

15 SEPTEMBER 2004

Intelligence

THREAT WORKING GROUP (TWG)



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ AMC/A23
(Mr. Stephen H. Dawidowicz)
Supersedes AMCI 14-106, 1 June 1999.

Certified by: HQ AMC/A23
(Mr. Stephen H. Dawidowicz)
Pages: 19
Distribution: F

This instruction implements AFD 14-1, *Air Force Intelligence Planning and Operations*, and AFI 14-119, *Intelligence Support to Force Protection (FP)*, at HQ Air Mobility Command (AMC). It prescribes rules, processes, and procedures for the HQ AMC Threat Working Group (TWG), and assigns responsibility for managing TWG processes and conducting TWG business. It also designates organizations and offices that may, if requested, support or facilitate TWG processes in the conduct of TWG business. This instruction does not apply to Air National Guard or Air Force Reserve Command units.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1. Threat Working Group.

1.1. **Charter.** Air Mobility Command's (AMC) Threat Working Group (TWG) is the command focal point for coordinated threat analysis and force protection (FP) recommendations for AMC operations in high-risk locations. The TWG provides a functionally integrated threat assessment of potential airfields. Based on TWG assessment, the TWG principals (O-6 level) make recommendations to the AMC/A3 who establishes Virtual Risk Assessment (VRA) policy.

1.2. **Meetings.** As a rule the TWG conducts two meetings each duty day. The TWG principals' meeting, which is chaired by the A2, and the Action Officer (AO)-level work group meeting that is chaired by the Intelligence Operations Division (A23).

1.2.1. The principals' meeting is the forum to raise issues and questions, task the TWG AOs, and review and validate all AO products, recommendations, and waiver requests, prior to submission to the A3. The principals will also conduct a review of all AMC missions into locations on the TWG Watch List occurring in the next seven days.

1.2.2. The AO meeting is a working-level meeting to analyze threats to AMC missions, review threat mitigation efforts, and assess needed FP measures. The AOs will review upcoming missions to determine the adequacy of existing FP measures. The AOs will make FP recommendations based on the localized threat and provide recommendations to the TWG principals for review/validation. All waivers, VRA updates, and general correspondence will be reviewed at this meeting and AO recommendations will be provided with an accompanying signature page (signed by the AOs from the Intelligence Analysis Division (A22), Combat Operations Division (A39), SF, SG, TACC, and OSI) to the TWG principals.

1.3. **Membership.** The TWG combines experts from intelligence, counterintelligence, medical, physical security and operations into a single forum to develop risk assessments and FP recommendations for the A3. The TWG consists of two bodies, the senior officer-level principals and the AOs, as well as various support entities, which are mentioned in detail in section five. All TWG principals, their alternates, and their AOs will have a current SCI indoctrination for SI, TK, G, and HCS.

1.3.1. The TWG principals are a multi-directorate body comprised of senior officers from A2 (Chair); SF; SG; A3; Commander, AFOSI Region-3; 18th Air Force (represented by TACC/XOZ), and TACC/XOC. The TWG assesses all source data to determine best course of action recommendations.

1.3.2. TWG principals will appoint highly qualified individuals to work on the TWG as AOs. The TWG AOs will meet every day the principals meet, and additionally as required. The A23 Division Chief chairs the AO meetings. Following is a list of primary AOs that are required for an AO quorum: A23 (chair), A22, A39, TACC/XOG and XOC (who act as AOs for TACC/XOZ), TACC/XOP, TACC/XOO, SG, SF, AFOSI Region-3. Representatives of the following offices are highly desired: A34, and AIA/67th IWF. The AOs will develop and use decision aid tools to quantify the Man Portable Air Defense System (MANPADS) threat and the recommendation for Defensive Systems (DS). Additionally, the AOs will assess in place FP measures that affect aircraft and aircrew physical security, health issues, route and ground transportation to/from airport, billeting arrangements, political unrest, terrorism, crime, foreign intelligence operations, and aircraft defensive systems and tactics. The AOs are responsible for evaluating risk and developing threat mitigation recommendations for consideration by the TWG principals.

1.3.3. Intelligence Operations Division (A23). A23 is the only TWG member manned for daily 24-hour operations. A23 is the central point of contact for the TWG. A23 chairs the TWG AO meeting, sets the agenda for the TWG principals' meeting, provides all administrative support to the TWG, publishes VRA updates, ensures the timely completion of TWG products, schedules TWG meetings, schedules airfield reviews, and performs other administrative support as required.

1.4. **Internal TWG Coordination.** The AOs will review upcoming missions and associated FP measures as they impact the command's mission, and make regular security assessments for countries and select airfields on the TWG Watch List. When VRA updates, waiver requests, and all other forms of formal TWG correspondence are forwarded by the TWG AOs to the principals for action, each primary AO will concur/non-concur with that action on a signature page maintained by A23. The principals will review and validate all TWG AO recommendations, products, and correspondence prior to distribution or submission to the A3 and will signify whether they concur or non-concur on a signature page maintained by A23. Not all TWG principals need to coordinate on all TWG recommendations. For example, the SG can independently represent the public health concerns for the command and, since the SG is not line of the Air Force, is not required to validate non-health FP issues.

1.4.1. Theater Coordination. The TWG will work with Theater component FP organizations. All threat assessments and policy recommendations created by this TWG are compared with Theater(s) Air Operations Center (AOC) assessments (if an AOC is established). Assessment differences between AMC and the theater will be resolved at the AO level, or if the differences cannot be resolved, the basis for the difference will be presented to the TWG principals prior to forwarding recommendations to the A3.

1.4.2. Contingency Support. The TWG is not manned for 24-hour operations. The TWG will support contingency operations as deemed necessary by the TWG principals. TWG principals make assessments and complete airfield reviews daily during regular duty hours. The functional areas represented on the TWG will have AOs to handle specific questions during duty hours and on-call during non-duty hours. When specific questions arise regarding threats to an airfield, the TWG AOs will provide the appropriate response with respect to their functional expertise.

1.4.2.1. Convening the TWG. Normal TWG duty hours are 0730-1630 Monday-Friday. When intelligence assessments change, a new threat is identified or a new time-sensitive airfield requirement is identified that cannot wait until the next normal duty day for resolution, the TWG Chairman may convene the TWG principals during non-duty hours with the purpose of preparing a subsequent recommendation to the A3 for policy implementation.

1.4.2.2. TWG Operations Center (TOC). A2 has established a TWG Operations Center (TOC) in the intelligence Sensitive Compartmented Information Facility (SCIF). This area includes meeting space and computer support for the TWG AOs as necessary. TWG AOs will convene in the TOC when recalled.

2. Process.

2.1. **Operational Risk Management (ORM).** Air Mobility Command uses a six-step ORM process to review both specific airfields and individual missions transiting TWG Watch List tier 1 and 2 locations around the world. The process involves making recommendations on individual missions or specific airfields by 1) identifying the hazard, 2) assessing the risk, 3) analyzing risk control measures, 4) making control decisions, 5) implementing risk controls, 6) and supervising, reviewing and analyzing feedback on implemented risk control measures. The TWG develops risk assessments, recommends FP policy and threat mitigation measures to the A3. The A3 policy matrix is a product of the ORM process.

2.2. **TWG Watch List (TWL).** The TWL is a list of countries broken out into three tiers according to the level of assessed risk to AMC operations. These tiers define minimum VRA production requirements; although VRAs may be created, as directed by the TWG, on an airfield or country, regardless of a country's tier level. The TWL is a TWG product, approved by the A3. The TWL will be updated as required; however, a comprehensive top-to-bottom review of the TWL with revalidation by the A3 will be conducted on an annual basis. The three tiers are:

2.2.1. Tier 1 countries present the greatest risk to AMC operations. VRAs are required for each airfield transited by AMC aircraft in Tier 1 countries. When AMC aircraft are planned to transit an airfield in a Tier 1 country not supported by a VRA, and there is not enough time to create an airfield VRA, then an A3 waiver is required utilizing the best all-source information available.

2.2.2. Tier 2 countries present a lesser risk to AMC operations than do Tier 1 countries. A country VRA is required for all Tier 2 countries. At the TWG's discretion, airfield VRAs may be created

when, for example, they are subject to frequent AMC use, or when airfield policy would differ from overall country policy. Note that an airfield VRA takes precedence over a country VRA in all cases. "Denied" countries, as defined by Defense Intelligence Agency (DIA), will be at least Tier 2 countries.

2.2.3. Tier 3 countries present little or no risk to AMC operations and usually have no restrictive operations policies. VRAs are not required on Tier 3 countries.

2.3. Virtual Risk Assessments (VRAs).

2.3.1. The primary product of the AMC TWG is the VRA. VRAs contain threat assessments and A3-approved FP policies. All AMC and AMC-gained mission planners and aircrews will follow A3 policies. VRAs are maintained by A23 in the Virtual Risk Assessment Database (VRAD). VRAs are created and maintained for airfields and countries as required by the TWG Watch List.

2.3.1.1. The A3 will approve all VRAs that result in new policies or policy changes.

2.3.1.2. The A3 may delegate authority to establish/update A3 policy (e.g., SG may be granted the authority to set malaria prophylaxis policy for airfields and countries with endemic malaria). This delegation will be done in writing and will kept on file by A23.

2.3.2. All VRAs consist of two sections. Section 1 contains the A3-approved FP policy for the airfield or country. Section 2 contains threat and security assessments that support the A3's policy and for use by intelligence personnel and aircrew members during mission planning.

2.3.3. TWG member VRA responsibilities for content are outlined below. All TWG members will ensure their section of the VRA does not contradict A3 policy. When AOs update a section a VRA with substantive changes, they will brief those changes at the next AO meeting. Similarly, when A2, OSI and SF create/update a MANPADS assessment and A39 creates a new DS assessment, the results will be briefed to the AOs and principals as required.

2.3.3.1. Intelligence: The Intelligence Applications Division (A22) will maintain the Terrorist and Military Threat sections of the VRA. A22 is also the OPR for MANPADS assessments.

2.3.3.2. Office of Special Investigation (OSI): OSI will maintain the Criminal and Counterintelligence Threat sections of the VRA, and will collaborate as required by A2 to complete the MANPADS assessment.

2.3.3.3. Security Forces (SF): SF will maintain the Airfield Security section of each airfield VRA, and will collaborate as required by A2 to complete MANPADS assessments.

2.3.3.4. Surgeon General (SG): Responsible for the Medical Threat section and the Additional Medical Restrictions policy block on the VRA. Medical threats that could potentially affect AMC transiting crews are elevated when aircrews RON or if there is a local medical or environmental threat that could impact mission success (i.e., a local active disease outbreak or local contaminated food or water). The TWG SG member will update medical intelligence in the VRA upon notification of a RON or when medical intelligence sources report a medical or environmental threat of operational significance is present at the projected operation location. The SG will also review and publish assessments on chemical and biological threats that might affect AMC missions.

2.3.3.5. 67th Information Warfare Flight (IWF): The 67th IWF is responsible for assessing the Information Operations threat, to include the PSYOP, Electronic Warfare, Operations Security

(OPSEC), and Computer Network Defense (CND) threats. However, these sections are only required if warranted by the threat.

2.3.3.6. Combat Tactics (A39): A39 is the OPR for the Tactics section and will also develop policy recommendations for DS, airfield operations restrictions, personal and aircraft armor requirements, and any additional flight restrictions that might be required. A39 will coordinate AMC DS policy with Theater DS policy during the VRA review process.

2.3.4. Policy Options. For each VRA, the TWG will make recommendations to the A3 for the following policy options: The requirement for Defensive Systems (DS), personal armor, aircraft armor, laser eye protection, and Phoenix Raven support; restrictions on commercial aircraft operations, airfield operations, remain overnight (RON), maximum number of aircraft allowed on the ground (MOG); and medical issues and restrictions.

2.3.5. Policy Change Recommendations. When AOs recommend a change to A3 policy, they will submit the respective VRA, with AO-level signature page and recommendations attached, to the TWG principals for concurrence/comment. This action will be required for all policy areas that have not been delegated by the A3, in writing, to a specific functional TWG principal (e.g., SG for medical policies).

2.3.6. VRA Updates. The TWG will initiate a complete VRA assessment and policy review as noted below:

2.3.6.1. Country and airfield VRAs will be reviewed when significant threat changes occur within a country that would result in the country moving to a higher Tier level.

2.3.6.2. All airfield VRAs will be reviewed, at a minimum, semiannually. However, VRAs on airfields located in designated combat zones, or as directed by the A3, will be reviewed at least quarterly.

2.3.6.3. Country VRAs will be reviewed, at a minimum, annually.

2.3.6.4. VRAs that are no longer needed will be deleted from the A2 website with A3 approval. Deleted VRAs will be retained in draft form in a VRA archive should it be necessary to reinstate the VRA in the future. When a VRA is deleted, its corresponding policies are no longer in effect.

2.3.7. A23 responsibilities in the VRA review process are:

2.3.7.1. To manage the VRA review process. A23 will ensure VRA reviews meet the TWL timeliness requirements. A23 will update the TWG principals on the status of the VRA review process on a weekly basis.

2.3.7.2. To publish VRAs on the A2 SIPRNET website. A23 will perform a quality control review of each VRA prior to publication. A23 will also ensure that VRAs with policy changes are not published until they are approved by the A3. VRA assessments with no corresponding policy changes may be published immediately.

2.3.7.3. Upon A3 approval, to delete VRAs from the A2 website that are no longer needed and archive them in draft.

2.3.8. Dissemination: TWG risk assessments and resulting A3 policies will be published on the A2 website (<http://www.amcin.scott.af.smil.mil>) under the Force Protection menu.

2.3.8.1. Changes to VRAs or A3 policies will be highlighted on the website for a period of seven days from the time the changes are posted to the website.

2.3.8.2. A23 is responsible for maintaining the FP portion of the A2 website, and will publish or delete all VRAs, supervise the online processing of policy waiver requests, and will add, modify, and delete all links and other documents as necessary.

2.4. Special Mission Review. Special mission reviews may be conducted collectively by the AOs for specific missions well in advance of mission execution at the request of the mission planners. Mission review requests must be accompanied by a mission itinerary. When such a request is received, the AOs will review the mission itinerary, noting locations needing waivers or that have threat, security, or medical concerns. Upon review completion, principal AOs will annotate their advice and comments and initial the mission itinerary. A23 will return the mission itinerary to the planners with the TWG AOs' comments. Note that this process does not preclude the mission planners from complying with A3 policy, or when deviating from policy, submitting formal waiver requests for TWG review.

2.5. Waiver Requests. Each VRA includes A3 operations FP policies that must be followed when planning and executing missions. All missions deviating from the FP policy must be waived, including DV airlift missions.

2.5.1. Deviations from established policy must be approved by the A3 after a case-by-case review and recommendation by the TWG. Waivers can only be submitted via A2's classified website (http://www.amcin.scott.af.smil.mil/waiver/waiver_main.asp). When submitted, the waiver form is automatically transmitted to A23 who will act on the request and forward the form to the TWG AOs for recommendation. When the above actions are complete A23 will present the waiver request to the TWG principals for action.

2.5.2. The A3 may delegate waiver authority, in writing, to subordinate units. Accordingly, the AMC/A3 may grant specific waiver authority to the wing commanders of the 6 AMW and the 89 AW, due to their unique DV mission requirements. The respective wing commanders may, in turn, further delegate this waiver authority no lower than their operations group commander, and/or the Presidential Pilot for Presidential aircraft operations.

2.5.2.1. This waiver authority pertains only to defensive system requirements, airfield operating restrictions, Laser Eye Protection (LEP), personal and aircraft armor, MOG, RON, Phoenix Raven requirements, and additional restrictions listed in the "Notes" section of the "Airfield Operating Restrictions" block of all VRAs. The 6 AMW or 89 AW may not waive the "AMC/A3 Approval Required" restriction.

2.5.2.2. Due to the high importance and visibility of many 6 AMW and 89 AW missions, they may refer any waiver request to the AMC TWG for final consideration. In addition, when a user's mission request isn't fully supported because the 6 AMW or 89 AW denies a waiver request, the wings will notify A23. A23 will then notify TWG principals of the waiver denial. The TWG will review the wing's decision, and if the customer still wishes to pursue the mission, the TWG chairman will notify the A3 of the wing's decision to deny the waiver, accompanied by a TWG assessment of the waiver request. On rare occasions, the A3 may direct the 6 AMW or 89 AW to fly a mission after the wing denies a waiver request for that particular mission. If the A3 requests the opportunity to review a wing's waiver decision, the wing will submit a waiver request via the on-line AMC Mission Waiver Request Form. The request must include the rationale for the wing's denial, as well as recommended tactics, techniques and

procedures (TTPs) to mitigate the threat if the A3 decides to overrule the wing's decision. The TWG will review the mission and the wing's recommended TTPs. If the TWG principals assess that additional TTPs are needed, they will recommend modifications or additions to the wing's TTPs and then make their overall recommendation to A3.

2.5.3. The waiver request should fully explain the circumstances that would justify a deviation from policy, and should include, at a minimum, the purpose and importance of the mission, as well as any planned threat mitigation measures. Waivers should be submitted as early in the planning process as possible.

2.5.3.1. When required, waiver requests may be submitted for missions in execution. Waiver requests should not, however, be delayed in order to receive last minute expedited approval.

2.5.3.2. Once the online waiver is submitted, A23 forwards the waiver request and suspenses the TWG AOs for waiver review. The AOs will consider all pertinent data, including any additional threat mitigation measures AOs believe are warranted. AOs will annotate their comments on the waiver form.

2.5.3.3. After AO review, A23 will brief the principals on the waiver request and present the waiver and AO comments for principal review and recommendation. The TWG principals will sign the waiver form, indicating their recommendation. A23 will then ensure the waiver form is forwarded to the A3 for approval/disapproval.

2.5.3.4. After the A3 has signed the waiver, it is returned to A23 who will maintain it on file and provide a copy of the waiver to the TACC senior controller (TACC/XOZ). A23 will also update the A2 website to indicate the approval/disapproval of the waiver.

2.6. **7-Day Mission Review.** Each time the TWG meets, it will review a list of all AMC missions planned to launch over the next seven days to locations in Tier 1 and Tier 2 countries. When missions are not in compliance with published AMC policy, or when TWG members detect a potential vulnerability that significantly increases risk, the mission will be referred back to the planner through the TACC/XOZ and/or TACC/XOC principal to be re-planned, processed for waiver, or cancelled.

2.7. **Non-Raven Required List Process.** The Non-Raven Required list identifies airfields where security is known to be acceptable and where Phoenix Raven support is not required. Aircraft transiting all other locations require onboard Phoenix Raven support to ensure aircraft security while on the ground. SF updates the Non-Raven Required List when reliable information is received denoting a change in security status at a specific airfield. The Non-Raven Required List is published on the A2 website and passed to the TACC/CC, TACC/XOC and TACC/XOZ. Additionally, when Raven requirements change for a given airfield, the airfield VRA with updated Raven policy will be reviewed by the TWG principals and then forwarded to the A3 for approval.

2.8. **Force Protection Condition (FPCON) Delta Evaluation.** When an airfield, country, or theater goes to FPCON Delta:

2.8.1. A23 will immediately inform the AMC TWG members.

2.8.2. The TWG will evaluate the specific threat(s) that initiated the FPCON change, assess aircraft, aircrew and passenger safety, review A3 policy; and, as needed, recommend TWG Watch List and FP policy changes to the A3.

2.9. TWG Support to DOD Contracted Carriers or Civil Reserve Air Fleet (CRAF) Assets.

2.9.1. IAW AFI 14-105, upon activation of the CRAF, the TWG is responsible for coordinating intelligence and FP support to CRAF assets. The TWG will perform this support via the normal TWG process, or additionally as required by A34Y.

2.9.2. Civilian carrier support to DOD missions: Civilian carriers are frequently contracted to augment DOD organic resources, without CRAF activation. This process allows the DOD to meet mobility requirements.

2.9.2.1. A22 is responsible for coordinating intelligence/FP support for CRAF and contracted carriers while performing DOD missions into threat regions. A22 will designate an analyst to work as a liaison with Transportation Security Administration (TSA) Intelligence to assure adequate coordination and information sharing occur in regard to CRAF and contract carrier support. The A22 analyst will keep A23 informed of information exchanged with TSA to ensure proper continuity is maintained.

2.9.2.2. Civilian crew access to information is based strictly on need-to-know considerations and verification of DOD mission assignment. Verification is the responsibility of the TWG. Confirmation will be accomplished by checking the Global Decision Support System (GDSS) to ensure there is a valid DOD mission being accomplished by the carrier.

2.9.2.3. The level of information disclosed is restricted to collateral SECRET and below. Enroute commercial aircrews can receive only oral and visual briefings--they are not allowed to obtain hard or soft copy documentation.

2.9.2.4. Hard copy documentation will only be released via secure means to an appropriately cleared point of contact (POC) at the commercial carrier's headquarters with approved classified storage capability.

2.9.2.5. If dissemination of the threat information might affect an operational policy change regarding how the DOD-contracted carrier or CRAF asset will execute a mission, TWG principals will coordinate with the TACC/CC and/or A3 prior to approving dissemination of the threat information.

2.9.2.6. Upon TWG principal approval to disseminate threat information to a DOD contracted carrier or CRAF asset, A23 will provide a copy of the coordinated threat information to A34 (or the CRAF Cell during CRAF activation) for transmission to the affected DOD contracted carrier or CRAF asset.

2.9.2.7. A22 will transmit a copy of the threat information to Transportation Security Administration (TSA) Intelligence to ensure TSA has a record of the threat information provided.

2.9.3. Technical Stop List. All locations in the United States and its territories are approved for contracted carriers to make passenger and cargo technical stops. In addition, all locations in Canada are approved for passenger/cargo technical stops, as well as locations approved for RON in the AMC Policy Matrix. AMC/A3 approval is required for contracted carriers to stop at all other commercial airports for passenger and cargo technical stops.

2.9.3.1. Technical Stop List. A23 will maintain a copy of the current A3-approved Technical Stop List. The Technical Stop List will contain commercial airports approved for contracted carriers to make passenger/cargo technical stops. A23 will provide a copy of the Technical

Stop List to A34Y, who keeps the contracted carriers informed of approved commercial airport technical stop locations.

2.9.3.2. Additions to Technical Stop List. Proposed changes to the Technical Stop List will be presented to the TWG AOs by A34Y. The TWG AOs will assess the new location and give recommendations to the TWG principals. TWG principals will review the new technical stop location, and forward their recommendation to A3 for approval/disapproval.

3. TWG Principal Membership and Support Responsibilities.

3.1. Director of Intelligence (A2).

3.1.1. The A2 chairs the TWG. The A2 is also responsible for delivering actionable mobility-focused intelligence to HQ AMC, Tanker Airlift Control Center, the TWG, and Active and AMC-gained Air National Guard and Air Force Reserve units. When applicable the A2 will info copy AFRC/A3I, on information pertaining to units under its control.

3.1.2. The A2 will maintain the Intelligence Operations Division (A23) for TWG support. A23 is responsible for implementing this instruction on behalf of the TWG, preparing items as directed by the TWG; bringing issues to the TWG for consideration; coordinating waiver requests to A3 policy; coordinating VRA updates to ensure its accuracy, integrity, and currency; and preparing/presenting any other items deemed necessary to support the TWG.

3.1.3. The A2 will also provide:

3.1.3.1. Meeting space and classified workstations in a secure working environment for members of the TWG in the Threat Operations Center (TOC).

3.1.3.2. AO members to the TWG as required.

3.1.3.3. Administrative and coordination oversight for all TWG products and correspondence records of all TWG recommendations and produces reports as required.

3.1.3.4. Take lead on all threat assessments and maintain MANPADS threat assessments on file.

3.1.3.5. Schedules for TWG meetings.

3.2. Director of Operations (A3).

3.2.1. The A3 will appoint a senior officer to serve as a principal member of the TWG. The A3 principal representative ensures operations issues related to TWG processes and FP are addressed. He also engages other A3 staff functions, as required, to facilitate TWG issues and tasking, and provides insight regarding A3 internal processes and organizations affecting or affected by TWG recommendations. The A39 Division Chief is the primary principal for A3. A3's senior on-call representative is the Deputy A3 (DA3), the Assistant A3 (DA3-1), or the A39 Division Chief when designated.

3.2.2. The Combat Operations Division (A39) will develop and maintain a tool to assess MANPADS vulnerability and determine DS recommendations. A39 provides expertise on aircraft DS and provides tactics, techniques and procedures to mitigate the threat. In addition, A39 ensures operations issues related to TWG processes and FP are addressed at TWG meetings.

3.2.3. Provide advice and recommendations on issues affecting commercial and contracted carrier matters.

3.3. Director of Security Forces (SF).

3.3.1. Assesses adequacy of supported command FP and security policies to ensure adequate protection for AMC resources.

3.3.2. Assesses adequacy of FP and security for AMC missions for Tier 1 and 2 countries from the TWG Watch List.

3.3.3. Develops FP and personnel protection guidance for inclusion in TWG risk assessments.

3.3.4. Ensures Phoenix Raven requirements are accurately reflected in Global Decision Support System (GDSS).

3.3.5. Maintains the Phoenix Raven airfield survey database, accessible on the A2 classified website (<http://www.amcin.scott.af.smil.mil>).

3.3.6. Develops, maintains and disseminates the Non-Raven Required List.

3.4. 18th Air Force (18 AF).

3.4.1. 18th Air Force is responsible for planning, scheduling, tasking and executing all AMC missions. AMC organic and commercial contracted aircraft/crews must adhere to A3 policy while flying worldwide missions. Within 18 AF, Tanker Airlift Control Center (TACC) mission planners and C2 controllers, operations directors and flight managers must, therefore, be familiar with and ensure adherence to A3 policy.

3.4.2. The TACC Director of Operations (TACC/XOZ, representing 18 AF) and the Director of Command and Control (TACC/XOC) are principal members of the TWG. They provide expertise and assistance to the TWG with current mission schedules and in addressing FP issues during mission execution. In addition, they provide insight on mission accomplishment, TACC internal processes, and players affecting or affected by TWG decisions and products, and engage other TACC directorates and processes required to facilitate TWG issues.

3.4.3. TACC planning directorates (XOG/XOO/XOP) provide AO representation on behalf of TACC/XOZ and TACC/XOC at TWG AO meetings to facilitate, coordinate and discuss issues relating to future missions and FP issues.

3.4.3.1. Identify CJCS exercise, contingency, Special Assignment Airlift Mission (SAAM) and air refueling mission requirements to the TWG to include mission support force deployments, airlift flow, level of participation, and any other unique requirements.

3.4.3.2. When feasible, provide a monthly projection for CJCS exercise, contingency, SAAM and air refueling missions requiring TWG assessments and recommendations.

3.4.3.3. Submit waiver requests for missions requiring exceptions to A3 policy using the electronic waiver form as early as possible to allow full investigation of mitigating factors by the TWG AOs.

3.4.4. AO representatives from TACC/RFG (Guard Advisor) and TACC/RFR (Reserve Advisor) will serve as advisors to the TWG on AMC-tasked Air National Guard and Air Force Reserve Command units and personnel.

3.5. Air Force Office of Special Investigation (AFOSI) Region 3. As a principal and AO-level TWG member, AFOSI Region 3/Office of Force Protection advises the TWG on antiterrorism and counterintelligence issues (collection, investigation, or counterespionage-related matters) and provides the TWG with the latest threat information available on terrorism, crime, and foreign intelligence matters.

3.6. Surgeon General (SG).

3.6.1. Force Health Protection (FHP) is integral to the entire spectrum of in-transit, pre-deployment, deployment, post-deployment, and steady state AMC operations. Planners must consider safety and security of local food and water sources, prevention of vector-borne and infectious diseases, sanitation and hygiene of local food serving and billeting facilities, and environmental threats prevalent throughout AMC operational locations. If medical threat prevention and mitigation are not in the forefront of planning, medical prevention becomes medical intervention. Since Operation DESERT STORM, more than 99 percent of hospitalizations of deployed US Service members were caused by preventable disease non-battle injuries (DNBI). Awareness of medical threats and implementation of practical medical threat mitigation recommendations will dramatically reduce the impact of DNBI on AMC personnel and increase mission success.

3.6.2. The Command Medical Intelligence Officer, Command Medical Intelligence NCO, and/or their representative will represent SG at the TWG and TWG AO meetings. The SG representative will:

3.6.2.1. Review all available medical threat information concerning AMC operational locations worldwide. Armed Forces Medical Intelligence Center threat information and threat categorization for AMC operational locations will serve as the baseline.

3.6.2.2. Ensure medical issues related to TWG processes and Force Health Protection is addressed in daily TWG meetings.

3.6.2.3. Provide medical threat updates and medical threat mitigation recommendations when requested at TWG AO meetings for inclusion into the A2 VRA.

4. Recommended TWG Support Membership and Functions.

4.1. Supporting TWG Members. The following non-AMC organizations or representatives are encouraged to participate in and observe TWG and TWG AO meetings.

4.2. USTRANSCOM Director of Intelligence (USTC/J2).

4.2.1. The USTC Joint Operations Intelligence Division (JOID) provides 24-hour Indications and Warning support for HQ AMC.

4.2.1.1. During non-duty hours, the JOIC will notify A23 and the TACC Senior Controller of significant threats or changing world events affecting planned or on-going air mobility operations.

4.2.1.2. Serves as the conduit for collection requirement validation and RFI submission to USTC/J2.

4.2.1.3. Serves as the liaison between AMC and Theater commands to ensure TWG issues are appropriately addressed.

4.3. **USTC Joint Intelligence Task Force – Counterterrorism (JITF-CT).** Provides Counterterrorism (CT) support for AMC operations by coordinating with service CT headquarters, the Joint Counterterrorism Support Branch (DIA), and the CT elements of the other unified commands.

4.4. **USTC Counterintelligence Support Office (CISO).** Provides Counterintelligence (CI) support for AMC operations by coordinating with service CI headquarters, the Joint Counterintelligence Support Branch (DIA), and the CI elements of the other unified commands.

4.5. **Director of Central Intelligence (DCI)/Central Intelligence Agency (CIA).**

4.5.1. Serves as the single point of contact for the TWG to the DCI/CIA regarding intelligence and FP issues.

4.5.2. Provides the TWG with the full range of DCI/CIA intelligence, collection capabilities, and all-source analytical products and services necessary to the formulation of TWG and TWG FP decisions and recommendations.

4.5.3. Provides DCI Counterterrorism Center analysis and comments on TWG risk assessments.

4.5.4. Responds in a timely fashion to intelligence information requests from the TWG.

4.5.5. Provides comments from CIA clandestine HUMINT collectors on TWG assessments.

4.6. **National Security Agency/Central Security Services (NSA/CSS).**

4.6.1. Serves as the single point of contact for the TWG to the NSA/CSS for Signals Intelligence (SIGINT) and Information Assurance (IA) issues.

4.6.2. Facilitates availability of NSA/CSS assets to efficiently meet the requirements of the TWG. Includes maintaining a Cryptologic Services Group (CSG) at USTC conducting continuous 24-hour operations. NSA-related after hours indications and warning (I&W) time-sensitive perishable information is routed from the NSA/CSG watch to the JOIC. The JOIC is the conduit for RFI work-order control, validation, and dissemination of Component information needs.

4.6.3. Advises and assists the TWG on issues regarding the procurement, exploitation, use and limitations of SIGINT in conducting operations in secure launch countries.

4.6.4. Advises and assists the TWG on issues relating to Information Assurance as part of Information Operations.

4.6.5. Assists the TWG in identifying intelligence requirements or gaps that could be resolved, in part or completely, through SIGINT operations. Assists in drafting Information Needs (INs) for submission in the National SIGINT Requirements Program.

4.6.6. Coordinates TWG requirements levied on the United States Cryptologic System (USCS) and ensure appropriate NSA/CSS offices are aware of TWG requirements. Provides AMC operational data such as the Secure Launch List to the USCS to aid in conducting operations.

4.6.7. Responds to TWG requests for SIGINT data either through local capabilities or through access to the USCS and ensures timely distribution of relevant SIGINT products.

4.6.8. Coordinates arrangements for en route flight following and threat advisories for aircraft transiting or terminating in areas suspected to be hostile to US military activities.

4.6.9. Arranges with Special Support Activity (SSA) for rapidly deploying special intelligence collection activities in situations where limited SIGINT collection exists and conditions require more thorough intelligence coverage.

4.6.10. Assists in developing and coordinating intelligence positions, assessments, and recommendations on placing countries on the TWG Watch List, assessing threats at operating locations in these countries, and resolving other issues affecting air mobility operations.

4.7. Defense Intelligence Agency (DIA).

4.7.1. Serves as the single point of contact for the TWG to DIA for intelligence and FP issues.

4.7.2. Provides tailored, finished intelligence support to the TWG.

4.7.3. Coordinates and ensures DIA terrorism analysis and assessments are made available to the TWG.

4.7.4. Supports the TWG by ensuring both RFIs and collection requirements generated by the TWG are given the proper visibility within DIA.

4.7.5. Oversees DIA input to TWG risk assessments, airfield surveys, and the general security situation in various countries.

4.7.6. Functions as DIA's Defense Human Intelligence (HUMINT) Service Representative when none is present for duty.

4.8. Defense Intelligence Agency/Defense HUMINT Service (DIA/DHS).

4.8.1. In concert with USTC Collection Management Office and A2 as appropriate, DHS will coordinate HUMINT collection with DHS Headquarters and the Defense Attaché Offices (DAO).

4.8.2. As required, communicates directly with DAOs to support TWG actions of an urgent or crisis nature.

4.8.3. Advises the TWG on Defense HUMINT Service (DHS) collection activities as appropriate.

4.8.4. Oversees DHS input of TWG risk assessments, airfield surveys, and the general security situation in various countries.

4.9. National Reconnaissance Office (NRO).

4.9.1. Serves as single point of contact for the TWG to the National Reconnaissance Office for space, intelligence and FP issues.

4.9.2. Serves as the TWG advisor regarding NRO Systems capabilities and limitations issues.

4.9.3. Develops and coordinates assessments and recommendations concerning National Systems support and future developments affecting TWG requirements.

4.10. 67th Information Warfare Flight (67th IWF).

4.10.1. Serves as the single point of contact for the TWG to the Air Intelligence Agency (AIA) for intelligence and information operations issues.

4.10.2. Under the TACON of TACC/XOC, 67 IWF provides the TWG with Information Operations (IO) threat expertise to improve situational awareness and facilitate courses of action.

4.10.3. Develops and coordinates assessments and recommendations concerning information warfare threats affecting AMC missions for publication in TWG VRAs. The TWG will use this information to assess the overall threat to AMC missions.

4.10.4. Provides OPSEC oversight to the TWG to protect operational information from adversaries. Provides IA and CND policy guidance and oversight as well as CND event notification to the TWG to protect friendly operations information from hostile sources when such sources are identified and potentially threaten AMC operations.

4.10.5. Engages other AMC and USTC units/offices as required to facilitate TWG issues and tasks.

4.11. Director of Communications (A6).

4.11.1. Secure, reliable communications and computer system support are integral to the entire spectrum of in-transit, pre-deployment, deployment, post-deployment, and steady state AMC operations. Planners must consider the security and reliability of deployed location communications.

4.11.2. The A6 representative will:

4.11.2.1. Ensure communications and systems issues related to TWG processes are addressed in daily TWG meetings.

4.11.2.2. Provide communications and computer systems threat updates and mitigation recommendations when requested for inclusion into the VRA.

STEVEN R. CAPENOS, Colonel, USAF
Director of Intelligence

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*
Joint Pub 3-07-2, *Joint Tactics, Techniques, and Procedures for Anti-terrorism*
USTC 31-2, *Security Awareness Guide to Combating Terrorism*
AFPD 71-1, *Criminal Investigations and Counterintelligence*
AFI 10-245, *Air Force Antiterrorism (AT) Standards*
AFI 10-245, *AMC supplement*
AFI 11-2 SAMV3, *Special Air Mission (SAM) Operations Procedures*
AFI 14-105, *Unit Intelligence Mission and Responsibilities*
AFI 14-119, *Intelligence Support to Force Protection (FP)*
AFI 31-101, Volume 2, *The Air Force Physical Security Program*
AFJI 31-102, *Physical Security*
AFI 31-209, *Air Force Resource Protection Program*
AFOSI Instruction 71-104, Volume 1, *Counterintelligence and Security Services*
AMCI 11-208, *Tanker/Airlift Operations*
AMCI 14-102, *Debriefing and Reporting*
AMCPAM 14-104, *Air Mobility Command Intelligence Cookbook*

Abbreviations and Acronyms

A2—Director of Intelligence
A3—Director of Operations
AFI—Air Force Instruction
AFOSI—Air Force Office of Special Investigations
AFPD—Air Force Policy Directive
AIA—Air Intelligence Agency
AMC—Air Mobility Command
AMCI—Air Mobility Command Instruction
AMW—Air Mobility Wing
AO—Action Officer
AOC—Air Operations Center

AW—Airlift Wing
AT—Antiterrorism
CI—Counterintelligence
CIA—Central Intelligence Agency
CJCS—Chairman, Joint Chiefs of Staff
COMSEC—Communications Security
CONOPS—Concept of Operations
CND—Computer Network Defense
CRAF—Civil Reserve Air Fleet
CSG—Cryptologic Services Group
CSS—Central Security Service
CT—Counterterrorism
DAO—Defense Attaché Office
DCI—Director of Central Intelligence
DDI—Duty Director for Intelligence
DHS—Defense HUMINT Services
DIA—Defense Intelligence Agency
DOD—Department of Defense
DS—Defensive Systems
EI—Essential Elements of Information
FAA—Federal Aviation Administration
FHP—Force Health Protection
FP—Force Protection
GDSS—Global Decision Support System
HUMINT—Human Resource Intelligence
I&W—Indications and Warning
IIR—Intelligence Information Report
IMINT—Imagery Intelligence
IN—Chief of Intelligence (Wing, Group)
IN—Information Needs
IA—Information Assurance
IO—Information Operations

IW—Information Warfare
J2—Director of Intelligence (Joint Command)
JIC—Joint Intelligence Center
JITF-CT—Joint Intelligence Task Force - Counterterrorism
JWICS—Joint Worldwide Intelligence Communications System
LEP—Laser Eye Protection
MANPADS—Man Portable Air Defense System
MC&G—Mapping, Charting, and Geodesy
MISREPS—Mission Reports
MOG—Maximum on Ground
NAR—National Agency Representative
NGA—National Geospatial Intelligence Agency
NRO—National Reconnaissance Office
NSA—National Security Agency
NSRP—National SIGINT Requirements Program
OPLAN—Operations Plan
OPORD—Operations Order
OPR—Office of Primary Responsibility
OPSEC—Operations Security
RFI—Request for Information
RON—Remain Over Night
RSO—Regional Security Officer
SCI—Sensitive Compartmented Information
SCIF—Sensitive Compartmented Information Facility
SIGINT—Signals Intelligence
SIPRNET—Secret Internet Protocol Network
SITREP—Situation Report
SF—Security Forces
SSA—Special Support Activity
TACC—Tanker Airlift Control Center
TALCE—Tanker Airlift Control Element
TOC—Threat Operations Center

TSA—Transportation Security Administration

TTPs—Tactics, Techniques, and Procedures

TWG—Threat Working Group

TWL—TWG Watch List

USCS—United States Cryptologic System

USTC—United States Transportation Command

VRA—Virtual Risk Assessment

VRAD—Virtual Risk Assessment Database

VTC—Video Teleconference

Terms

AMC Policy Matrix—Approved A3 FP policies are published in the AMC Policy Matrix and made available to mission planners and executors worldwide via A2's SIPRNET website (<http://amcin.scott.af.smil.mil>). This product is provided as a quick reference tool, summarizing the policies listed in each VRA. The Policy Matrix does not replace the VRA. Each policy block in the matrix is expanded in the remarks section of the VRA (explained further in section 3.2) and must be reviewed by crews and mission planners at all levels prior to initiating operational planning.

Anti-terrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations, etc. conducted for, or on behalf of, foreign powers, organizations, or persons; or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Counterterrorism—Offensive measures taken to prevent, deter and respond to terrorism.

Force Health Protection (FHP)—Integrated preventive, surveillance, and clinical programs designed to protect the 'total force.' The goal of FHP is to provide a fit and healthy force when and where the mission requires. FHP is about preventing medical threats from affecting military forces. It is designed to improve existing health, proactively address health threats, and finally provide care for any illness or injury that does occur.

Information—Data and the instructions required giving that data meaning.

Information Warfare (IW)—IW is action taken to deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations, while protecting friendly forces against similar actions.

MANPADS—The Man Portable Air Defense System (MANPADS) is an effective series of weapons proliferated worldwide. Having great mobility, relatively low cost, and simple operation, these missile systems are popular among non-state actors such as terrorist and insurgent groups. These systems represent one of the greatest threats to mobility aircraft. Typically containing an Infrared (IR) seeker, these systems often offer little opportunity for a warning before impact.

Non-Raven Required Locations List—This list identifies airfields where security is sufficient to justify

stopping AMC aircraft without an on-board security team. Aircraft transiting all other locations require on-board Phoenix Raven support.

Operations Security (OPSEC)—A process identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems; determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together; or select and execute measures that eliminate, or reduce to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation.

Phoenix Raven Team—Two to six-person security team tasked with providing close-in security for AMC aircraft at OCONUS areas where the local security has been assessed as inadequate or the security situation is not fully known.

Technical Stop List—The Technical Stop List will contain commercial airports approved for contracted carriers to make passenger and cargo technical stops.

TWG Watch List (TWL)—The TWG Watch List is a list of countries, broken into Tiers based on threat level, which defines VRA production requirements and sets operations policy. The TWG Watch List is approved by the A3.

Virtual Risk Assessment (VRA)—A VRA is an online document published on the A2 SIPRNET website that includes threat assessments and A3-approved policies for an airfield or country.

Virtual Risk Assessment Database (VRAD)—The VRAD is a compilation of all VRAs into an online SIPRNET database accessible worldwide from the A2 website (<http://www.amcin.scott.af.smil.mil>).