Participant Information Sheet for Security Operators and Managers of Critical Infrastructure Systems

UCL Research Ethics Committee Approval ID Number: **17355/001**

YOU WILL BE GIVEN A COPY OF THIS INFORMATION SHEET

Title of Study: **Modelling for Socio-Technical Security (Modelling and Simulating the Social and Technical aspects of Security in Critical Infrastructure Systems/Organisations).**

Department: **Science Technology Engineering and Public Policy & Computer Science**

Name and Contact Details of the Researcher(s):
Professor Steve Hailes (s.hailes@ucl.ac.uk)
Dr Uchenna Ani (u.ani@ucl.ac.uk)
Dr Nilufer Tuptuk (n.tuptuk@ucl.ac.uk)

Name and Contact Details of the Principal Researcher:
Professor Jeremy Watson (jeremy.watson@ucl.ac.uk)

1. Invitation Paragraph

You are being invited to take part in a Modelling for Socio-Technical Security (MASS) Staff research study. Participation is voluntary. Before your decision, it is important for you to understand why the research is being done and what participation will involve. Please take time to read the following information carefully and discuss it with others if you wish. Be sure you understand everything you read, and if there is anything that is not clear or if you would like more information, please ask us. Take time to decide whether or not you wish to take part. Thank you for reading this.

2. What is the project's purpose?

Security incidents that have affected critical infrastructure systems/organisations reveal the importance of the complex interaction between humans, organisational structures and engineered systems. With Internet of Things (IoT) integrations, studies show that the points of security compromise and failure in critical infrastructures have not always been technical and have included social behaviours related to human and/or organisational traits. For example, how humans engaged with the technical and procedural components of the system. So, addressing security in this type of system will require both social and technical measures equally. This can be more effectively if done early – at the design stage – resulting in the development of more robust IoT-enabled critical national infrastructure

The aim of this project is to investigate how to achieve better security risk monitoring and management in critical infrastructure systems/organisations. The project looks to achieve this by understanding the knowledge and use of the IoT and security modelling & simulation approaches within critical national infrastructure (CNI) systems/organisations. The project also looks to understand if, and how social and technical system attributes are considered and applied in security modelling and simulations. Furthermore, it will investigate how security modelling & simulations tools are being evaluated and validated, understand their maturity within industry, and identify any barriers and enablers for their use in practice.

3. Why have I been chosen?

You have been chosen to participate in this study because you have been identified to be within one of the categories of those who operate or manage the security of a part or whole of the critical infrastructure systems/sectors of focus/interest in this study. Others handle similar roles within critical infrastructure organisations will be/are being approached to also participate in the study. Those who operate and manage security of systems that have no direct integration or link with critical infrastructure components, devices, and systems are excluded from participation. Operators and managers of other functionality aspects not related to security are also excluded.

By speaking to, and hearing from you, we are able to aggregate the necessary information, draw insights, and think about how IoT-integrated cyber-physical systems used in CNI organisations can leverage security modelling & simulation to support better threat monitoring, vulnerability identification, and security risk management. In turn, this can help you, and organisations like yours to do their job better, more securely, and safer.

4. Do I have to take part?

Taking part in the study is entirely voluntary, so it is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep. You will also be asked to sign a consent form attached to this participant information sheet. You can withdraw participation without giving a reason and without it affecting any benefits that you are entitled. You can withdraw anytime during the interview, and withdraw your input 4 weeks after the interview as indicated in the consent form. If you decide to withdraw you will be asked what you wish to happen to the data, you have provided up that point.

5. What will happen to me if I take part?

The research study is scheduled to last for 24 months, and you may be involved in research activities spanning about 2 weeks in total. After your consent to participate is received in writing and documented, your research participation will involve an online one-to-one discussion that takes about 45 minutes to respond to semi-structured interview questions. Your responses to interview questions will not include any special category personal data, but only include your views, experiences, and knowledge related to security management, modelling and simulations. These responses will be recorded, transcribed, and the data analysed qualitatively. The interview will be done via online channels. We would find it helpful to audio-record the interview for reference and analysis of responses, you can still participate in the interview if you choose for the interview not to be audio-recorded, in which case we have to make do with capturing your responses through note-taking.

A one-time cross-engagement workshop is intended which is entirely voluntary to participate besides the interview. The purpose would be to discuss initial study desk-based research findings and engage in a comparative cross insight analysis with analysed interview results. This will be hosted at a more central place in London (if government restrictions on people meeting face-to-face and travelling to work are lifted), and travel expense reimbursed to participants if requested. Otherwise, an online medium will be employed to achieve a similar objective. Your response data can be removed at any point prior to incorporation into analysis and reporting. You may be contacted for future research and related activities, of which participation will be entirely voluntary. Details about the workshop – topic guide, participant information leaflet, and consent form – will be submitted as an amendment once the details are clear in the future.

6. Will I be recorded and how will the recorded media be used?

The audio recordings of your responses and activities made during this research will be used only for the purpose of analysis. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings. We would find it helpful to audio-record the interview for reference and analysis of responses, you can still participate in the interview if you choose for the interview not to be audio-recorded, in which case we have to make do with capturing your responses through note-taking.

7. What are the possible disadvantages and risks of taking part?

The only reasonably foreseeable disadvantage/risks of taking part in this research involves the concern about information disclosure to a third party. To mitigate against this, a research consent form has been provided which states the clear terms for the collection, storage, use, and sharing of the research information from participants. Aspect of data confidentiality are well captured in the consent form.

8. What are the possible benefits of taking part?

Whilst there are no immediate benefits for those people participating in the project, it is hoped that this work will come beneficial to the organisations research participants are affiliated. Participants and their affiliate organisations will benefit first access to the research reports of findings, insights and recommendations that can help them achieve a better depth of reasoning about their organisational security with modelling and simulations. Research participants will benefit from helping to shape future research and solutions on socio-technical security modelling and simulations in critical infrastructure environments.

9. What if something goes wrong?

You can contact the Principal Investigator, Professor Jeremy Watson – jeremy.watson@ucl.ac.uk If you wish to raise a complaint regarding how you are were/being treated or your data was/is being (mis)handled by interviewers and/or researchers during/following your participation in the study.

However, if something more serious occurs following your participation in the project, or you feel your complaints have not been handled to your satisfactions by the Principal Investigator, you can escalate your complaints by contacting the Chair of the UCL Research Ethics Committee – ethics@ucl.ac.uk.

10. Will my taking part in this project be kept confidential?
We assure you that all the responses/information that will be collected during the course of the research will be kept strictly confidential. This means that information about you and your interview responses will be pseudonymised using codes to replace all identifiable information, and the records of the codes will be kept and used. Only the pseudonymised data will be shared with the research team members and used for academic and research purposes. No external/third-party outside of the research team will be used to transcribe the research data. We will ensure that any information we include in aggregated findings; any ensuing reports or publications does not identify you as the respondent. Where necessary, only paraphrased forms of participants' sentences will be used within scientific publication or reports to ensure that no identifiable information is used. You may also decline to answer any question(s) or stop the interview at any time and for any reason. Are there any questions about what I have just explained?

11. Limits to confidentiality
Please note that assurances on confidentiality will be strictly adhered to unless evidence of wrongdoing or potential harm is uncovered. In such cases the University (UCL) may be obliged to contact relevant statutory bodies/agencies. Confidentiality will be maintained as far as it is possible, unless during conversation researchers hear anything that raises concerns that someone might be in danger of harm, researcher might have to inform relevant agencies of this.

Confidentiality will be respected unless there are compelling and legitimate reasons for this to be breached. If this was the case, we would inform you of any decisions that might limit your confidentiality. Confidentiality may be limited and conditional and the researcher has a duty of care to report to the relevant authorities any possible harm/danger to the participant or others.

12. What will happen to the results of the research project?
The data obtained during the research will be stored and archived securely for up to 2 years after data collection – ensuring completion of all planned documentations, reporting, and publications. All collected data will be stored in an encrypted format on encrypted media and in a secure location for the duration of storage period, and subsequently destroyed in line with research data management. Only UCL recommended encryption software will be used. Only the UCL research team will have access to the research data, and these will not be shared with any third parties. Only the UCL research team members may re-use the data for subsequent/related research or to shape future research directions.

In line project plan and deliverable outlines, the results of the research will be disseminated in reports for industries, and publications in articles (conference and journals) for both industry and academy. Typically, this is expected to happen between of 5-7 months after the interview, but it can take longer depending on review process. You will receive information (and links) to gain direct access to copies of published reports and publications, and you will not be identified in any of the reports or publications.

13. Local Data Protection Privacy Notice

Notice:
The controller for this project will be University College London (UCL). The UCL Data Protection Officer provides oversight of UCL activities involving the processing of personal data, and can be contacted at data-protection@ucl.ac.uk

This 'local' privacy notice sets out the information that applies to this particular study. Further information on how UCL uses participant information can be found in our 'general' privacy notice:

For participants in research studies, click here

The information that is required to be provided to participants under data protection legislation (GDPR and DPA 2018) is provided across both the 'local' and 'general' privacy notices.

The categories of personal data used will be as follows:
- Signed consent forms and contact details (name, organisation name, and email addresses) of participants
- Audio-recorded interview expressions of opinions of the participants concerning the specific context of study (IoT and Security Modelling and Simulations)

- Audio-recorded participants' experiences and intentions relative to the study contexts (IoT and Security Modelling and Simulations)
- Transcripts of audio-recorded interviews of participants' expressions of opinions, experiences, and intentions relative to the study contexts.
- Desk-based research and analysis data on socio-technical security modelling approaches.

The lawful basis that would be used to process your *personal data* will be '**Performance of a task in the public interest**'.

Your personal data will be processed so long as it is required for the research project. If we are able to pseudonymise the personal data you provide, we will undertake this and will endeavour to minimise the processing of personal data wherever possible.

If you are concerned about how your personal data is being processed, or if you would like to contact us about your rights, please contact UCL in the first instance at data-protection@ucl.ac.uk.

The research data will not be shared or transferred to any recipient(s) outside of the EEA

14. Who is organising and funding the research?
The MASS (Modelling for Socio-Technical Security) project is part of the PETRAS National Centre of Excellence for IoT System Cybersecurity catalyser projects funded by the Engineering and Physical Sciences Research Council (EPSRC).

16. Contact for further information
You should give the participant a contact point for further information. This can be your name, address and telephone number or that of another researcher in the project (if this is a supervised-student project, the address and telephone number of the student's supervisor).

Remember, as a participant in the research, you should receive a copy of this information sheet. You are also required to keep a signed copy of the consent form for your record and future reference.

For any further information, you may reach a member of the research team using the following contact details:

Dr Uchenna D Ani
PETRAS National Centre of Excellence for IoT Systems Cybersecurity
Department of Science, Technology, Engineering, and Public Policy
University College London (UCL)
Shropshire House
11-20 Capper Street
London
WC1E 6JA
Tel: +44(0)20 3549 5155

OR

Dr Nilufer Tuptuk
Department of Computer Science
University College London (UCL)
Gower Street, Bloomsbury
London
WC1E 6EA
Tel: +44 20 3108 7118

Thank you for reading this information sheet and for considering taking part in this research study.