iMerit

USING SWOT ANALYSIS TO ASSESS AGENCY USE IN GOVERNMENT AI

E-BOOK

To cast a clear-eyed, balanced view of current data governance, iMerit has applied the familiar business tool known by its acronym SWOT -- Strengths, Weaknesses, Opportunities, Threats. These observations are derived by the Content Team at iMerit from various resources referenced in this report.

STRENGTHS:

- Agency AI/ML use is spread across a wide range of policy areas and serves diverse regulatory functions.
- A majority of profiled AI use cases (53%) were supervised by in-house agency technologists, which speaks to strong internal capability, even as other agencies rely on private contractors to build out AI capacity. In-house expertise yields AI tools that are better tailored to complex governance tasks and more likely to be implemented in a lawful, policy-compliant, and accountable fashion. (Stanford-NYU-ACUS)
- Public-private partnerships are finding traction, with agencies such as the National Oceanographic and Atmospheric Administration (NOAA) and Department of Education forming working alliances with the private sector and with academic institutions. It provides continued access to government data and adds value for private stakeholders and the economy.

WEAKNESSES

- Only one in eight agency use cases rated their AI tools as high in sophistication, underscoring the need for agencies to acquire and make use of more advanced AI technology. (Stanford-NYU-ACUS)
- Half of CDOs surveyed say their resources are under-funded.
- Three in four CDOs surveyed don't think the resources at their disposal to fulfill their job requirements are adequate.
- Data literacy in the federal workforce is spotty, relative to the need for all hands on deck to support the Federal Data Strategy. According to MIT, data literacy is "the ability to read, work with, analyze, and argue with data." (Federal News Network)
- When a CDO is "dual-hatted" (the same person holding two or more positions at once), it can undermine the efficacy and specialized nature of the CDO role. ability to read, work with, analyze, and argue with data." (Federal News Network)

- Lack of full alignment -- depending on agency and the local workplace culture -- between the CDO's understanding of the role and how the supervisor (such as a CIO) sees it. A related issue is how agency leadership looks upon the rising priority of evidence-informed decisions anchored by data.
- Government agencies do not consistently apply data-driven decision-making practices. Smarter use of data and evidence is needed to orient decisions and accountability around service and results. Despite advances in interactive, usercen tered design, the American public often lacks the same opportunity to provide feedback on federal programs and services that it has for services it receives from the private sector, making it harder to continuously improve federal services.

OPPORTUNITIES

- One study found that the Department of Veterans Affairs (VA) spent more than 150 million hours on documenting and recording information. It also projected that the Department of Homeland Security (DHS) could save 800,000 hours annually by increasing automation of compliance with standards. The Government needs more nimble and effective approaches to keep technologies and workforce skills current, and to ensure that the Federal workforce can meet future needs. (President's Management Agenda)
- Too many Federal employees perform outdated duties that rely on outdated skill sets, and the government too often struggles to award effective, timely contracts. (Stanford-NYU-ACUS)
- Managed well, algorithmic governance tools can modernize public administration, promoting more efficient, accurate, and equitable forms of state action. (Stanford-NYU-ACUS)
- By fully vesting authority in the CDO as a leadership role equal to comparable C-level positions, agencies would further support and elevate the performance of Chief Information Officers, Chief Evaluation Officers, and others.
- CDOs are well positioned to make the case for data as a strategic asset that is useful by stakeholders in and out of government. They should have a seat at the table with other senior agency leaders as decisions are made. (Data Foundation)

- More than half of federal agencies have yet to experiment with AI and related machine learning tools.
- The National Security Commission on Artificial Intelligence (NSCAI) told a U.S. House of Representatives panel in fall 2020 that "existing programs will not bring enough digital talent into the public service workforce to meet serious shortages. We propose building a United States Digital Services Academy."Eric Schmidt, former CEO of Google and chair of NSCAI, called the proposal a "profound change that's needed," adding that there is "infinite appetite for this idea if we can find the money." (MeriTalk)
- Agency administrators, judges, technologists, legislators and academics should think carefully about how to spur government innovation involving the appropriate use of AI tools, while ensuring accountability in their acquisition and use. (Stanford-NYUACUS)

THREATS:

- AI has the potential to raise distributive concerns and fuel political anxieties. Growing agency use of AI creates a risk that AI systems will be gamed by better-heeled groups with resources and know-how. An enforcement agency's algorithmic predictions, for example, may fall more heavily on smaller businesses that, unlike larger firms, lack a stable of computer scientists who can reverse-engineer the agency's model and keep out of its cross-hairs. If citizens come to believe that AI systems are rigged, political support for a more effective and tech-savvy government will evaporate quickly. (Stanford-NYU-ACUS)
- Managed poorly, government deployment of AI tools can hollow out the human expertise inside agencies with few compensating gains, widen the public-private technology gap, increase undesirable opacity in public decision-making, and heighten concerns about arbitrary government action and power. (Stanford-NYU-ACUS)
- The most frequent use cases of AI in government are in law enforcement. Customs and Border Protection (CBP) has invested in facial recognition technology and risk prediction modeling. AI/ML tools may, as in CBP's case, significantly expand an agency's scope and reach, and enable it to make agency operations more efficient and accurate. At the same time, such programs raise privacy and security risks and reveal basic tensions between the goals of law enforcement and agency transparency. (Stanford-NYU-ACUS)