

## Executive Summary from “AI Incidents: Key Components for a Mandatory Reporting Regime”

In our past publication, “[An Argument for Hybrid AI Incident Reporting](#),” we proposed implementing a federated\* and comprehensive artificial intelligence incident reporting framework to systematically record, analyze, and respond to AI incidents. The hybrid reporting framework proposes implementing mandatory, voluntary, and citizen reporting mechanisms. This document describes the critical content that should be included in a mandatory AI incident reporting regime and should also inform voluntary and citizen reporting efforts.

In this publication, we define a set of standardized key components of AI incidents that can be used as a reporting template to collect vital AI incident data. These components include, but are not limited to, information about the type of AI incident, the nature and severity of harm, technical data, affected entities and individuals, and the context and circumstances within which the incident unfolded. While intentionally high level, our proposed set of components distills information from existing AI initiatives that track real-world events, harms, and risks related to AI, and incorporates lessons learned from incident reporting systems and practices in the transportation, healthcare, and cybersecurity sectors.

If adopted and used widely and consistently by governments, regulators, professional organizations, developers, and researchers, these reporting components can help enhance AI safety and security measures by:

- Facilitating consistent data collection of AI incidents
- Promoting tracking, monitoring, research, and information sharing of AI incidents
- Enhancing knowledge around AI-related harms and risks
- Ensuring that essential AI incident data is collected to prevent reporting gaps
- Building a foundational framework for agile incident reporting that adapts to AI advancements

To fully utilize the benefits of this list of components, we recommend publishing mandatory AI incident reporting formats based on them and establishing an

---

\* We define a federated framework as a centralized framework prescribed by a singular authoritative government body or the federal government. The framework stipulates a set of minimum requirements that can be adapted and implemented across government agencies or nongovernmental organizations.

independent investigative agency to uncover incident data that may not be immediately discernible at the time of reporting. This list can also serve as a template for desirable disclosure guidelines of incident data for voluntary and citizen AI incident reporting systems.

**For more information:**

- Download the report: <https://cset.georgetown.edu/publication/ai-incidents-key-components-for-a-mandatory-reporting-regime/>
- Contact us: [cset@georgetown.edu](mailto:cset@georgetown.edu)