Guidance for Discussing Security with Grantees

General approach to security	Good practices
✓ How does the grantee define security (IT, physical, travel?)	Holistically, with security considerations incorporated into program planning and activities.
✓ Does the grantee engage/inform with you about security in your meetings, proposals or other communications?	The grantee should engage the grantmaker, and not just about funding needs. 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?	Open communications. Rather than failures, organizations should see security incidents as opportunities to improve security management.
✓ Has the grantee trained staff in security in the last 3 years?	Training on personal and communications security at the very minimum.
✓ Does the grantee proactively network with authorities to “cultivate” sympathizers and support in the case of need?	Developing a safety net by identifying allies who could provide information or be called upon in emergencies is critical.

Specific questions	Good practices
✓ **Security planning**: Do you have security policies? Is security included in your budgets? Do you carry out risk assessments?	A structured approach—which includes dedicated resources, a threats, vulnerabilities and risks assessment, and adequate planning to mitigate the identified risks—is ideal.
✓ Do you have a protocol for when a security incident occurs (if yes, what is it, and what changes as a result of an incident)?	Grantee has developed a protocol for the most likely security incidents (staff detained, office break-in). After an incident, protocols are reviewed and updated to include lessons learned.
✓ 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.
✓ **Physical security:** What types of measures have you taken to secure your offices (i.e. guard, CCTV, anti-burglary system)?	Physical security should be more than just a guard at the door. Organizations should consider CCTV, securing IT hardware, managing trash, and avoiding break ins.
✓ **Travel security:** How do you prepare staff for field missions (risks assessment with supervisor, check-in protocol)?	Grantees should document travel plans, evaluate risks related to the context and mission, institute a check-in procedure, make field contact prior to travel, and identify safe havens.
✓ **IT security:** How do you manage IT security (passwords for computers and phones, server back-up, online server, avoid carrying sensitive data)?	IT protocols are in place. Strong passwords are used on all IT devices, documents and data are backed up regularly and to a remote server, staff are trained to secure their data, strong anti-virus software (not just a free version) is installed and updated on all computers.

What are the priority security needs of the grantee?

- Staff training (IT, personal security, security management, first aid, defensive driving): How does your organization evaluate trainings and assess whether they are they useful (or not)?
- Developing a global security policy
- Reinforcing physical security at the office
- Addressing IT security needs

Developed by Alexandre Carle, OTHER SOLUTIONS Consulting, acarle@othersolutions.eu, Katie Skartvedt, kskartvedt@wellspringadvisors.com, and Catherine H. Townsend chtownsend@wellspringadvisors.com