CSET | CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Summary of Repurposing the Wheel: Lessons for AI Standards

Standards are key components of promoting good governance. However, establishing standards for rapidly evolving and diverse artificial intelligence (AI) technologies is a challenge. CSET and the Center for a New American Security co-organized a series of workshops in the fall of 2022 to examine case studies of other standards created across several industries to draw lessons for AI.

We found:
- **Finding 1: AI risk assessment and mitigation should include examining how interdependencies affect systemic risk.**
  - Recommendation 1: Critical infrastructure owners and operators should track the interdependencies of their AI systems.
  - Recommendation 2: The Office of Management and Budget (OMB) and the Office of Science and Technology Policy Directors' forthcoming guidance on minimum risk management practices for AI should require that agencies identify the risks that could emerge from interdependencies between their AI systems and other entities.

- **Finding 2: Guidance on testing and re-approval of AI systems should be calibrated to risk and account for changes to AI systems over time.**
  - Recommendation 3: The U.S. Department of Defense should create thresholds or triggers for different levels of rigor and oversight for testing military AI systems.
  - Recommendation 4: U.S. government agencies should establish processes for the reassessment and re-testing of systems as they change over time and share these processes with each other.

- **Finding 3: Compliance assistance can help small- and medium-sized businesses prepare for and implement AI regulation.**
  - Recommendation 5: Congress should create a pilot AI Compliance Assistance Office within the U.S. Department of Commerce, which should later expand to other government agencies.

- **Finding 4: Third-party organizations can remove barriers to standards development, implementation, compliance, and tracking.**
  - Recommendation 6: OMB should direct a study by an independent body to inform the designation of third-party accreditation bodies that ensure certifiers evaluate the implementation of AI standards in a consistent manner.
  - Recommendation 7: Professional organizations should establish AI standards access funds, whistleblower protection programs, and reporting programs to gather anonymized information on AI risks from industry participants.

- **Finding 5: Non-regulatory governance is one mechanism that can support the safe development and use of AI systems.**
  - Recommendation 8: The United States should commence discussions in the G7 about creating the equivalent of a Financial Action Task Force for AI.
  - Recommendation 9: The National Institute of Standards and Technology (NIST) should create an online portal to ensure technical developments relevant to standards are captured and publicized.

- **Finding 6: Coordination and regular efficacy checks of standards can ensure that standards development is efficient and effective.**
  - Recommendation 10: Standard-setting bodies should host biannual summits to coordinate on standards interoperability and efficacy.
  - Recommendation 11: NIST should support the development of testbeds to monitor AI standards for effectiveness.

For more information:
- Download the report: https://cset.georgetown.edu/publication/repurposing-the-wheel
- Contact Us: Mina Narayanan mjn82@georgetown.edu