This award funds the conceptualization phase for the SCiMMA institute, with the goal of providing trustworthy infrastructure allowing the astrophysical community to interoperate.

Multi-messenger astronomy is a new field, combining the efforts of research groups and facilities from around the world, often through proprietary data-sharing agreements that limit which astronomers will participate in a given research effort and in what manner. In such an environment, trustworthiness is central to the adoption of the resulting cyberinfrastructure by the astrophysical community.

The SCiMMA Security Working Group advances the security effort for SCiMMA by defining and guiding development and prototyping efforts while at the same time evolving new strategies and creating new security tooling as SCiMMA evolves.

Overall governance and policies for the security effort are stated in the Master Information Security Policy and Procedures, which was formulated with the help of the Trusted CI organization.

The main thrusts of the Security Working Group are:

- An Identity and Access Management (IAM) capability.
- Fulfilling SCIMMA’s role in the AWS shared security model.
- Identifying and implementing applicable elements of the CIS and OWASP baselines.

The Security Working Group is integrated closely with the project’s agile software development processes for in-house software development.

While, at its best, security is always well integrated with other activities in an organization, the level of interactivity and flexibility employed here was unique in the experience of the security group and may provide a model for security work in other similar projects in the future, as well as a template for ongoing security activities for SCiMMA.