A Message From Leadership

October and early November have been an incredibly busy and productive time at AITO. These are also months when our Nation recognizes the importance of cybersecurity, and of vigilantly protecting the critical infrastructure we rely on as the foundation for our prosperity and security.

And thanks to groundbreaking work pioneered at DOE’s national labs, artificial intelligence is playing a growing role in both.

As you’ll read in this month’s edition, I recently traveled to DOE’s Pacific Northwest National Laboratory (PNNL) to hear directly from some of the world’s leading experts in AI and cybersecurity on their efforts to leverage the latest cutting-edge technologies to protect America’s electrical grid and other critical infrastructure.

But just as AI becomes a central component of high consequence systems with little room for failure, there is an urgent need to recognize that the data, models, and algorithms -- on which AI relies -- are in need of protection too.

The same adversaries that seek to disrupt our cybersecurity are stepping up their efforts to infiltrate and corrupt our data sets and machine learning models. This fact threatens our human decision-making based on AI results and increases risks to the reliability of autonomous systems.

But despite these vulnerabilities, investment in AI assurance to combat what is called “adversarial AI,” has yet to rise to the level of the threat.

As our world has grown more digitally connected, cybersecurity has become an essential industry. Adversarial AI is the next front line for America’s security experts. It’s time we recognize that as the role of AI in our security grows, so too does the need for securing the AI itself.

As always, thank you for your interest in our work at AITO. While we all prepare to gather (safely) for Thanksgiving and the coming Holiday Season, I would like to wish you all good health and Happy Holidays!

Cheryl Ingstad
Director
Artificial Intelligence & Technology Office
Our Top Story

AITO Director Cheryl Ingstad recently visited the Pacific Northwest National Laboratory (PNNL) in Richland, WA to see first-hand how PNNL scientists are applying AI and ML to enhance grid security, ensure a secure, flexible, and resilient electric power system, and receive an update on the First Five Project.

This Month's Highlights

PNNL pilots two use cases applying blockchain technology to improve the cybersecurity of critical electricity infrastructure.
Ripples is a first-of-its-kind network analysis tool that -- when coupled with the power of a supercomputer -- can speed real-time applications for cybersecurity, transportation, and infectious disease tracking.

As AITO continues to grow, we are pleased to announce that two 2021 Presidential Innovation Fellows have joined our team.

Tricia Martinez will bring her experience and passion to our efforts to develop an AI-ready workforce at DOE.

Scott Gorman will be primarily focused on the ever-increasing challenge of adversarial AI and how we protect our data and algorithms from external corruption.
Welcome Tricia and Scott! We’re honored to have you both as part of the AITO team.

Named for the Greek word for wisdom, SOPHIA is an AI-optimized software sentry that protects energy sector networks and control systems from cyberattacks and helps network operators detect intruders and other anomalies.
A true privilege to tour the #HooverDam at @lakemeadnps with @ScienceUnderSec. The Dam is a marvel of American ingenuity, imagination, and determination. I encourage you to learn more about its mission and critical importance to the American Southwest!

4:07 PM · Oct 30, 2020 · Twitter Web App

🔗 FOLLOW @AiDirector on Twitter!