjust parameters used to make decisions based on iterative inputs. An example is a voice-activated digital assistant that automatically learns and recognizes individual user voices.

(3) The third wave is a technology that combines the strengths of the first and second waves and adds the capabilities of contextual sophistication, abstraction, and explanation. Third-wave systems can adapt to new situations and explain the reasoning behind decisions. An example is a ship that can navigate without human intervention for an extended period, sensing other ships, adjusting to weather conditions, navigating sea lanes, and conducting necessary tasks.

Further, the review used the following definitions of computer vision and sensor fusion technology:

- Computer vision is a subset of AI that includes systems that analyze information from digital images, videos, or other visual inputs to categorize objects, people, and items of interest.
- Sensor fusion is a subset of AI that combines and compares data from multiple inputs to produce a more accurate or complete representation of the environment for evaluation or presentation to the user.

3.0 RESULTS

This report documents the results of the review in four sections. Section 3.1 examines DOE's requirements for using AI technology to meet physical security needs. Section 3.2 presents the AI technologies that DOE sites are evaluating or deploying. Section 3.3 describes the potential risks and vulnerabilities associated with using commercial AI technologies in DOE physical security applications. Section 3.4 provides considerations for piloting commercially available AI.

3.1 DOE Requirements

3.1.1 DOE Requirements Promulgation

The Secretary of Energy, the Deputy Secretary of Energy, and three Under Secretaries (the Under Secretary for Infrastructure, the Under Secretary for Nuclear Security and Administrator for the National Nuclear Security Administration, and the Under Secretary for Science and Innovation) are the Department's principal officers responsible for the multitude of business units. These officers employ deputy administrators, directors, and assistant secretaries and a system of directives to promote operational consistency in DOE activities, including physical security. The DOE directives contain contractor requirements documents, which promulgate contractor responsibilities through formal contract mechanisms. In addition, the PSOs sometimes publish supplemental directives that mandate specific methodologies to implement Departmental directives, provided they do not contradict, delete, or duplicate provisions in the policy, regulation, or order.

3.1.2 DOE Requirements for the Use of AI

DOE maintains multiple safeguards and security (S&S) directives that establish requirements for protecting Departmental assets and using technology for physical security. For example, DOE Order 470.4B, *Safeguards and Security Program*, requires that "S&S programs must be tailored to address site-specific characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner." DOE Order 473.2A, annex 2, *Department of Energy Tactical Doctrine*, requires sites to "use technology to distract, interrupt, disable, or neutralize anyone who has obtained unauthorized access to target locations" and to "integrate

technology such as advanced detection and observation systems with response force tactics." Additionally, DOE Order 473.1A, *Physical Protection Program*, requires intrusion detection systems to "utilize appropriate sensor technology to address applicable environmental conditions." Although DOE does not have an explicit requirement to consider using AI technologies, sites are directed to use technology in a cost-effective manner and encouraged to identify cost savings.

3.2 AI Technologies Evaluated or Deployed for Physical Security

Commercially available physical security technologies are primarily first-wave technologies, and although algorithms are becoming more advanced, most technologies rely primarily on fixed programming. Some are second-wave technologies, which employ aspects of machine learning and adaptive algorithms. This technology is primarily used in video analytics applications, such as object of interest detection and facial recognition. It leverages adaptable algorithms to learn and reduce repeated false or nuisance alarms. Few third-wave physical security technologies exist because of a lack of industry standards for analytic models, comprehensiveness of available data sets, and limitations in current software and hardware capabilities.

3.2.1 First Wave

DOE sites are deploying or evaluating systems and applications that meet the definition of first-wave AI technologies, including:

- *Thermal and visual spectrum video analytics.* These technologies use computer vision to discriminate moving targets, determine whether the target is a potential external threat, and make an autonomous decision to initiate an alarm to a human user. The video analytic systems use a combination of target characteristics, including size, speed, travel direction, and visual or infrared signature, to classify the target and then compare the target data to user-established geographical parameters or boundaries that, if crossed, indicate a potential external physical security threat.
- *Computer vision-based facial recognition*. This matching technology compares captured facial recognition data to images of authorized individuals within a database. The system associates the individual with their access control records and can alert users in the event of a mismatch.
- *Multiple two-dimensional radar system technologies*. These systems use combinations of target characteristics, such as radar signature, speed, and travel direction, to classify and identify potential threats. The systems compare target data to user-established parameters to determine whether to initiate an alarm. Many designs are integrated with assessment cameras and provide video to a human user in conjunction with the alarm.
- *Video content analytics.* This first-wave video analytic technology leverages computer vision to continually evaluate surveillance camera video streams, classifying objects and recording metadata on object characteristics and timestamps. The technology allows users to rapidly isolate and review historical video footage showing user-selected sets of attributes or individual objects of interest.
- *Fiber-optic vibration detection systems.* The systems are calibrated to identify the cause of detected vibrations on a security barrier. The systems discern between vibrations caused by environmental phenomena and those by a physical security threat traversing or defeating the security barrier. The system fuses inputs from additional sensors, such as anemometers, to improve environmental filtering and the accuracy of initiating an alarm.
- *Gunshot detection technologies.* These technologies fuse the acoustic signature and timing received from several sensors to a catalog of recorded gunshot signatures to initiate an alarm that includes the classification and origin of the gunshot.

Deployed First-Wave Technologies

PSO	Technology	Application
Office of Environmental Management location(s)	Thermal spectrum video analytics	Human intrusion detection along security layer boundaries
	Visual spectrum video analytics	Early-warning vehicle detection in areas approaching security layer boundaries
Office of Science location(s)	Visual spectrum video analytics	Human and vehicle intrusion detection along security layer boundaries
	Video content analytics	Rapid video forensics
Office of Nuclear Energy location(s)	Visual spectrum video analytics	Human and vehicle intrusion detection along security layer boundaries
	Two-dimensional radar surveillance and assessment	Early-warning human and vehicle detection in areas approaching security layer boundaries
	Fiber-optic vibration detection	Human intrusion detection across security layer barriers
National Nuclear Security Administration location(s)	Visual spectrum video analytics	Human intrusion detection along security layer boundaries
	Two-dimensional radar surveillance and assessment	Early-warning human and vehicle detection in areas approaching security layer boundaries
	Gunshot detection	Rapid identification and location of threats outside of security layer boundaries

Evaluated First-Wave Technologies

PSO	Technology	Application
Office of Environmental Management location(s)	Facial recognition matching	Identification of personnel who have accessed security areas through comparison to an image database.

3.2.2 Second Wave

DOE sites are evaluating and deploying a technology that meets second-wave AI criteria:

- *Facial recognition system.* This technology (1) applies machine learning and utilizes facial recognition capability, and (2) leverages existing access control systems to authenticate authorized personnel initially and uses facial biometrics for verification. DOE sites use this system for automated "contactless" access control or as part of multi-factor authentication when paired with existing access controls.

Evaluated and Deployed Second-Wave Technologies

PSO	Technology	Application
Office of Science Location(s)	Facial recognition with adaptive enrollment	Used for both access control and biometric multi-factor authentication in multiple locations.

3.2.3 Third Wave

DOE is not currently evaluating or deploying any third-wave technologies.

3.3 Risks and Vulnerabilities Associated with Commercial AI in Physical Security Applications

The industry acknowledges the risks of using commercially available AI in physical security applications. These risks include legal liabilities, unintended biases, vulnerabilities in managing and controlling personal privacy and information, lack of integrity and comprehensiveness of data sets, auditing limitations, and inadequate cost-benefit analyses.

3.3.1 Non-Compliance and Legal Considerations

The use of AI in physical security applications may be subject to legal and compliance requirements, including regulations related to video surveillance, data privacy, and consent. It is essential to ensure that the use of AI in physical security applications complies with all applicable laws, regulations, and organizational policies. This may include obtaining consent from monitored individuals, ensuring appropriate use of data, and complying with legal requirements for data retention and disposal. Non-compliance may expose DOE to legal liabilities.

3.3.2 Unintended Bias

Biases in AI security technologies can result in discriminatory outcomes, such as profiling based on race, gender, or other protected characteristics. Proprietary source codes, model algorithms, or data sets may contain unintended or unknown biases, which could expose DOE to public embarrassment and legal liabilities.

3.3.3 Privacy Violations and Personally Identifiable Information (PII) Data Compilation List

AI technology that facilitates the correlation of information about individuals across large and numerous databases poses challenges in protecting privacy and sensitive data. As AI evolves, there is an ever-increasing possibility of misusing personal information and intruding on privacy interests. Although DOE establishes privacy program requirements to safeguard PII, commercial propriety AI systems and technologies may not comply with DOE requirements and standards. PII, such as financial, relationship, and health status, can be used to target DOE employees, potentially allowing unauthorized individuals or adversaries to map individuals, predict responses, or attempt to manipulate behavior.

3.3.4 Lack of Integrity and Comprehensiveness of Data Sets Used for Training and Validation

Machine-learning AI models learn from large quantities of data, or training sets, to predict results or perform tasks. The quality, reliability, and comprehensiveness of the training sets directly affect the accuracy of the expected outcome or task. However, no industry standards exist for evaluating or vetting public or commercial data. Using commercial AI technologies with proprietary information complicates DOE's ability to validate the training framework and data sets. In physical security applications, this introduces risks with machine-learning AI technology's ability to reliably discern and prioritize threats and avoid "false negative" decisions.

3.3.5 Limitations to Auditing Third-Party and Proprietary Algorithms

AI proprietary source codes or model algorithms pose unique challenges for independent assessments and audits because not all aspects of the framework, input, and operations are visible to users and auditors. This limits the ability to audit how the AI system makes its decisions. This presents risks for users and auditors to have confidence that machine-learning-enabled security technology will reliably detect and prioritize threats.

3.3.6 Reduced Cost-Effectiveness

Implementing and maintaining AI systems, including hardware, software, training, and ongoing operational expenses, may provide cost-effective benefits for improved security and operational efficiency and reduced false alarms. However, without a thorough cost-benefit analysis to assess the AI system's long-term viability and return on investment, DOE could implement security technologies with a negative return on investment.

3.4 Considerations for Technology Evaluations and Pilot Programs

As covered in section 3.1.2, *DOE Requirements for the Use of AI*, DOE has requirements that direct sites to evaluate the most cost-effective means to meet security requirements, including advancements in security technology such as AI. DOE recognized that as technology and AI advance, the benefits in incorporating advancements into physical security applications, DOE is also aware that the decisions must include careful consideration based on assets, threat assessment, interoperability with existing systems, locations, compliance and legal requirements, training and user adoption, cybersecurity, and maintenance.

Accordingly, the review surmises that as the systems mature, the cost of the applications decreases, the industry addresses the legal, and compliance concerns, and system reliability improves that PSOs, Field Offices, and its management and operating contractors will leverage AI technologies to decrease labor costs and to more cost-effectively manage the physical security programs protecting some of the nation's most significant assets.

4.0 CONCLUSION

DOE does not explicitly require using AI to implement technology-related security requirements. However, DOE Directives require its sites to utilize technology cost-effectively and encourage sites to identify cost savings.

Accordingly, some DOE sites use commercially available AI technologies to detect, track, classify, and identify external physical security threats; technologies include computer vision, including video analytic platforms, facial recognition, rapid video forensics, and deployed sensor fusion technologies, including

fiber-optic vibration detection and gunshot detection. Other locations evaluate technologies based on known risks, including legal liabilities, unintended biases, managing and controlling personal information and privacy, lack of integrity and comprehensiveness of data sets, and auditing limitations.

DOE is confident as AI technologies mature, the risks of use and the cost of the applications decrease, its PSO, Field Offices, and its management and operating contractors will take more opportunities to leverage AI technologies as cost-effective methods to reduce labor costs and improve their abilities to address the physical security threats.

REFERENCES

Government Accountability Office, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Agencies* (Washington, D.C.: June 2021)

National Defense Authorization Act (January 21, 2021) AI Definition: Public Law 116-283

John Launchbury, *A DARPA Perspective on Artificial Intelligence* (2016)

National Security Commission on Artificial Intelligence, *The Final Report* (2021)

Executive Order 13859 of February 11, 2019, *Maintaining American Leadership in Artificial Intelligence*, 84 Fed. Reg. 3967

Executive Order 13960 of December 3, 2020, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*