**Immersive Technologies Cybersecurity and Privacy Topics for Feedback**

**I. Background**

Advances in computer vision, data processing, and other technologies have enabled novel Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) solutions, collectively called immersive technologies. In general, immersive technologies are hardware and software systems that create interactive digital visual and spatial environments that users can inhabit. These immersive environments can vary in the extent to which they incorporate virtual components. For example, AR layers digital objects over the user’s “real-world” environment, while VR can transport users to an entirely virtual alternate environment. These technologies hold promise to drive innovation and economic growth in numerous areas such as workforce, accessibility, and healthcare. Their creation and use can, however, generate cybersecurity and privacy risks, some of which may be novel.

These new technologies have interdisciplinary and integrative implications as well. They mix knowledge and approaches from myriad fields, such as neuroscience, psychology, behavioral studies, and statistics. Further, their integration with other emergent technologies like Artificial Intelligence (AI) and Internet of Things (IoT) adds complexity to the unique context in which cybersecurity and privacy risks can arise and will need to be managed.

With these motivations, NIST aims to learn more about potential cybersecurity and privacy considerations associated with immersive technologies. We seek comment or feedback on a variety of topics (described below) to help inform future research and development of guidelines, tools, and other resources to support effective privacy and cybersecurity risk management for immersive technologies.

NIST will gather feedback on these topics at a variety of roundtables, meetings, workshops, and other engagements, but we also welcome direct feedback via our email: immersivetech@nist.gov. Updated information on this workstream is available at <https://www.nist.gov/securing-emerging-technologies>.

**II. Topics for Feedback**

Respondents can address one or more of the following topics and need not respond to all topics.

*A. Immersive Technology Ecosystem and Use Cases*

NIST seeks comment on the ecosystem of entities that support immersive technologies. This ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships. Complexity can increase when entities are supported by a chain of sub-entities (e.g., manufacturers supported by multiple component suppliers). In particular, NIST seeks stakeholder feedback on the following topics:

1. Types of entities and roles (e.g., manufacturer, developer, customer, user, and business partners) that characterize the immersive technologies ecosystem
2. Ways in which the immersive technologies ecosystem is unique from other data processing ecosystems

NIST also seeks comments on current and potential future uses and misuses of immersive technologies across all applicable sectors and user bases, including any barriers to adoption. In particular, NIST seeks stakeholder feedback on the following topics:

1. Current and potential future use cases for immersive technologies, including benefits to innovation and to the public interest
2. The role(s) of emergent technologies (e.g., AI, IoT, blockchain, etc.) in current or potential future immersive technology use cases
3. The role(s) that emerging, but nascent, technologies (e.g., quantum computing, brain-computer interfaces) could play in potential future immersive technology use cases
4. Ways in which immersive technologies could be misused, including potential harms such misuse could create for individuals or groups
5. Barriers (e.g., technical limitations, costs, usability, etc.) that hinder the development or deployment of current and future immersive technologies

*B. Privacy and Cybersecurity Risk Considerations*



Cybersecurity and privacy risks are distinct but can overlap, as illustrated in the Venn diagram above.[[1]](#footnote-2) For example, data confidentiality may be both a cybersecurity and privacy consideration for a system. But system availability considerations may not involve privacy, while secondary use of information derived from user engagement may not involve system cybersecurity. Immersive technologies may generate cybersecurity and privacy risks, some of which can be novel or mix in complex ways. NIST seeks comment on this topic, including the following:

1. Examples of cybersecurity or privacy risks associated with immersive technologies
2. Cybersecurity or privacy risks that are unique or novel to immersive technologies
	* If such risks exist, factors that make them unique or novel (e.g., the type(s) or characteristics of data processed, the context in which the data is processed, etc.)
3. Ways in which immersive technologies can improve cybersecurity or privacy outcomes
4. New technological, organizational, or societal approaches to cybersecurity and privacy that are available or needed for immersive technologies
5. Ways in which the use of machine learning and other AI techniques or systems impact cybersecurity and privacy risks for immersive technologies
6. Ways in which delivery of other trust factors or engineering objectives (i.e., privacy, safety, resiliency, reliability) rely on, or are hindered by, cybersecurity in the context of immersive technologies
	* Ways, if any, that cybersecurity enables immersive technologies to be privacy-, and safety-preserving, resilient, and reliable for users
	* Ways, if any, that cybersecurity when applied to immersive technologies may be detrimental to privacy, safety, resiliency, or reliability
7. How traditional privacy principles (e.g., data minimization) are applied in the context of immersive technologies
	* Ways in which these technologies support privacy principles or pose challenges to upholding privacy principles
8. How security and privacy engineering objectives are applied in the context of immersive technologies
9. Risk mitigations for privacy and cybersecurity for immersive technologies
* The role(s) of privacy enhancing technologies (e.g., differential privacy, secure multi-party computation, privacy-preserving federated learning, etc.) in managing risks associated with immersive technologies
1. The extent to which immersive technologies impact the cybersecurity and privacy workforce, including examples of potential benefits and problems
2. The regulatory landscape and the relationship (whether positive or deficient) to managing privacy and cybersecurity risk

*C. Immersive Technology Standards and Risk Management Resources*

Standards and guidelines play a critical role in cybersecurity and privacy. Immersive technologies may break existing cybersecurity and privacy assumptions, requiring adaptation or update to tools and techniques documented in standards and guidelines. Additionally, immersive technologies may warrant new standards and guidelines efforts to complement existing resources. To inform NIST’s understanding of these considerations, NIST seeks comment on the following:

1. The current state of standards and standards development for immersive technologies
2. NIST’s role in supporting development of standards for immersive technologies
3. NIST’s role in supporting effective risk management for immersive technologies through guidelines, resources, and tools

*D. Other Topics and Considerations*

NIST welcomes stakeholder feedback on any other topics and considerations related to immersive technologies.

1. For more information on the relationship between cybersecurity and privacy risk, see, e.g., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (2020), at p. 2. Available at https://doi.org/10.6028/NIST.CSWP.01162020. [↑](#footnote-ref-2)