SECURITY POLICIES AND PROCEDURES: ARK and TGSN have implemented strategic communications projects in Syria since 2012 and 2013 respectively, and CMC has been carrying out M&E activities in Syria for the last two years. The consortium is acutely aware of the risks this project runs, given an operating context in Syria where any effective moderate opposition or FSA body risks being targeted by armed extremist groups or by the regime and its proxies. Given the potential risks involved in this project, the consortium's highest priority will be staff and beneficiary safety and security, encompassing both physical and mental welfare. All companies in the consortium have demonstrated that they are able to manage the risks inherent in operating in a conflict area, handle incidents quickly and responsibly, and run projects discreetly and effectively.

STAFF AND PARTNER SECURITY: Given the consortium's existing portfolio in Syria, it fully understands the risks involved in this project and all three companies work with Syrian partners and beneficiaries who would be undertaking these types of activities, regardless of the consortium's involvement. Staff and partners are fully supported with appropriate security briefings throughout the project, and additional training and equipment is provided as required. Security and risk management standard operating procedures are documented and available for HMG review. ARK and TGSN carry out regular security reviews of their operations and physical office locations, and office location details are restricted to relevant ARK, TGSN and HMG staff. ARK and TGSN have strong working relationships with HMG and their project leads already raise security issues to HMG as required. For example, ARK has developed detailed security Standard Operating Procedures (SOPs), which it has shared with HMG to provide examples of best practice, while TGSN has made trauma support available to all staff and has invested in training one female member of staff as a trauma trainer. Security and safety of staff conducting field research is also the highest priority for CMC and its local partner EMI. The main approach to risk mitigation is situational awareness and relying on a broad network of local contacts with a deep understanding of the context on the ground, but CMC will also conduct a tailored risk analysis and develop a risk mitigation plan in conjunction with EMI before it commences any field work under this project. CMC project staff have received relevant UK-based hostile environment training (HEAT, HEST) and all staff involved have taken online awareness trainings at a minimum and receive extensive, regular and up-to-date security briefings through EMI's management. This procedure and process has been successfully applied during recent assignments inside Syria with the same CMC/EMI team. Taking do-no-harm seriously means not taking unnecessary risks and erring on the side of caution. Should there be any credible information as to unusual or additional security risks, field work will either be postponed or changed to a remote approach (such as use of phone calls instead of face-to-face interviews).

The consortium takes detailed measures to ensure that partner safety and security are not compromised by their participation in existing projects, which would continue with the project's award, with all outputs remaining unattributable to the UK. Both ARK and TGSN have been implementing protective strategies for members of their platform, production and dissemination networks for years and have extensive experience anonymising personal stories without losing the importance of the information or emotion being conveyed. All communications with staff and partners inside Syria are carried out through platform-linked rather than company emails to ensure that safety would not be compromised by any leak associating them with a Western government-backed project. Staff and partners working with the consortium are well aware of the potential risks involved in parts of the project, and as a result, adhere to the security guidance they are provided with. Partners are provided with quarterly reminders in physical and IT security policies. Both ARK and TGSN project management teams review key products prior to release to ensure that they do not pose an increased risk to individuals or groups and stringers are briefed to make all interviewees aware that they may appear online or on satellite broadcast channels and to ensure that they participate freely.

ONGOING RISK MONITORING: Risk management is an integral component of effective programming across all aspects of the consortium's activities. The operational security risk register, which will build on the risk assessment included in this response, will be reviewed in the project team's weekly meetings. This incorporates specific risk and contextual information from staff, partners, beneficiaries, networks and donor governments, as well as ongoing open source media monitoring. ARK has a Head of Physical and IT Security with 15 years of experience working in the UK Military Special Forces and four years working

with ARK on Syria programming. He will continue to work closely with the project director and the management team to ensure all security risks are appropriately identified and mitigated.

INCIDENT RESPONSE: Routine security issues will be communicated to project staff and partners by WhatsApp/Viber, and in the event of a significant incident, a cascading emergency call tree structure will be in place to ensure that all staff can be accounted for and provided with specific instructions on how to respond to the incident. All ARK-issued phones and laptops have Meraki software installed that is used to geo-locate these devices in the event that staff members cannot be contacted. This software also enables all data to be wiped from phones and laptops remotely, if required. ARK and TGSN have media handling procedures ready in the event of public interest in response to an event.

In the event of a significant incident affecting either project strand or any part of the consortium, the project management team will meet to assess the situation, review existing security protocols and provide required actions and advice to all relevant employees, beneficiaries and donors. An incident report will then be generated and logged, including initial response and subsequent mitigating actions. Incidents will be grouped into relevant security domains (for example, Physical or Cyber) and analysed post-event to look for specific trends that may affect programming or staff safety. This enables the consortium's senior management teams to devise additional mitigating strategies to limit impact. Both ARK and TGSN have already handled a wide range of risks, including targeting of staff and platforms.

COMMUNICATION WITH HMG PROJECT MANAGERS: This project will be run out of Istanbul, where both ARK and TGSN have offices (through their Turkish legal entities) and where CMC's Project Manager (full-time) and Team Leader (part-time) will be based. ARK also has offices in Amman, Beirut and London a footprint which ensures redundancy and flexibility in the event that security issues (related either to the project specifically or to issues relating to the host country) prevent project teams from operating. This laydown also enables the team to communicate regularly with HMG project managers face-to-face. The consortium will provide copies of its security operating procedures to HMG at the start of the project and will ensure that any changes are briefed into the HMG project team. The consortium will also be available to provide a detailed overview of SOPs for the project following contract award. ARK and TGSN project managers are currently in regular contact with the HMG project team via email, secure messaging and telephone, maintaining a continuous dialogue about all project-related issues.

CYBER SECURITY: ARK invests heavily in IT Security across all areas, including its corporate back office, delivery teams and third party partners. Its layered approach focuses on protecting end-point devices and network boundaries, as well as policies and procedures to define what users can and cannot do, and a continuous training and awareness cycle to maintain a high-level understanding of the cyber threat landscape. All ARK data is stored remotely on the dark cloud, ensuring that in the event of loss or damage of equipment, no information is stored on laptops. ARK staff are able to identify and report suspicious activity against themselves and the company. As a result of the stringent IT security systems in place, ARK has been able to successfully repel multiple attacks against its network.

TGSN-run platforms on the MAO project have repeatedly come under attack from highly-capable hostile forces. As such, TGSN has prioritised IT security, with all configurations periodically tested to ensure they are appropriate and efficient. All hardware is fully encrypted and all staff have been given cyber security training and have been issued ESET software to minimise risk. Refresher cyber security courses and systems checks are run periodically, and similar IT support is provided to key Syrian partners and TGSN's in-country outreach & training centres.

CMC employs strict security protocols for IT security, monitoring and assessing threat levels on an ongoing basis and assigning adequate measures, including encryption of hardware and communication. The team is trained and experienced in handling sensitive, confidential and personal information obtained through field work, including interview material and protocols and names of training course participants and research subjects.