ADS Chapter 573

Partner Liaison Security Offices

New Edition Date: 12/14/2017
Responsible Office: SEC
File Name: 573_121417

Functional Series 500 – Management Services
ADS 573 – Partner Liaison Security Offices
POC for ADS 573: Nancy Aposporos, naposporos@usaid.gov

This is a new ADS chapter.

Table of Contents

573.1 OVERVIEW 3

573.2 PRIMARY RESPONSIBILITIES 4

573.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES 5

573.3.1 Establishment of Partner Liaison Security Offices 5

573.3.2 Functions of Partner Liaison Security Offices 6

573.3.3 SEC Support for Partner Liaison Security Offices 8

573.3.4 Partner Liaison Security Office Relationship with the Regional Security Office 9

573.3.5 Conclusion 9

573.4 MANDATORY REFERENCES 9

573.4.1 External Mandatory References 9

573.4.2 Internal Mandatory References 10

573.5 ADDITIONAL HELP 10

573.6 DEFINITIONS 10

ADS 573 - Partner Liaison Security Offices

573.1 OVERVIEW

Effective Date: 12/14/2017

USAID is increasingly being called upon to implement stabilization, development, and reconstruction programs in countries and regions identified by the Department of State, Diplomatic Security Service (DSS) as High Threat Posts (HTPs), as well as other countries and regions with challenging operating environments. In these areas, the need for a consistent and appropriate level of safety and security support for the Agency's Implementing Partners (IPs) is critical. To address this need, USAID Missions, in consultation with Chiefs of Missions, should consider the establishment of a Partner Liaison Security Office (PLSO).

The basic function of the PLSO is to act as a liaison to and facilitate communications between the IPs in order to enable the IPs to better use and share publically available security information so that the IPs are better informed about their own security. Liaison activities include maintaining coordination with pertinent in-country entities such as the United Nations, international NGOs, the host government, and other international donors for the purpose of sharing and aggregating security information among partners working in the same environment.

As outlined in **2 FAH-2-110**, USAID's IPs do not fall under Chief of Mission (COM) authority. Post is not required to provide security for IPs as it does for U.S. Government employees. While IPs are ultimately responsible for the safety and protection of their employees and programs, the PLSO provides safety and security related support to USAID's IPs, regardless of their organization's country of origin. The PLSO serves in a coordinating and information sharing role helping to disseminate open source information and promote security best practices. The PLSO must always respect the security philosophies and policies of each IP and all guidance will be non-prescriptive in nature. IP participation with the PLSO is voluntary and each IP can determine how or if the information provided by the PLSO is used.

Information provided by the PLSO will be open-source and non-prescriptive in nature, and will not contradict the messaging provided by the U.S. Embassy. PLSOs are permitted to disseminate open source information that is publicly available. This restriction ensures PLSOs do not violate any aspects of **7 FAM 050, Consular Information Program, Messages for U.S. Citizens, and the no double standard policy**. All disseminated PLSO information will be shared with the Department of State's Overseas Security Advisory Council.

The PLSO program is a Mission-funded endeavor. Typically, program funds are used to finance PLSO operations due to the support that PLSOs provide to IPs. The PLSO also ensures that the USAID Mission and the broader COM community benefit from the increased visibility of the operational environment where IPs are delivering U.S. Government funded assistance.

573.2 PRIMARY RESPONSIBILITIES

Effective Date: 12/14/2017

a. The **Director, Office of Security (DIR/SEC)** supports Partner Liaison Security Offices (PLSOs) established at Missions.

b. The **Office of Security, International Security Programs (SEC/ISP)** assists Missions in the establishment of PLSOs and provides oversight of and guidance to PLSOs, as requested by the Mission, following initial formation.

c. The **Partner Liaison Security Office (PLSO)** collects and disseminates open source safety and security related information from/to the Mission's Implementing Partners (IPs). The PLSO coordinates security efforts with the appropriate Mission staff and the IPs and provides updates through the EXO to the USAID Mission Director, the Contracting/Agreement Officer, SEC, and applicable geographic and functional Bureaus regarding all matters related to the security of Mission IPs. The PLSO supports the IP in the dissemination of security information, and is not a replacement for an IP's security measures, or a primary source of security intelligence for IPs.

d. The **Mission Director (MD)** may establish a PLSO in accordance with identified criteria and ensure the PLSO provides IPs with operational security support commensurate with the environment. This includes all IPs in the field providing development and humanitarian support regardless of whether they are funded by the Mission or via a centrally-funded mechanism. Additionally, the Mission Director or their designee will inform all of the Mission's Implementing partners of the functions of the PLSO and the IP relationship to the PLSO. The Mission Director will ultimately determine the entity to which the PLSO reports. Typically, the PLSO reports to the Executive Officer as Mission security responsibilities fall under EXO duties, as indicated in **ADS Chapter 527, Functions of the Mission Executive Officer**.

e. The **Executive Officer (EXO)** assists Mission Directors in establishment, oversight, and administration of the PLSO. EXOs are responsible for day-to-day PLSO operations. The EXO, with administrative oversight and as the Unit Security Officer (USO), has general oversight and assists in the implementation of the USAID security program within the overseas Mission. This includes support to IPs as outlined in **ADS Chapter 527, Functions of the Mission Executive Officer**.

f. The **Mission-based Contracting/Agreement Officer (CO/AO)** and **Contracting Officer's Representative/Agreement Officer's Representative (COR/AOR)** consult with the PLSO on security-related requirements prior to their inclusion in award terms and conditions. If so delegated, the COR/AOR monitors compliance with all other security-related award terms and conditions. For Washington-based mechanisms, Activity Managers at Missions may be responsible for carrying out some of the above-described COR/AOR duties.

g. The **Resident Legal Officer** advises the Mission on the proper hiring mechanisms to staff the PLSO, assists in drafting notices and guidance to IPs on

security matters, advises on options available to the USG for helping to ensure IP security, and helps to ensure that PLSO engagement with IPs does not result in the appearance of any assumption of liability by the Mission.

573.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

573.3.1 Establishment of Partner Liaison Security Offices

Effective Date: 12/14/2017

Recognizing the varying needs and conditions at Post, Missions have significant discretion and authority when establishing a PLSO. The Office of Security is available to support Mission efforts in the establishment of a PLSO. In addition, Missions have numerous options regarding PLSO hiring mechanisms and models for staffing implementation. PLSOs may consist of Direct-Hires, Personal Service Contractors, eligible family members, or institutional contractors. The model selected will have implications for the functions the PLSO may perform, and Missions must decide which mechanism will best meet the needs of the Mission.

If the Department of State (DOS) Diplomatic Security Service (DSS) designates a Mission as a High Threat Post (HTP), SEC highly recommends that the Mission establish a PLSO. The DSS maintains the list of Posts to which this designation applies. The HTP list is designated as Sensitive But Unclassified. The current list can be obtained from SEC/ISP by calling (202) 712-0990 or (202) 712-5609.

Missions that don't fall under the DOS HTP designation may elect to establish a PLSO to assist with providing a consistent and appropriate level of safety and security support. The following factors may be relevant in determining the need for a PLSO:

a. Sustained elevated risk of violence and crime in the areas where the Mission is executing programming.

b. A lack of host government desire to provide a response and/or a lack of host government capability to provide a military/law enforcement response to a critical incident involving a USAID partner.

c. Limited ability for Implementing Partners to safely travel and operate in the local environment and to securely and effectively implement or facilitate respective projects.

d. Limited ability for Mission staff to safely travel in the local environment and to securely and effectively monitor and evaluate Mission programs.

e. The Crime, Political Violence and Terrorism designations for the Mission's operating environment, as indicated on the DSS Security Environment Threat List (SETL), are high and/or critical.

f. Host government instability and its lack of support to the U.S. Government, specifically USAID activities.

g. Any combination of the above factors or any other security condition negatively impacting the effective implementation or monitoring of Mission programs/projects.

Once the Mission Director determines the need for the establishment of a PLSO, Missions must coordinate with SEC/ISP. This coordination includes, but is not limited to, advising on Mission security needs, reviewing draft Mission PLSO policies, and assisting with implementation of the PLSO program.

SEC/ISP review and clearance approval is required prior to the issuance of PLSO vacancy announcements or PLSO scopes of work (SOW), and at least one SEC/ISP officer must be present on the PLSO Technical Evaluation Committees (TEC), where applicable.

573.3.2 Functions of Partner Liaison Security Offices

Effective Date: 12/14/2017

The scope of responsibilities of the PLSO is determined by the size, needs, and available budget of the Mission; the number and needs of the IPs; and the security operating environment. SEC/ISP will make recommendations to the Mission regarding the functions and deliverables of the PLSO. The Mission Director, or their designee, retains the authority to make the final determination.

The PLSO will ensure that no information provided to the IPs is prescriptive in nature. However, the PLSO will refer IPs to their COR/AOR regarding any changes the IPs would like to make to their security plans/postures based on information provided by the PLSO. While the PLSO may not approve the security plans of an IP, the PLSO will be available to advise the CO/AO and COR/AOR concerning any such requested changes.

The PLSO will facilitate IP access to the in-country Overseas Security Advisory Council (OSAC) as well as work to identify other potential sources of information and security support available to IPs. The PLSO will also liaise with Post’s Regional Security Office (RSO) on security-related matters.

The PLSO will work in a non-prescriptive advisory capacity and provide holistic security and safety related support to IPs, as determined by the Mission Director or their designee. The PLSO must abide by **7 FAM 052**. All "duty to warn" threat notifications made to U.S. private sector organizations at Post must be coordinated with the Bureau of Diplomatic Security, Threat Investigations and Analysis, Overseas Security Advisory Council (DS/TIA/OSAC) to ensure that a simultaneous or near-simultaneous threat warning is also conveyed to the domestic headquarters of the U.S. organization.

The PLSO may perform any combination of the following functions:

a. In conjunction with the EXO, OAA, and SEC, and M/CIO develop and maintain a notification system (i.e.: email, SMS, texting, etc.) or a similar type of communication. This system can disseminate emergency information to an IP's Security Manager or Security Focal Point to ensure the PLSO can notify and receive staff accountability and updated incident information from IPs during emergency situations.

b. Establish and manage an IP security incident reporting system to disseminate information to the Mission, DOS Regional Security Officer (RSO), SEC/ISP, IPs, and other individuals and groups with a need-to-know in a timely manner for situational awareness. The PLSO will file the incident information for the duration of the IP's contract or grant. If incident information is disseminated to the IP community, the report will be sanitized so the source of the information is not revealed.

c. Conduct trend analysis based on information collected, to be disseminated to, and for the benefit of, IPs.

d. When another established review process is not already in place, review and provide feedback on security plans provided by IPs to the CORs/AORs, re-reviewing security plans as appropriate over time and as security conditions on the ground change. PLSOs may also archive and keep files of security plans. As noted above, however, IPs will maintain sole responsibility for their security plans and the security of their local staff, and PLSOs and USAID assume no liability for IP security as a result of any such review or feedback.

e. Upon significant changes in the country threat environment, the PLSO may provide non-prescriptive guidance/advice to IPs via the CO/AO regarding security upgrades. PLSOs must avoid making unauthorized commitments. Any discussions involving the potential for increased costs must include the CO/AO to facilitate any necessary CO/AO approvals.

f. If allowed by the mechanism used to fulfill the PLSO position(s), the CO/AO may request that the PLSO participate on TEC panels and/or provide the CO/AO feedback on security plans submitted as part of solicitations.

g. Advise the Mission Director, EXO, CO/AO, other senior USAID personnel, SEC/ISP, the Regional Security Office (RSO), and other individuals or groups with a need-to-know on all security matters pertaining to IPs.

h. Serve as a member of the in-country Overseas Security Advisory Council (OSAC).

i. Provide electronic or verbal security briefings and training to newly arrived USAID employees, IPs (e.g., at Post-award orientation conferences), IPs already in-country, and IP staff who are TDY, as requested.

j. Provide a weekly activity report to the MD, EXO, CO/AO, COR/AOR, and SEC/ISP containing pertinent security-related information provided to IPs as well as security incident information reported by IPs.

k. Hold regular meetings with IPs and Mission entities with a vested interest to focus on security issues affecting the IP community. The PLSO may also attend regularly held meetings with Mission security entities, when possible.

l. Visit IP offices and project sites to execute security assessments, as requested by IPs. The PLSO will provide findings and any non-prescriptive recommendations to the CO/AO and COR/AOR.

m. Provide the CO/AO with accurate and up-to-date security information for inclusion in solicitations and assist with responses to questions regarding Mission security requirements/mandates/guidance.

n. Provide other services as determined by the Mission, in consultation with SEC, to be prudent and necessary.

All information disseminated by the PLSO must be unclassified, and must have appropriate caveats and disclaimers on how the information can be used to ensure the information is not construed as a directive. The Mission's Resident Legal Officer and Contracting/Agreement Officer must clear these caveats.

573.3.3 SEC Support for Partner Liaison Security Offices

Effective Date: 12/14/2017

SEC/ISP assists Missions in the establishment of PLSOs and provides oversight and guidance by:

a. Providing TDY support to Missions that establish a PLSO to help determine the needs of the Mission and IPs and to develop the structure and functions of the PLSO.

b. Assisting the Mission with drafting PLSO position descriptions or Statements of Work which will reflect IP needs in the security operating environment.

c. Assisting the Mission with PLSO candidates' selection by serving on the Technical Evaluation Committee panel, if requested by the Contracting Officer.

d. Depending on the mechanisms used to staff the PLSO, SEC/ISP will provide the PLSO with initial on-site training.

e. Conducting thorough programmatic assessments of the PLSO on a yearly basis and providing findings to the Mission Director, SEC, and others with a need-to-know.

f. As it is received at SEC headquarters, providing timely, pertinent security-related information to the PLSO.

g. Distributing PLSO “best practices” information between PLSO Missions.

h. Providing other PLSO-focused security support, as required.

Missions interested in the establishment of a PLSO should contact SEC at (202) 712 -0990.

573.3.4 Partner Liaison Security Office Relationship with the Regional Security Office

Effective Date: 12/14/2017

PLSOs work very closely with the Regional Security Office (RSO) to ensure full understanding and support of the program. RSOs view the PLSO as an asset and a force multiplier for the dissemination of safety and security information. PLSOs provide real-time security information to the RSO from on-the-ground sources in typically isolated IP locations. This type of information allows the RSO to have a greater operational picture and increase the overall security of a broader Chief of Mission (COM) community.

The RSO’s mandate is the safety and security of Chief of Mission staff. While RSOs occasionally provide support to USAID IPs, their primary mission is the Embassy and U.S. Government constituents.

573.3.5 Conclusion

Effective Date: 12/14/2017

The PLSO does not have the authority to order IP action or compliance pursuant to PLSO recommendations. The PLSO will never direct IPs to take action or not take action. PLSOs will only disseminate publicly available information to IPs and will not provide information that would result in an unfair advantage to the IP. However, IPs retain autonomy on how to best utilize the information provided.

573.4 MANDATORY REFERENCES

573.4.1 External Mandatory References

Effective Date: 12/14/2017

a. 2 FAH-2 H-110, Chief of Mission Authority and Overseas Staffing

b. 14 FAM 240, Critical Environment Contracting

c. Federal Acquisition Regulation, 1.601, Contracting Authority and Responsibilities

d. **Federal Register, Volume 76, Number 161, Contractors Providing Private Security Functions**

e. **National Defense Authorization Act for FY 2013, section 846**

573.4.2 Internal Mandatory References
Effective Date: 12/14/2017

a. **ADS 101, Agency Programs and Functions**

b. **ADS 200, Development Policy**

c. **ADS 302, USAID Direct Contracting**

d. **ADS 561, Security Responsibilities**

e. **ADS 562, Physical Security Programs (Overseas)**

573.5 ADDITIONAL HELP
Effective Date: 12/14/2017

There are no additional help documents for this chapter.

573.6 DEFINITIONS
Effective Date: 12/14/2017

See the **ADS Glossary** for all ADS terms and definitions.

award
A form of an implementing mechanism through which USAID transfers funds to an implementing partner, generally selected through a competitive process, resulting in a contract, grant, or cooperative agreement. (**Chapter 200** and **573**)

High Threat Post
A country, city, area, sub-region, or region in which USAID is hindered from accomplishing its mission due to security risks, such as specific targeting of U.S. interests; a favorable operating environment for terrorist groups; intelligence indicating an imminent threat; or other risk factors as identified by SEC, the RSO, or other U.S. Government officials in consultation with the RSO. (**Chapter 573**)

need to know
A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform official duties. The determination is not made solely by virtue of an individual's office, position, or security clearance level. (**Chapter 545, 569, 573**)

Partner Liaison Security Office
A USAID Mission entity that provides safety and security support to USAID Implementing Partners through proactive engagement including meetings, site visits, and other communications. The PLSO assists with monitoring critical security information. (**Chapter 573**)

Security Environment Threat List
List of countries with U.S. diplomatic Missions compiled by the Department of State and updated semiannually. The listed countries are evaluated based on transnational terrorism; political violence; human intelligence; technical threats; and criminal threats. Threat levels for each of these four categories are designated as critical, high, medium, or low. (**Chapter 573**)

573_062722