GRANTEE SECURITY: SOME ASSEMBLY REQUIRED

A GUIDE TO HELPING GRANTEES WITH THE BLUEPRINTS OF SECURITY

YOUR GRANTEES' SECURITY NEEDS

Talk with your grantees about their priorities. These might include:

○ **Training staff** in personal security, security management, first aid, defensive driving, and IT.

○ **Evaluating trainings** to assess whether they are useful and what additional support might be needed.

○ Developing **security policies and plans.**

○ Enhancing **physical security at the office.**

○ Addressing **IT security needs.**

LAYING THE GROUNDWORK

QUESTIONS TO ASK	GOOD PRACTICES
○ How does the grantee define security? Does the definition include office, IT, travel, and personal security?	○ The grantee defines security holistically, incorporating security and protection into program planning and activities.
○ Does the grantee discuss security issues in your meetings, proposals, or other communications?	○ The grantee should engage with you on this topic and not just about funding. A meaningful discussion about security maintains a trusting relationship and reflects the reality in the field.
○ Does the grantee talk openly or reluctantly about security? Why?	○ Grantees should see security incidents as opportunities to learn and improve security management. Grantmakers should foster open communication – even about failures.
○ Has the grantee conducted security training for staff in in the last 3 years?	○ Regular training on personal and communications security provides critical knowledge before an incident occurs.

DRAWING UP THE PLANS

Security planning raises questions. which should grantmakers ask, and what should the end product look like?

QUESTIONS TO ASK	FINISHED PRODUCT
○ Do you have security policies? Is security included in budgets? How do you carry out risk assessments?	○ Ideally, the grantee has developed a structured approach that includes dedicated resources, assessments of threats and vulnerabilities, and regular planning to mitigate the identified risks.
○ Do you have a protocol for when a security incident occurs? If yes, what is it, and what changes as a result of the incident?	○ The grantee has developed a protocol for the most likely security incidents (e.g., staff detained, office break-in). After an incident, protocols are reviewed and updated to include lessons learned.just about funding. A meaningful discussion about security maintains a trusting relationship and reflects the reality in the field.
○ How do you organize a sensitive meeting or event safely?	○ The grantee knows how to recognize threats and adapt security protocols (location, timing, participants, and visibility) based on the potential sensitivity of its activities.
○ Do you proactively network with authorities and other organizations to "cultivate" sympathizers and support in the case of need?	○ The grantee has developed a safety net by identifying allies who could provide information or be called upon to help in crisis situations.

Updated in 2018, developed in 2014 by Alexandre Carle, OTHER
SOLUTIONS Consulting, Katie Skartvedt and Catherine H. Townsend

GRANTEE SECURITY: SOME ASSEMBLY REQUIRED

A GUIDE TO HELPING GRANTEES WITH THE BLUEPRINTS OF SECURITY

SOUND SECURITY MODELS

QUESTIONS TO ASK	SOUND MODELS
○ **Physical security:** What measures have you taken to secure your offices? (guards, closed-circuit television (CCTV) cameras, alarm systems)	○ Physical security should go beyond just a guard at the door. Grantees should also secure IT hardware, manage trash, and take steps to avoid break ins.
○ **Travel security:** How do you prepare staff for field missions? (risks assessment with supervisor, check-in protocols and post-travel assessments)	○ The grantee should make field contact prior to travel, evaluate risks of the mission, document travel plans, institute a check-in procedure, and identify safe havens. A meaningful discussion about security maintains a trusting relationship and reflects the reality in the field.
○ **IT security:** How do you manage IT security? (passwords for computers and phones, server back-up, online server, avoid carrying sensitive data)	○ IT protocols require strong passwords on all devices, anti- virus software on all computers that is regularly updated, and periodic data back-ups to cloud-based storage or an encrypted flash drive. Staff is trained on digital security.
○ **Well-being:** How do you support health and wellness for the staff? Do you have resources and networks to support staff dealing with trauma?	○ Grantees should openly acknowledge the importance of personal well-being and support staff in managing stress and the “compassion fatigue” often associated with human rights advocacy.

Updated in 2018, developed in 2014 by Alexandre Carle, OTHER SOLUTIONS Consulting, Katie Skartvedt and Catherine H. Townsend