International Workshop
Assessing the Security Implications of Genome Editing Technology

11-13 October, 2017
Herrenhausen Palace ● Hanover, Germany

Instructions for the Breakout Session

The breakout sessions are a critical dimension to meet the workshop goals. Breakout sessions will enable workshop participants to engage in detailed discussion and idea exchange idea about the security implications of genome editing.

As you join in the discussions, please keep in mind the overarching goals of the workshop:

- To launch a proactive, international discussion about what constitutes an evidence-based security concern, outlining the potential near- middle- and long-term security concerns – relating to intentional misuse – that may arise from genome editing applications.
- To describe potential technical, operational, regulatory and governance strategies that may aid the scientific and security communities in preventing or mitigating security concerns
- To develop a network of genome engineering, security studies, and public policy experts to build awareness and facilitate information exchange about common areas of study and concern, and potential communication mechanisms.

CHATHAM HOUSE RULE

In order to encourage open discussion and brainstorming, we kindly ask participants to adhere to the **Chatham House Rule** during the breakout sessions. That is, individuals are free to use the information received in outside activities, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed. Please carefully review the Communication and Social Media Guidelines posted on the workshop website ( )

DISCUSSION TOPICS AND ASSIGNMENTS

Breakout group discussion will take place in Session 2 and Session 4 of the workshop. Each session has four breakout discussion groups on the following topics:

Group 1: Human cells

Group 3: Agriculture

Group 3: Gene drives

Group 4: Microbes

All registrants were invited to sign-up for a breakout session group in advance of the workshop. In most cases, workshop registrants were assigned to their preference of breakout topic. However, please understand that, in order to balance numbers and expertise across the four groups, some participants may be allocated to a group other than their preference. Registrants will be notified of their breakout session at the workshop.

Individuals, who did not sign-up for a breakout session group in advance, will have the opportunity to sign up during the workshop.

BREAKOUT DISCUSSION QUESTIONS

SESSION 2 ASSESSING THE SECURITY DIMENSIONS ASSOCIATED WITH SPECIFIC APPLICATIONS OF GENOME EDITING

1. What are the major security dimensions that have been identified or postulated for this application?
2. How much consensus or disagreement is there about potential security implications with regard to:
    - Timeframe – current, near-, medium, or long-term
    - Feasibility of using this application in this way
    - Accessibility to a range of potential nefarious actors
3. What is the evidence base for identifying security implications? What additional evidence would assist in analyzing and assessing potential risks?
4. What other societal or broader non-technical considerations need to be taken into account as applications are introduced? Are there particular stakeholders groups that should be consulted? If yes, who?

SESSION 4 ADDRESSING AND MITIGATING POTENTIAL SECURITY RISKS ASSOCIATED WITH SPECIFIC APPLICATIONS OF GENOME EDITING

1. Given the potential security implications associated with this application, what are the primary legal, regulatory, and policy approaches that could be applied to address and mitigate them? In addition, are there technical approaches for specific applications that are being or could be developed to address these risks?

2. Are there approaches that seem particularly appropriate for this application? Any approaches that seem particularly inappropriate?

3. If safety or other key considerations emerged in the previous breakout session as a major source of concern, how would addressing those considerations affect the potential security implications associated with this application?