12 FAM 420
POST SECURITY MANAGEMENT

(TL:DS-93; 10-22-2003)
(Office of Origin: DS/PPB/PPD)

12 FAM 421 CHAIN OF COMMAND

(TL:DS-66; 03-07-2000)

a. The regional security officer is responsible to the Assistant Secretary of State for Diplomatic Security and to the chief of mission at Foreign Service posts for implementing the Department's security program abroad.

b. The regional security officer (RSO) or post security officer (PSO) and their staff are subject to the administrative direction of the chief of mission or principal officer in countries assigned, or where they are detailed on official temporary duty.

c. The deputy chief of mission is the direct supervisor and designated rating officer for the senior regional security officer at post. The designated reviewing officer for the senior RSO is the ambassador. RSOs will rate their immediate subordinates who will be reviewed by the DCM. At constituent posts, RSOs report directly to and are rated by the principal officer. The senior RSO in country is the reviewing officer. (See 3 FAH-1 H-2813.3, For Regional Personnel.)

d. All RSOs report to the Director of the Diplomatic Security Service (DS/DSS) through the Director of Overseas Operations (DS/DSS/OP).

12 FAM 422 REGIONAL SECURITY OFFICER (RSO)

12 FAM 422.1 General

(TL:DS-93; 10-22-2003)

a. The regional security officer (RSO) is a U.S. Foreign Service security officer serving abroad at an embassy or consulate who is responsible for implementing and managing the Department's security programs for a geographic region which includes at least one Foreign Service post. RSOs are resident at a particular post and may have constituent posts within their region for which they are responsible. The day-to-day management of security programs at their constituent posts is the responsibility of a post security officer (see 12 FAM 423.4).

b. The responsibilities and duties of an RSO are enumerated in the following sections, although some specific elements may be reallocated to other post personnel by the chief of mission in accordance with 2 FAM 110. If the chief of mission changes duties *of the RSO*, *the* RSO should notify DS/DSS/OP.

12 FAM 422.2 Security Briefings

(TL:DS-39; 08-15-1994)

RSOs, PSOs, and security officers provide security briefings at post directed primarily toward maintaining a high level of security awareness on the part of post employees by providing the necessary knowledge of specific security regulations, procedures, and techniques. See 12 FAM 424 for types of briefings.

12 FAM 422.3 Reporting

(TL:DS-39; 08-15-1994)

a. See 12 FAM 426 for RSO reporting requirements to DS/DSS/OP.

b. At all posts without a resident RSO, the PSO will send copies of all correspondence relating to the post's security programs to both DS/DSS/OP and the responsible RSO.

12 FAM 422.3-1 Reporting Security Incidents

(TL:DS-74; 04-04-2001)

a. PSOs will immediately report to the responsible RSO and to the Bureau of Diplomatic Security (DS/DSS/OP) all incidents that could affect a post's security status adversely.

b. Information security incidents involving the possible or actual compromise of classified information (see 12 FAM 550) will be reported immediately (within 24-hours) to DS/ISP/APB via DS channels. Initial reports must be entitled "POSSIBLE SECURITY COMPROMISE—(DATE OF INCIDENT)", and include, if available:

(1) Summary of the incident;

(2) Circumstances of discovery;

(3) Name of suspected violator;

(4) Highest classification of material involved;

(5) A list of compromised material;

(6) Action taken by RSO to negate further unauthorized disclosure of material; and

(7) The RSO's assessment of the degree of compromise.

c. Follow-up reports will include the following information, at a minimum:

(1) Additional information since the initial report;

(2) Status of post's damage assessment; and

(3) Any requests for DS/ISP/APB assistance.

12 FAM 422.3-2 DS Channels—General Guidance

(TL:DS-93; 10-22-2003)

a. DS channels caption messages provide control over communications between DS and a regional security officer (RSO) or *the post security officer (PSO)* on security matters of a highly sensitive nature and will be used only for this purpose. The strictest need-to-know principle applies to such communications. The need-to-know principle does not relieve the security officer of the obligation to keep the principal officer, or other responsible officers, informed of matters of genuine official interest relating to personnel or operations of any post under the general supervisory jurisdiction of the chief of mission. *Since telegram distribution is appropriately restricted to the RSO at post, sharing such information with the chief of mission (COM) should be person-to-person to preclude disclosure to others*. (S*ee 5 FAH-2 H-444.*)

b. The DS channel is used for telegrams between the Assistant Secretary and/or Deputy Assistant Secretaries of Diplomatic Security, and other appropriate DS personnel, and the responsible DS officer concerning criminal investigations involving U.S. citizens or foreign nationals, who are not U.S. Government employees; special protective equipment; and other sensitive subjects which the drafter deems should be restricted to DS personnel at posts or within the Department. RSOs must ensure that communication program unit (CPU) distribution is in accordance with 5 FAH-2 H-444. The Executive Director for Diplomatic Security (DS/EX) authorizes access to DS Channel message traffic at the headquarters level. This caption may be used laterally in the field. Use ASEC as the only TAGS on this message traffic. (See 5 FAH-2 H-444.)

(1) The Diplomatic Security Background Investigations (DSBI) channel is to be used exclusively by RSOs for cable reporting of information (derogatory and non-derogatory) developed during the course of background investigations (BI) or periodic reinvestigations (PRI) to the Personnel Security and Suitability Division of Diplomatic Security (DS/SI/PSS) and other RSOs. This channel restricts, for Privacy Act reasons, distribution of cable reporting only to RSOs and DS/SI/PSS; creates a direct channel of communications between RSOs and DS/SI/PSS; and is not available to Department personnel outside of DS/SI/PSS. The Senior Coordinator for Security Infrastructure (DS/SI) authorizes access to DSBI Channel message traffic at the headquarters level. This caption may be used laterally in the field. Use ASEC as the only TAGS on this traffic. (See 5 FAH-2 H-444.)

(2) The DSX channel is used for telegrams between the Assistant Secretary and/or Deputy Assistant Secretaries of Diplomatic Security and other appropriate DS personnel, and the responsible DS officer concerning criminal and special investigations involving U.S. citizens, U.S. Government employees or DS employees; counterintelligence investigations; adverse personnel security actions; investigations concerning spouse or child abuse; confidential sources; undercover operations; and other sensitive subjects which the drafter deems should be highly restricted. RSOs must ensure that communication program unit distribution (CPU) law is in accordance with 5 FAH-2 H-444. The Director for the Office of Investigations and Counterintelligence (DS/DSS/ICI) authorizes access to DSX Channel message traffic at the headquarters level. This caption may be used laterally in the field. Use ASEC as the only TAGS on this traffic. (See 5 FAH-2 H-444.)

12 FAM 422.4 Other Responsibilities and Duties

(TL:DS-91; 07-11-2003)

The RSOs other responsibilities and duties are but not limited to:

(1) Serve as the focal point at post for programs to protect U.S. classified and sensitive information, facilities and personnel from terrorism, hostile foreign intelligence activity, and criminal acts.

(2) Monitor and inspect the security programs at constituent embassies or consulates and provide comprehensive training and planning guidance to post security officers (PSOs) at these posts through periodic visits and exchanges of correspondence.

(3) Manage the regional security office, including the supervision of any assigned:

(a) Assistant regional security officers (A/RSOs);

(b) Security engineering officers (SEOs) (see 12 FAM 500);

(c) U.S. Marine security guards (see 12 FAM 430);

(d) U.S. Navy Seabees (see 12 FAM 600);

(e) Foreign Service national investigators (FSNIs) (see 6 FAH-5 H-405.1-6);

(f) Local guards under personal services contracts (see 12 FAM 320 and 12 FAH-7*, Local Guard Program Handbook*);

(g) Special bodyguards; and

(h) Secretarial staff.

(4) Maintain official liaison with host-country, third-country, and U.S. intelligence, security, and law enforcement organizations to conduct exchanges of current terrorist, counterintelligence, and criminal investigative data and to coordinate post defensive security programs or planning.

(5) Report and interpret information of security significance developed through host-country liaison activity.

(6) Serve as a member of the embassy emergency action committee, other pertinent committees, and the country team, providing security insights to other members based upon information received through foreign liaison and specialized knowledge of the security policies or programs being discussed.

(7) Establish and manage, where required, a special security program for the personal protection of the chief of mission and other U.S. officials targeted by terrorist groups, closely monitoring all available intelligence to determine the need for changes in operational protective tactics and techniques.

(8) Arrange and provide protective security coverage, host-country security liaison, and other services for U.S. VIP visits and conferences within the region.

(9) Develop, as the chief of mission or principal officer may direct, the security portion of the post emergency action plan (EAP) to address security issues including terrorist attacks, internal defense, riots, coups, and demonstrations.

(10) Participate in the conduct of bureau training or other programs that ensure the effectiveness of the EAP and the efficient utilization of post personnel and resources.

(11) Continually assess the vulnerability of resident and constituent posts to terrorism and hostile foreign intelligence information gathering activities, adjusting post defensive counterintelligence and/or counterterrorist planning and programs accordingly.

(12) Review current and near-term intelligence, Foreign Service reporting, and local news reporting available on political, military, security, and intelligence developments in a region to identify any security concerns.

(13) Prepare and coordinate comprehensive threat assessments for use by the Department and the post, including revising assessments when intelligence information so requires.

(14) Provide unclassified security threat countermeasure briefings and other professional security advice to U.S. business executives and other U.S. private citizens at a level of frequency commensurate with host-country threat conditions.

(15) Perform defensive counterintelligence functions and coordinate activities involving U.S. officials or Foreign Service national (FSN) employees who are targeted by hostile intelligence services.

(16) Maintain current knowledge of tactics and techniques being used locally by hostile intelligence services.

(17) Participate in the post counterintelligence working group (CIWG).

(18) Conduct, when directed by DS headquarters or the chief of mission, investigations of allegations or occurrences involving violations of U.S. criminal law or U.S. Government regulations by official employees, in accordance with 12 FAM 220 (Investigations).

(19) Conduct full field background investigations of all applicants for appointment to Foreign Service national (FSN) positions within the limits imposed by existing liaison agreements with the host government, which includes both making maximum use of host-country investigative records or resources when possible to ensure the fullest development of investigative leads and evaluating all information developed as a basis for the issuance or denial of the required certification for employment.

(20) Conduct full field background investigations of all contract employees of a U.S. mission and/or review investigations conducted by contractors on their employees; evaluate all information developed as a basis for the issuance or denial of the required certification for employment.

(21) Conduct update investigations on all FSN and contract employees on a five-year cycle and evaluate the results for the purpose of issuing or denying the required recertification for employment.

(22) Conduct security surveys of resident and constituent posts to include official office buildings and residential areas utilized by mission personnel and, as necessary, recommend major physical security changes or improvements revealed by such surveys to chiefs of mission; coordinate the implementation of all approved and proposed projects until completed; and modify internal defense planning concepts as necessary to incorporate improved physical security features as they are added.

(23) Design, implement, and manage post's local guard program (see 12 FAM 320).

(24) Design, implement, and manage post's residential security program (see 12 FAM 320).

(25) Provide professional security advice to dependents and employees of all U.S. country team elements at post.

(26) Formulate and conduct education and training programs pertinent to the conduct of post information security programs and ensure adherence to Foreign Service and other pertinent U.S. Government security regulations.

(27) Investigate and report to DS/ISP/APB all instances of possible information security incidents. (see 12 FAM 550).

(28) Serve as the mission focal point for the general oversight and coordination of special security programs managed by Bureau of Diplomatic Security offices.

(29) Coordinate the conduct of technical surveillance countermeasures inspections at posts with DS/IST/CMP, the regional engineering service center (ESC) and, if resident, the post security engineering officer (SEO) (see 12 FAM 500).

(30) Coordinate with the private sector on threat levels and help establish country councils for the Overseas Security Advisory Council (OSAC).

(31) Offer to provide professional security advice and unclassified security threat briefings to administrators of schools in which dependents of U.S. Government direct-hire employees are enrolled.

(32) Where appropriate at post, serve as the contracting officer's representative (COR) for local guards and residential security contracts.

(33) Design, implement, and manage post's surveillance detection program.

(34) Perform additional duties as directed by a chief of mission or the Bureau of Diplomatic Security.

12 FAM 423 SECURITY PERSONNEL

12 FAM 423.1 Post Needs

(TL:DS-74; 04-04-2001)

a. Posts are encouraged to identify breaks in security personnel staffing that may require temporary duty (TDY) coverage. Direct requests for TDY security personnel to DS/DSS/OP. RSOs should notify their respective DS/DSS/OP regional director at least two months prior to any anticipated absences.

b. During an RSO's absence from post due to a permanent change of station, home leave, medical evacuation, or annual leave, DS/DSS/OP will consider providing TDY coverage to post if:

(1) The post is at the critical or high-threat level in the terrorism and/or crime categories, or it is facing a specific threat even though the post is not in a high-threat category;

(2) There is no experienced professional security officer replacement at post. If an assistant regional security officer (A/RSO) (see 12 FAM 423.3) has been serving satisfactorily at post for more than six months, DS will consider this officer to be sufficiently experienced to replace the RSO on a short-term basis;

(3) The request is received with sufficient lead time to permit an orderly selection and briefing of the TDY replacement; and

(4) Sufficient funding for the TDY is available.

c. DS/DSS/OP will notify DS/ICI/CI of breaks in security personnel staffing at critical human intelligence threat posts and will coordinate requests for TDY support from those posts with DS/ICI/CI (see 1 FAM *260*).

12 FAM 423.2 Security Officer (SO)

(TL:DS-39; 08-15-1994)

a. For some RSO posts, DS/DSS/OP may approve (with the concurrence of DS/DSS) the establishment of a security officer (SO) position because of the exceptional priority that security is accorded there. The SO is a professional security officer with prior RSO experience. The SO reports to the RSO.

b. Security officer responsibilities and duties are similar to those of an RSO; however, they are limited to the post of residence, whereas an RSO manages the security program for a given geographic region. SOs are usually assigned to posts with a large (three or more) number of assistant RSOs (A/RSOs) and serve as the rating officers for the A/RSOs.

12 FAM 423.3 Assistant Regional Security Officer (A/RSO)

(TL:DS-39; 08-15-1994)

An assistant regional security officer (A/RSO) assists an RSO with all matters pertaining to post security programs. At posts without an assigned SO, in the RSO's absence, the A/RSO becomes the acting RSO. A/RSOs perform a wide range of duties designated by the RSO.

12 FAM 423.4 Post Security Officer (PSO)

(TL:DS-74; 04-04-2001)

a. Post security officers (PSOs) are U.S. officers whom the chief of mission or principal officer designates to manage security programs at posts which do not have a resident RSO. PSOs assume responsibility for day-to-day security matters. Most tasks assigned to PSOs are similar to those assigned RSOs, but are more limited in scope because PSOs are not Diplomatic Security officers.

b. PSO duties consist of:

(1) Administering post security policies and procedures;

(2) Administering the security incident program;

(3) Providing arrival and departure briefings to all U.S. employees and their dependents;

(4) Reporting threats and other post security situations to the RSO;

(5) Conducting investigations as requested and directed by the RSO;

(6) Conducting investigations of Foreign Service national (FSN) applicants, in accordance with existing liaison agreements with the host government, and submitting results to the RSO;

(7) Supervising the Marine security guard detachment commander and maintaining control of the Marine security guards;

(8) Managing the local guard program and supervising local guards hired under personal services contracts;

(9) Maintaining liaison with host-country officials and post officials;

(10) Formulating and coordinating emergency plans and conducting drills; and

(11) Conducting physical security surveys on proposed new-lease or purchase residential and/or official building properties, as directed by the RSO.

c. The chief of mission must designate each PSO in writing and send a copy to the RSO who has regional responsibility for the post.

12 FAM 423.5 RSO Secretary

(TL:DS-74; 04-04-2001)

U.S. citizen employees may be hired or assigned as RSO secretaries to posts where there is a resident RSO. They perform many specialized tasks not typically performed by other secretaries and are knowledgeable of security policies and procedures, in addition to secretarial skills. RSO secretaries are also responsible for:

(1) Typing specialized reports such as the security survey reports, investigative reports, security incident reports, and quarterly status reports;

(2) Disseminating threat information and information regarding policy changes; and

(3) Answering questions and resolving minor security problems in the RSO's absence.

12 FAM 423.6 Locally Hired FSN Investigators

(TL:DS-39; 08-15-1994)

a. Foreign Service national investigators (FSNIs) work in the security office and perform a variety of tasks that support the entire security program abroad primarily by:

(1) Providing expertise concerning the language, culture, and customs of the host country;

(2) Maintaining contacts with police and other host-government authorities;

(3) Obtaining information concerning potential security threats to the post; and

(4) Conducting investigations including background and criminal investigations.

b. The RSO or PSO is the FSNI supervisor. They control FSNI access to information pertaining to U.S. citizens and minimize the use of FSNIs in investigations involving U.S. citizens. FSNIs are prohibited from access to the security files of U.S. citizens and their access to the investigative files of other FSNs is controlled on a need-to-know basis. FSNIs may not interview U.S. sources or review U.S. citizen-controlled post files.

12 FAM 424 TYPES OF SECURITY BRIEFINGS

12 FAM 424.1 New Arrival Briefings

(TL:DS-39; 08-15-1994)

a. The RSO or PSO will provide a mandatory comprehensive security briefing to employees shortly after their arrival at post. The briefing must acquaint newly arrived personnel with the security situation at post and the total security environment, including the general security requirements and procedures in effect.

b. Routine arrival briefings must include general counterterrorism and counterintelligence policy and procedures relating to the post and country of assignment. As threat situations change, RSOs and PSOs must provide briefings for senior post officials and other employees and dependents to minimize the dangers posed by the change.

c. The briefing officer should use an outline at each briefing to ensure that all required subjects are covered. RSOs and PSOs will maintain a record of all briefings, including the dates and identities of all employees briefed, and they must establish procedures for ensuring employee participation. The employee must sign a statement that he or she has received a briefing, what material was covered, and that he or she understood the material covered.

12 FAM 424.2 Spouse and Dependent Briefings

(TL:DS-39; 08-15-1994)

a. Post management should strongly emphasize the advisability of having all spouses and adult dependents briefed on the security situation at post and actively encourage them to attend all security briefings.

b. The RSO or PSO should make unclassified security briefings available for spouses and other adult dependents of post employees as soon as possible after their arrival at post. Regularly scheduled post orientations may be used for this purpose. However, if a post does not have a formal orientation program, the security officer should make arrangements with the post's community liaison office (CLO) to establish a dependent briefing program that would include all adult dependents.

c. The CLO can assist in the subsequent dissemination of general security information to dependents. The security officer and CLO should jointly work out such a mechanism that possibly includes having the security officer participate in scheduled CLO dependent or community briefings.

d. The briefing will address all real threats and dangers to post personnel and dependents, and other related issues. The following are suggested topics of discussion for such a briefing:

(1) Local criminal activity affecting personal and residential security;

(2) High-crime areas of the city and country;

(3) An overview of narcotics available in the country and in the U.S. community, including local law enforcement and judicial action;

(4) An unclassified discussion concerning terrorist activity in the country directed against the host country, the diplomatic community, and U.S. interests;

(5) An unclassified discussion of the post's emergency action plan with emphasis on the warden system, actions to take during civil disorders, emergency plans for dependent schools, etc.;

(6) The post's specific problems, cultural differences, sensitivity to host-country customs and attitudes;

(7) The location where dependents can obtain information concerning the security situation; and

(8) Emergency telephone numbers including local police, fire and medical, and post security elements.

12 FAM 424.3 Rebriefing or Refresher Briefing

(TL:DS-39; 08-15-1994)

Security officers must periodically repeat briefings on the security situation at certain posts where personnel live under hostile intelligence or terrorist threats for long periods of time. Updating and restating procedural details reduces their vulnerability to approach or surveillance.

12 FAM 424.4 Security Incident Program

(TL:DS-74; 04-04-2001)

Security officers must brief all employees during their arrival briefing on the security regulations and methods concerning the safeguarding of classified information. This will assist employees with the secure handling of classified material and help prevent security incidents. RSOs and PSOs must also brief each employee who receives a security incident report and sign as a witness to the employee's signature acknowledging receipt of the notification packet. The briefing will include why the employee was responsible for receiving an incident report, how to prevent getting others, and the type of disciplinary action he or she may receive for further repeated incidents. (See 12 FAM 557.2.)

12 FAM 424.5 Special Travel Briefings

(TL:DS-74; 04-04-2001)

Special travel briefings cover the counterintelligence regulations pertaining to employee travel to critical human intelligence threat posts (see 12 FAM 200).

12 FAM 424.6 Departure Debriefings

(TL:DS-39; 08-15-1994)

a. The RSO or PSO will schedule an exit interview for all U.S. citizen employees before their permanent departure from post. Each departing employee should be interviewed separately and given an opportunity to comment on any aspect of the post security program including:

(1) Any significant contacts with foreign nationals of designated countries;

(2) International travel during their tour of duty; and

(3) Any security problems encountered.

b. The security officer will make a record of the exit interview, including any security-related comments received from the employee, and maintain these records in the post security office files.

12 FAM 424.7 Separating Employees

(TL:DS-74; 04-04-2001)

a. Security officers will give a detailed security debriefing to personnel who are terminating their employment abroad and are not returning to the United States or are otherwise to be separated for a continuous period of 60 days or more.

b. The employee must sign Form OF-109, *Separation Statement* (see 5 FAM 413), and the security officer must advise him or her of the applicable laws on the protection and disclosure of classified information.

12 FAM 425 RSO RESPONSIBILITIES

(TL:DS-74; 04-04-2001)

a. RSOs and PSOs work closely with the information systems security officer (ISSO) at post (see 12 FAM 600) on systems security issues and have specific responsibilities for:

(1) Ensuring that all personnel with access to a classified system have an appropriate security clearance;

(2) Coordinating briefings with the ISSO for system users upon their arrival at post, concerning the security considerations of classified systems;

(3) Issuing Form OF-117, *Notice of Incident*, for security incidents on the system based upon either the RSO's or ISSO's investigation;

(4) Periodically checking alarm systems that protect computer equipment to ensure proper functioning; and

(5) Conducting or verifying the security clearances of local vendor personnel who service system components.

b. Pursuant to their role as the overall manager for security at a post, RSOs or PSOs must also provide the ISSO with guidance and/or information regarding the:

(1) Department prohibition on processing classified security information on an unclassified system;

(2) Physical and equipment security measures;

(3) Security processing for staff and maintenance employees with access to an automated information system;

(4) Identification of a secure storage area for back-up copies of system data files and software;

(5) Suspected incidents of fraud or manipulation of data on a system, the unauthorized disclosure or the destruction of data, or the personal use of system resources; and

(6) Coordination and monitoring of the conduct of periodic security indoctrination and training sessions for personnel assigned to a post.

12 FAM 426 QUARTERLY STATUS REPORT

(TL:DS-74; 04-04-2001)

a. Each RSO must submit a Quarterly Status Report (QSR) to the Directorate for Overseas Operations by the fifth working day of the appropriate month:

(1) January 5th – 4th Quarter (calendar year) for October, November and December;

(2) April 5th – lst Quarter for January, February and March;

(3) July 5th – 2nd Quarter for April, May and June; and

(4) October 5th – 3rd Quarter for July, August and September.

NOTE: QSRs should not be sent over the DS channel.

b. RSOs should review QSR reports carefully for sensitive or classified information. The RSO should either remove such information from QSR reports and report it separately or mark paragraphs appropriately. QSRs are internal documents and not for distribution to other agencies, however, internal post distribution as RSOs deems appropriate is encouraged. Additionally, the QSR is meant to be an overview of RSO activities and not a daily log of RSO action.

c. Security officers will always use the caption TERREP or TERREP EXCLUSIVE on telegrams pertaining to terrorism subjects including:

(1) Terrorist groups, threats, or acts;

(2) Anti-terrorist measures by other governments; and

(3) Conversations with foreign officials about terrorism.

12 FAM 427 THROUGH 429 UNASSIGNED