

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE HANDBOOK 31-115,  
VOLUME 1**



**29 APRIL 2015**

Certified Current 7 April 2016

**Security**

**SECURITY FORCES SUPPORT TO THREAT  
INFORMATION INTEGRATION**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** This publication is available for downloading or ordering on the e-Publishing website at [www.e-publishing.af.mil](http://www.e-publishing.af.mil).

**RELEASABILITY:** There are no restrictions on the release of this handbook.

---

OPR: AF/A4SO

Certified by: AF/A4S  
(Brig Gen Allen J. Jamerson)

Pages: 48

---

This Air Force Handbook (AFH) complements and amplifies guidance in AFI 31-101, *Integrated Defense*, and contributes to the Security Forces' mission of securing Department of Defense (DoD) and Air Force assets. This publication outlines the role of the Security Forces liaison contributing to Threat Information Integration (TII). Actions outlined in this publication should be considered baseline measures for Security Forces Staff S-2 function personnel to perform during Integrated Defense (ID) operations within the Continental United States (CONUS). These baseline measures can and should be expanded when operations are performed in Outside Continental United States (OCONUS) and expeditionary environments based on increased capabilities and/or restrictions. It provides baseline tactical-level guidance for Security Forces personnel contributing to TII. It identifies tasks Security Forces should be completing, and methods on how to complete them. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS) located at <https://www.my.af.mil/gcss-af61a/frims/frims/>. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*, and route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

<b>Chapter 1—S2 ROLE IN INTEGRATED DEFENSE (ID)</b>	<b>3</b>
1.1. Organization and Role. ....	3
1.2. Training. ....	4
1.3. Equipment. ....	5
<b>Chapter 2—THREAT INFORMATION INTEGRATION OVERVIEW</b>	<b>7</b>
2.1. Information Sharing. ....	7
2.2. Information Integration. ....	10
2.3. Threat Information Integration. ....	10
<b>Chapter 3—OPERATIONAL PROCESSES</b>	<b>13</b>
3.1. Scope of Effort. ....	13
3.2. Data Integration Process. ....	14
Figure 3.1. Source Reliability/Information Validity Matrix. ....	15
3.3. Ground Tasking Order Process. ....	22
Figure 3.2. Ground Tasking Order Process. ....	23
<b>Chapter 4—INTELLIGENCE PREPARATION OF THE BATTLESPACE</b>	<b>25</b>
4.1. Introduction. ....	25
4.2. Step 1 – Define The Battlespace Environment. ....	25
4.3. Step 2 – Describe The Battlespace’s Effects. ....	27
4.4. Step 3 – Evaluate The Threat. ....	28
4.5. Step 4 – Determine Threat COAs. ....	31
4.6. Tips for Success. ....	32
<b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>34</b>
<b>Attachment 2—REQUEST FOR INFORMATION (RFI) EXAMPLES</b>	<b>40</b>
<b>Attachment 3—PATTERN ANALYSIS EXAMPLE</b>	<b>41</b>
<b>Attachment 4—SITUATIONAL AWARENESS BULLETIN EXAMPLE</b>	<b>42</b>
<b>Attachment 5—STORYBOARD EXAMPLE</b>	<b>44</b>
<b>Attachment 6—GROUND TASKING ORDER EXAMPLE</b>	<b>45</b>
<b>Attachment 7—PATROL AFTER ACTION REPORT (PAAR)</b>	<b>46</b>
<b>Attachment 8—AREA OF INTEREST MAP</b>	<b>47</b>
<b>Attachment 9—MODIFIED COMBINED OBSTACLE OVERLAY</b>	<b>48</b>

## Chapter 1

### S2 ROLE IN INTEGRATED DEFENSE (ID)

**1.1. Organization and Role.** NOTE: For the purpose of this handbook, all references to battlespace refer to the Base Security Zone (BSZ) and areas within the BSZ. Additionally, the terms “information” and “data” are used interchangeably within this document.

1.1.1. In accordance with AFPD 31-1, *Integrated Defense*, “It is an Installation Commander’s inherent responsibility to identify risks and develop risk management strategies to produce effects-based, integrated defense plans to ensure unhindered Air Force, Joint and Coalition missions.” ID incorporates multidisciplinary active and passive, offense and defense capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations. Per AFI 31-101 one of the key tasks of creating flexible, responsive ID operations within varying threat environments is to operationalize force protection intelligence (FPI). This can be accomplished for the Defense Force Commander (DFC) through the development of a robust intelligence/information collaboration, analysis and fusion capability.

1.1.1.1. It is important to note DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*, prescribes how DoD Criminal Intelligence (CRIMINT) collection, maintenance, use, and dissemination of personally identifiable information and law enforcement information will occur. Additionally, in accordance with DoDD 5200.27 the gathering of CRIMINT and predictive intelligence (PI) regarding persons without a connection to DoD or reasonable expectation of threat or direction of interest toward DoD personnel or facilities is prohibited. Additional policies and guidance regarding DoD CRIMINT activities are outlined in DoDI 5525.18, *Law Enforcement Criminal Intelligence (CRIMINT) in DoD*.

1.1.1.2. Further, due diligence should be given to intelligence oversight issues when carrying out the FPI process. The duties and obligations placed on DOD intelligence organizations to protect the rights of individuals stem from the U.S. Constitution, Presidential Executive Order 12333, and DOD Regulation 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, which spells out how the Presidential Executive Order applies to Defense intelligence activities.

1.1.2. The Security Forces S2 is responsible for coordinating with Air Force Office of Special Investigation (AFOSI) and the appropriate level intelligence FPI representative to facilitate Threat Information Integration. The goal of this coordination is to provide the DFC the information required to conduct ID operations.

1.1.2.1. The S2 contributes law enforcement data within Security Forces purview, to include data in the Security Forces Management Information System (SFMIS) and from debriefings of security/law enforcement patrols within the installation’s Area of Interest (AOI).

1.1.2.2. AFOSI is responsible for contributing information/intelligence derived from independent criminal investigations, counterintelligence activities, and specialized

investigative and force protection support as well as information gleaned from liaison with federal, state, local and foreign nation law enforcement, counterintelligence and security agencies. Per AFI 71-101, Volume 1, *Criminal Investigations Program*, AFOSI is the AF interface between the JTTFs, FBI and local law enforcement for suspicious activity reporting.

1.1.2.3. The FPI representative is responsible for coordination of force protection-related products (i.e. daily intelligence summaries, terrorist handbooks, threat documents and briefings, etc.) and services with AFOSI to de-conflict responsibilities and ensure S2 requirements are satisfied. The FPI representative is also responsible for providing Intelligence Preparation of the Battlespace (IPB). The S2 will use information generated by the TII process to keep the DFC (and through the DFC, the Installation Commander) aware of the circumstances, patterns, trends, or incidents regarding criminal intelligence related to SF operations.

1.1.3. The DFC is the approval authority for all products generated by the S2 released within the security forces squadron. Material produced collaboratively by the TII or expected to be released outside of security forces should be coordinated with all TII functional areas (i.e., DFC, AFOSI Detachment Commander (DetCo), Senior Intelligence Officer) prior to dissemination outside their agencies or their respective chains of command. Products generated by the collaborative agencies and the S2 are discussed in greater detail in Chapter 3.

**1.2. Training.** To provide effective situational awareness to the DFC, the S2 must be able to contextualize all-source information for the purpose of supporting ID operations. This requires skills similar to many civilian law enforcement criminal intelligence analysis functions. This type of training is readily available through multiple venues and it is the responsibility of each DFC to assess the skill level of their S2 personnel. The DFC is also responsible for determining which type of training would best suit the S2. DoDI 5525.18 requires analysis of CRIMINT to be accomplished by analysts that possess professional training and practical experiences consistent with the professional standards articulated by the International Association of LE Intelligence Analysts. Other courses may take an IC approach and train in accordance with Intelligence Community Directive (ICD) 203, *Analytic Standards*. Regardless of which venue, the goal of this training is to facilitate more effective communication between TII contributors by teaching the S2 how analysts perform their mission and allow the S2 to “speak the same language” as OSI and intelligence representatives rather than turn the S2 into an intelligence analyst. Additionally, this type of training will teach the S2 what their agencies bring to the fight which will help them better shape their requests for information when needed. The following are venues where these skills can be acquired.

1.2.1. The Air Mobility Command’s Force Protection Intelligence Formal Training Unit (FP IFTU) course. This course provides basic FPI skills necessary to conduct intelligence preparation of the operating environment (IPOE) and intelligence preparation of the battlefield (IPB) as well as an introduction to the intelligence community (IC) and the basics of analytical tools and processes.

1.2.2. Another venue is the Army Intelligence Analyst Course. Additionally, S2s should consider pursuing courses taught or administered by/through Army Knowledge Online (AKO), the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), the

Defense Security Service (DSS), and the Advanced Global Intelligence Learning Environment (AGILE)(<https://www.agile.mil>).

1.2.3. Certification is not required to perform S2 duties within the Security Forces purview. Certification through national-level agencies can, however, enhance relationships through establishing credibility recognized across the Criminal Intelligence Analysis enterprise. The Foundations of Intelligence Analysis Training Program taught through the Association of Law Enforcement Intelligence Units and the National White Collar Crime Center (NW3C) is widely used and can greatly contribute toward establishing the communication skills necessary for the S2.

1.2.4. Many low-cost or no-cost training options are available. These options should be considered and exploited to the greatest extent possible. Training can be requested/conducted through organic installation training venues per AFI 14-119, *Intelligence Support to Force Protection*.

1.2.4.1. Awareness. The broadest, most diverse types of intelligence training could best be described as “awareness” training. These programs, which vary in length from 2 hours to 4 days, tend to include information about the intelligence discipline (i.e., definitions, methods, processes, etc.) as integrated with a specific subject matter (e.g., drugs, terrorism, auto theft). The Bureau of Justice Assistance State and Local Antiterrorism Training (SLATT), Federal Law Enforcement Training Center (FLETC), and other groups offer this training throughout the country.

1.2.4.2. Intelligence Analyst. Intelligence analysts training programs have a reasonable degree of consistency in the subject matter topics; however, the hours of training on each topic have more variance. In some cases, the curricula include substantive modules on subject matter. For example, the FBI Center for Intelligence Training program integrates intelligence methods specifically with crimes within FBI jurisdiction. Similarly, DEA curricula integrates intelligence methods with material on drug trafficking.

1.2.4.3. Specialized Training. This training focuses on a narrow aspect of the entire intelligence process and/or specific tools available to intelligence analysts. Courses that fall into this category are generally software courses such as classes on how to use a particular type of intelligence software (typically either analytic software or databases).

### **1.3. Equipment.**

1.3.1. In order to effectively perform their duties in support of the Integrated Defense Risk Management Process (IDRMP), the S2 should, at a minimum, be provided the following equipment/resources:

1.3.1.1. Computer workstation with Non-classified Internet Protocol Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) connectivity.

1.3.1.2. Microsoft Office<sup>®</sup> for word-processing, document publication, and spreadsheet support.

1.3.1.3. Adobe Pro<sup>®</sup> for product development and protection.

1.3.1.4. Access to authoritative databases and systems such as eGuardian (Law Enforcement Online (LEO)), State/National Crime Information Center systems (NCIC),

Regional Information Sharing Systems (RISS), and the Homeland Security Information Network.

1.3.1.5. Google Earth Client<sup>®</sup>

1.3.1.6. Tools for data consolidation and/or collaboration (e.g., analysis software (as necessary), i2 COPLINK<sup>®</sup>).

## Chapter 2

### THREAT INFORMATION INTEGRATION OVERVIEW

**2.1. Information Sharing.** The need to develop and share information has significantly changed in recent years. Experience □ both good and bad □ has reinforced the premise that threat mitigation is contingent upon the ability to gather, evaluate and share information and intelligence regarding those who intend to attack Air Force assets; the tactics, techniques, and procedures they use; and the targets they intend to select. Information sharing procedures ensure data and analysis are placed in the hands of the appropriate entities in a timely manner. Whether the aggressor is a trained operative from an international terrorist organization, a self-radicalized lone offender, or a disgruntled individual, risk mitigation is contingent upon an environment that facilitates the continual and rapid exchange of information. Information sharing also fosters an environment in which individuals possess a common baseline of familiarity with threat information. That framework permits faster identification and contextualization of new or changing threats, minimizing the time it takes to start mitigation procedures for legitimate concerns, and decreasing time wasted on items of negligible concern. The following sections contextualize the information sharing environment and provide the foundation for information sharing at the installation level.

2.1.1. Guiding Principles for Information Sharing. Entities responsible for combating and responding to malevolent threats along the threat continuum must have access to timely and accurate information regarding potential threat actors. That information guides combined efforts to:

2.1.1.1. Identify immediate and long-term threats.

2.1.1.2. Identify persons and/or groups involved in threat-related activities.

2.1.1.3. Identify tactics and capabilities of known persons and/or groups.

2.1.1.4. Identify potential targets.

2.1.1.5. Facilitate efforts to conduct Intelligence Preparation of the Battlespace (IPB).

2.1.1.6. Implement information-driven and risk-based detection, prevention, deterrence, response, protection, and emergency management efforts that yield effects which support mission assurance.

2.1.2. Information Sources. Criminal and terrorism-related intelligence is best derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for threat-related information. It can materialize through the efforts of the intelligence community, law enforcement authorities (both military and civilian), other government agencies, public and private sector sources, as well as open sources.

2.1.2.1. Since the events of September 11, 2001, the focus of information sharing has pertained to terrorism; however, the need for collaboration extends beyond terrorism-related issues to encompass all aspects of Force Protection Information as defined in AFI 14-119, *Intelligence Support to Force Protection*. Force Protection is defined in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, as

preventive measures taken to mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information.

2.1.2.2. Information does not typically come neatly packaged and labeled to indicate its subject matter or domain of interest. Information from one domain may prove valuable in another, often at a different time and in another form.

2.1.3. Information Sharing Foundations. The following core principles and understandings, adopted from the *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism Related Information Sharing* (2007), serve as a foundation for implementing an effective information sharing program:

2.1.3.1. Strong Partnerships. Effective information sharing comes through strong partnerships among key principals and stakeholders (e.g., AFOSI, Security Forces, Intelligence, Operations, Emergency Management, etc.). Strong partnerships build investments in cross-organizational interaction that outlast mission stressors and personnel turnover.

2.1.3.2. Collaboration. To maximize information sharing, key principals/stakeholders must communicate and collaborate. The objective is to leverage resources and expertise while improving the ability to detect and prevent threat activity. Fostering a collaborative environment builds trust among participating entities, strengthens partnerships, and creates individual and collective ownership in the overall force protection mission. The purpose of collaboration is to increase capacity, communication and continuity of service while decreasing duplication. Collaboration also provides key principals access to bodies of information not normally accessible within their purview, permitting a comprehensive view of threat data. All units on an installation support the installation commander. Ultimately, the goal of information integration is to provide the installation commander the information needed to protect his/her installation, resources, and personnel.

2.1.3.3. Functional Awareness. Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, to information from other sources. Successful information sharing relationships endure because key principals are aware of the requirements and challenges, background and worldview of all other members.

2.1.3.4. Information Sharing Culture. Information sharing must be woven into all aspects of TII, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, incident preparedness, and response to and recovery from catastrophic incidents.

2.1.3.4.1. Interconnectivity. Key force protection principals must communicate effectively. The ultimate goal is to eliminate barriers to communications, close gaps in mission essential information cross flow, and develop and exchange information vital to protecting installation personnel and resources.

2.1.3.4.2. Multidisciplinary Awareness and Education. All personnel should be trained to identify suspicious activities or threats and provide information to appropriate personnel. Specific training should pertain to the identification and reporting of suspicious anomalies or behavioral indicators that may be indicative of potential criminal or terrorist activity.

2.1.3.4.3. Reporting Mechanisms. Personnel must be familiar with local reporting requirements and have the ability to utilize the variety of different resources to exchange information. Reporting mechanisms include, but are not limited to, 911 systems, installation Eagle Eyes program, Crime Stop lines, eGuardian, and routine numbers for on- and off-installation law enforcement agencies. Intelligence community reports include SITREPS, Spot Reports and a host of different vehicles pertaining to diverse domestic and global developments or impending incidents. These reporting mechanisms provide the preponderance of tactical-level information that ultimately form the foundation for risk mitigation planning efforts.

2.1.3.5. Intelligent Integration and Mutual Respect. The procedures, processes and systems that support information sharing must draw upon and integrate existing technical capabilities and must respect established functional authorities and responsibilities.

2.1.3.5.1. To the greatest extent possible, agencies participating in information sharing endeavors should leverage existing information sharing initiatives. Leveraging the databases and systems already available via participating entities will help maximize information sharing and eliminate redundancy.

2.1.3.5.2. The core contributors of the TII process should be comprised of SFS/S2, AFOSI, and appropriate level FPI representatives. Additional members, such as medical intelligence, civil engineers, etc. may be added at the Installation Commander's direction.

2.1.3.5.2.1. It is important to note that no single functional area owns the threat information integration process. The process, as well as the members present, support the installation commander.

2.1.3.5.2.2. At its core, threat information integration is simply sharing data with other functional areas with the overall goal of increasing the analytic capability of installations to identify and process what is known and unknown regarding threats. The TII functional areas must work together to achieve a systematic, mutually-supportive, and collaborative information-sharing environment that serves the information needs of all force protection entities on the installation. Each TII collaborator represents a conduit of information and/or intelligence from his or her agency that can infuse agency-specific information into the collective body of information for analysis. While TII is designed to be a collaborative effort between intelligence and information hubs, Operational Control (OPCON), Tactical Control (TACON) and Administrative Control (ADCON) of the contributing members remain with the owning commander of each of these functional areas.

2.1.3.5.3. Clearly defining the TII roles of participating agencies in the Integrated Defense Plan (IDP) is necessary to define the terms, responsibilities, relationships, intentions, and commitments of each participating entity. The IDP should also provide an outline of the "who, what, where, when, why, and how" of TII. Participating agencies will become greater stakeholders to the process and be more inclined to hold to the policies defined within this installation plan. Information sharing can be, and often is, facilitated in a virtual environment.

2.1.3.6. Outreach and Partnerships. Higher Headquarters (e.g., MAJCOM, NAF) information sharing organizations and agencies represent a valuable information sharing resource and should be incorporated into information sharing frameworks as much as possible. Official liaison relationships should be established at the appropriate levels in accordance with existing policy.

**2.2. Information Integration.** The concept of information integration has emerged as the fundamental process to facilitate the sharing of threat information. The ultimate goal of integration from the perspective of the S2 is to ensure that intelligence and/or information shared under the guidelines above is of the best possible quality and enables Integrated Defense (ID) forces to achieve the desired effect of Anticipation. For the purpose of this guide, integration refers to the overarching process of assimilating information and/or intelligence from contributing agencies identified by the installation commander to achieve the desired FP effects of detect, deter, preempt, negate, and mitigate. It goes beyond establishing an information/intelligence center or creating a computer network. TII members need to minimize/delete redundancy by being knowledgeable and respecting each agency's primary role(s) in TII and avoiding overlap. The information integration process supports the planning and implementation of the IDRMP as outlined in AFI 31-101.

2.2.1. Data integration is the process of gathering and evaluating information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected enemy, hostile or potentially hostile activity. It draws on the complementary strengths of all intelligence disciplines, and relies on an all-source approach to intelligence collection and analysis. Data integration is an on-going process involving the delineation of roles and responsibilities; creating requirements; and collecting, integrating, evaluating, and disseminating critical information-not all of which tasks are conducted by S2 personnel.

2.2.1.1. Data integration also involves the exchange of information from different sources including law enforcement, public safety, and the private sector, with analysis and synthesis resulting in meaningful and credible intelligence while adhering to existing policy and law. Integration also allows for continual reevaluation of existing data in context with new data in order to provide constant updates and more comprehensive situational awareness of the local operating environment.

2.2.1.2. Data integration relies on collection and analysis efforts that optimize the strengths of the different sources. Information is sought from the widest possible range of sources to avoid any bias that can result from relying on a single source of information and to improve the accuracy and completeness of intelligence. The collection of information from multiple sources is essential to countering the adversary's operations security and deception operations.

**2.3. Threat Information Integration.** The purpose of the functional communities participating in threat information integration is to proactively seek out, evaluate and share information in order to identify threats to the installation and its resources. The role of the SF/S2 in TII is to liaise with subject matter experts (SMEs) from AFOSI and intelligence communities to ensure the most complete and credible threat picture is provided to the installation commander. A primary focus of TII is the intelligence and information integration process, through which information is collected, evaluated, and disseminated. Nontraditional providers of this type of information, such as Security Forces, Explosive Ordnance Disposal, the general population, and

private sector organizations, possess important information (e.g., crimestop and suspicious activity reports) that can be “integrated” with other data, IAW established policy and law, to provide meaningful information and intelligence about potential terrorist threats and criminal activity in a timely manner.

2.3.1. Interagency intelligence collaboration should be encouraged whenever possible consistent with applicable National, Joint, Departmental, and USAF policy, or organizational procedures and classification guidelines. Successful interagency intelligence collaboration depends upon many factors, to include: strong relationship networks, trust and respect among colleagues, sharing a common vision, minimizing territorial issues, continuous communication, and commitment from the leadership of collaborating organizations. Liaison personnel are instrumental in bridging gaps and working through barriers that may arise between organizations. An aggressive liaison effort is critical to developing and maintaining unity of effort from initial planning through execution. However, analysts must base their collaboration on classification, need-to-know, need-to-share, applicable law, and national, DoD, service, agency or organizational guidelines. Regardless of the basis for collaboration, all TII is conducted IAW Intelligence Oversight rules.

2.3.2. The following principles for interagency information/intelligence collaboration should be adhered to during TII:

2.3.2.1. Establish Strong Relationship Networks. Collaboration is built upon the relationships and networks of colleagues developed throughout their careers. Without knowledge of who one’s subject matter experts are in intelligence organizations, collaboration on assessing the threat is nearly impossible. Techniques for building relationship networks include attending or hosting conferences, visiting counterparts in other organizations and exchanges of personnel through inter-organizational rotational assignments.

2.3.2.2. Build Mutual Trust and Respect among Colleagues. As evaluators work intelligence problems, they count on one another to share all relevant data from within their particular field of expertise. Trust and respect is facilitated by proactively communicating information to colleagues and counterparts and by ensuring they are recognized by their organizations for their expertise and contributions.

2.3.2.3. Share a Common Vision. This shared common vision starts with the commander’s intent. A shared common vision should include the goal of providing the most comprehensive, accurate Local Threat Assessment (LTA) possible to the customer (i.e., Installation Commander and functional chains of command). It should be noted that AFOSI also produces an annual Criminal Threat Assessment (CTA) that is provided to the Installation Commander and the Security Forces. The combination of both assessments should provide the necessary awareness to execute FP activities. Sharing a common goal among collaborators is facilitated by taking the initiative to alert others when new information becomes available, working together instead of competing and tipping off the target of information/intelligence collection. By synchronizing efforts, the strengths of each community can be maximized for the benefit of all collaborators.

2.3.2.4. Minimize Territorial Issues. Reducing the potential for inter-organizational conflicts is vital to successful intelligence collaboration. It is important an S2 embarking on a collaborative effort recognize that turf issues are likely to occur and should not be

ignored. These issues may be minimized by anticipating their occurrence, developing a plan for addressing them as they emerge and stressing the mutually beneficial aspects of collaboration such as sharing organizational credit for the final product(s). AF participants in threat information integration should have a clear understanding of standing installation FP information/intelligence requirements, the capabilities and limitations of their respective organization's mission as it relates to intelligence, counterintelligence, threat collections, investigations and law enforcement liaison. A clear understanding of these lanes in the road will help to minimize territorial issues.

2.3.2.5. Encourage Continuous Communication. Continuous communication among data sharing colleagues and counterparts is critical to overcoming barriers to collaboration. Communication may be enhanced through frequent meetings, teleconferences, phone calls, e-mail, and other sources of dialogue, as well as less formal methods such as periodic working lunches.

## Chapter 3

### OPERATIONAL PROCESSES

#### 3.1. Scope of Effort.

3.1.1. The focus of the S2 is to enhance effects-based security operations at the installation level by conscientiously and continuously monitoring current and developing threats within the BSZ and the AOI, maintaining ever vigilant situational awareness, and providing accurate and timely assessments to Security Forces decision makers with the goal of achieving the ID effect of Anticipation.

3.1.2. Information requirements are primarily based upon the installation LTA and CTA. Additionally, reports, assessments, observations, and tactical-level information (e.g., field interviews, patrol reports, etc.) collected locally will be considered and/or utilized to ensure the S2 has both a “macro” and “micro” view of the potential threat environment. This continuous integration of information from multiple levels will assist the S2 in maintaining situational awareness of threats to the installation. The S2 must guard against simply forwarding information; intelligence and data obtained from other sources must be evaluated for pertinence and forwarded as appropriate.

3.1.2.1. Information and Intelligence Requirements. S2s should leverage installation Threat Working Groups (TWG) that are required to develop and refine terrorism threat assessments. TWGs should develop a threat matrix from the analysis of the LTA. If properly completed, the threat matrix will identify the Design Basis Threat (DBT) for all identified threats. If gaps in information exist, the TII process should be leveraged to fill threat information gaps to meet the Installation Commander’s Critical Information Requirements (CCIR) in order to facilitate the COA development process. The S2 must know where to submit requests for information in order to close remaining information gaps. For this very reason it is imperative that the S2 be an integral part of ID planning and risk analysis processes. If, during ID planning, it is determined that insufficient information is available to make an informed decision (i.e., during enemy course of action (COA) or friendly COA development), the S2 should identify the information gap and initiate contact with (or through) AFOSI, local law enforcement agencies (IAW the AFOSI and SF investigative matrix) and/or the FPI representative, as applicable, to gain additional information in order to better formulate recommendations for risk decision-makers. Every effort should be made to seek out already published products and assessments that may fill information gaps prior to initiating a Requests for Information (RFIs) to meet Commander Critical Information Requirements (CCIR), based on unfilled Priority Intelligence Requirement (PIR) and/or Friendly Forces Information Requirement (FFIR).

3.1.2.2. If, after exhausting all other means and methods, information gaps still exist, the S2 should submit an RFI (See Attachment 2) to the appropriate agency, normally through the AFOSI or FPI representative. Good RFIs have three things in common: they ask only one question (e.g., inquire about enemy status or action); they focus on a specific fact, incident, or activity; and they provide the intelligence required to support a single decision (e.g., if the enemy does *this*, then I have to decide what to do). AFOSI and/or

FPI representatives can assist the S2 in drafting the RFI by focusing on the correct questions to ask.

**3.2. Data Integration Process.** The TII process leverages all-source intelligence to identify and evaluate threats that may affect installation personnel, assets, infrastructure, information and resources. This includes threats to the installation from foreign actors, domestic terrorists, sophisticated and unsophisticated criminals, vandals, protestors, narcotics trafficking, or hate groups; suspicious or possible pre-operational activity reporting; and correlation with incidents, intelligence, and law enforcement products related to the protection of installation resources.

3.2.1. Step 1 – Identify the incident. The first step in this process is initiated when an incident occurs or information is received that either directly affects the installation or is of such significance it must be monitored for aggressor tactic, technique, or procedure (TTP) value and/or situational awareness. A TWG may be convened and leverage TII to gather information about the incident from a variety of sources to include open source media reporting; however, the most likely (and preferred) sources will be information-sharing networks like the Homeland Security Information Network (HSIN) or LEO.

3.2.2. Step 2 – Threat Categorization. The second step is to evaluate the information that has been received and determine the threat posed to installation assets. The S2 shares this information with other TII stakeholders and the S2's chain of command IAW established policy and law. Subsequently, the threat posed is categorized by the Installation Commander. Classification will determine subsequent TII actions and fall into one of three categories:

3.2.2.1. Threat: If the S2 believes the data reveals a threat to the installation or its assets, the S2 will immediately report this information to the DFC. This may initiate a Threat Working Group (TWG) and S2 and other TII participants should attempt to develop as much information as possible about the threat.

3.2.2.2. Unknown: If the nature of the information and its potential threat is unknown, the S2 will continue to monitor/evaluate and seek further information until termination. The S2 should utilize their best judgment or a pre-coordinated notification matrix to determine whether this situation warrants immediate notification to their chain of command.

3.2.2.3. No Threat: If the information does not represent a threat to the installation, the S2 will continue to monitor the situation for potential TTP identification and situational awareness.

3.2.3. Step 3 – Information Evaluation. In the third step, the S2 evaluates data through a structured process to determine its value and relevance. During this processing/exploitation step, the S2 sifts out the useless, non-relevant and/or incorrect information and then arranges/evaluates the remaining information to establish relationships between seemingly disparate data. The process is designed to scrutinize the source, quality, and legitimacy of the information prior to the analytical phase and consists of three primary decision points.

3.2.3.1. Determination of relevance to the installation. Some questions to consider include:

3.2.3.1.1. Is the information meaningful to the installation?

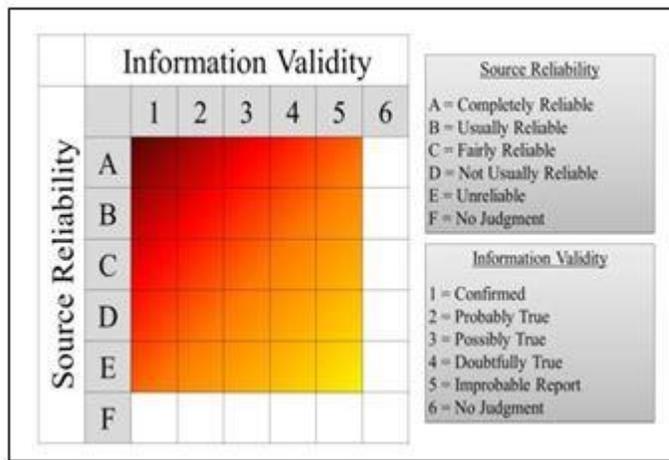
3.2.3.1.2. Does the information have merit? (Both on its own or when combined with other information.)

3.2.3.2. Determination of information reliability based on confidence levels reflected in the source document. Some questions to consider include:

3.2.3.3. Determination of information plausibility/validity. Consider key source information used in the product, addressing factors such as potential strengths and limitations of available information, notable inconsistencies in reporting, important information gaps, or other factors that the producing organization deems relevant.

3.2.3.4. Source reliability and information validity are assessed using the ordinal scale in Figure 3.1. This method, although not foolproof, serves as the baseline procedure for assigning a level of credibility to the information received by the TII contributors. It is important to note that this system is not perfect. A credible source can provide erroneous information and a non-credible source can provide valid information. The credibility of the source and the validity of the information should be assessed individually. NOTE: This information is for informational purposes only as the S2 will not usually be in a position to determine the reliability or validity of a source.

**Figure 3.1. Source Reliability/Information Validity Matrix.**



3.2.4. Step 4 – Analysis: Turning Information into Intelligence (Analysis/Production).

3.2.4.1. The end goal of TII is the collection, assessment and analysis of threat information relating to installation personnel and resources and the subsequent dissemination of information that is actionable to installation leadership. Analysis is the fundamental process where raw data is processed using a scientific approach to problem solving, logical reasoning, and the objective interpretation of data. Analysis establishes connections between the different data, cause and effect, and correlations of activities and behaviors. The new knowledge derived from analysis can provide insights into imminent and emerging threats, as well as potential interdiction methods. TII contributors should:

3.2.4.1.1. Blend data, information, and intelligence received from multiple sources.

3.2.4.1.2. Reconcile, de-conflict, and validate the credibility of data, information, and intelligence received from collection sources.

3.2.4.1.3. Evaluate and examine data and information using SMEs.

3.2.4.1.4. Identify and prioritize the risks facing the installation and tenant units.

3.2.4.1.5. Produce value-added intelligence products that can support the development of performance-driven, risk-based prevention, response, and emergency management programs.

3.2.4.1.6. Coordinate specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages.

3.2.4.2. Analytic Standards. The process used by TII contributors should meet applicable IC and/or LE analytical standards (articulated by the International Association of LE Intelligence Analysts). The following standards are listed in ICD 203:

3.2.4.2.1. Objectivity. S2s need to be able to perform their analytic and informational functions from an unbiased perspective. Analysis should be free of emotional content, give due regard to alternative perspectives and contrary reporting, and acknowledge developments that necessitate adjustment to analytic judgments.

3.2.4.2.2. Independent of Political Consideration. S2s provide objective assessments informed by available information that are not distorted or altered with the intent of supporting or advocating a particular policy, political viewpoint, or audience.

3.2.4.2.3. Timeliness. S2s will strive to deliver their products in time for them to be actionable by customers.

3.2.4.2.4. Based upon all available sources of data/intelligence. The S2's analysis will be based upon all available relevant information. Where critical gaps exist, the S2 will work with collectors (AFOSI and FPI) to develop appropriate collection, dissemination, and access strategies.

3.2.4.2.5. Exhibits Proper Standard of Analytic Tradecraft, specifically:

3.2.4.2.5.1. Properly describes quality and reliability of underlying sources. The S2's products will accurately characterize the information in the underlying sources and explain which information proved key to analytic judgments and why.

3.2.4.2.5.2. Properly caveats and expresses uncertainties or confidence in analytic judgments. S2 products should indicate both the level of confidence in analytic judgment and explain the basis for ascribing it. Sources of uncertainty, including information gaps and significant contrary reporting, are noted and linked logically and consistently to confidence levels in judgments. As appropriate, products will also identify indicators that would enhance or reduce confidence or prompt revision or existing judgments.

3.2.4.2.5.3. Properly distinguishes between underlying intelligence and analysts' assumptions and judgments. S2 products explicitly identify the critical assumptions upon which analysis is based and explain the implications for judgments if those assumptions are incorrect. As appropriate, analytical products

should identify indicators that would signal whether assumptions or judgments are more or less likely to be correct.

3.2.4.2.5.4. Incorporates alternative analysis where appropriate. S2 products identify and explain the strengths and weaknesses of alternative hypotheses, viewpoints, or outcomes in light of both available information and information gaps.

3.2.4.2.5.5. Demonstrates relevance to US national security. S2 products provide information and insight on issues relevant to the products' intended consumers and/or provide useful context, warning, or opportunity analysis.

3.2.4.2.5.6. Uses logical argumentation. S2 analytical presentations should facilitate clear understanding of the information and reasoning underlying analytical judgments.

3.2.4.2.5.7. Exhibits consistency of analysis over time, or highlights change and explains rationale. S2 analytic products should deliver a key message that is either consistent with previous production on the topic from the same analytic element or, if the key analytic message has changed, highlights the change and explains its rationale and implications.

3.2.4.2.5.8. Makes accurate judgments and assessments. Analytic elements should apply expertise and logic to make the most accurate judgments and assessments possible given the information available to the analytic element and known information gaps.

### 3.2.4.3. Critical Thinking.

3.2.4.3.1. Identify and clarify the question/situation. Recognize and clearly identify the true nature of the question/situation. In this regard, S2s will ensure that analysis is based upon clearly defined and logical questions. The questions may come from outside agencies, or they may be analytical starting points established by the S2s themselves. In either case, the intent will be the same – to ensure the question/situation is clearly understood before the analytical process is initiated.

3.2.4.3.2. Gather information. Learn more about the question/situation. Look for possible causes and solutions. Review facts, data, evidence, or previous experiences. Reference existing analysis, bulletins, summaries, other agency products, etc. Ensure collected data supports *multiple* scenarios and not just the scenario one would expect (be objective).

3.2.4.3.3. Evaluate the evidence. Where did the information come from? Does it represent various points of view? What biases could be expected from each source? How accurate is the information gathered? Is it fact or opinion? Can the evidence be corroborated?

3.2.4.3.4. Consider alternatives and implications. Draw conclusions from the gathered evidence and pose solutions. Weigh the particulars of each alternative. *What is the most likely scenario?* Does the evidence suggest a threat? Is the scenario consistent with the threat environment?

3.2.4.3.5. Choose the best action and implement. Select an alternative that is appropriate for the situation (i.e., discard the information, notify the TWG, forward the information for situational awareness, notify an outside agency, etc.) and take action.

3.2.4.4. Analytical Tools. A number of analytic tools are available to S2s. “Tools” essentially refers to methodological techniques that help *organize, integrate, compare, correlate, and illustrate* a body of raw information. None of the tools will produce actionable intelligence alone; each adds a component of new knowledge – or at least new insight – about the data which, collectively, contributes to the analysis and/or leads to the definition of new intelligence requirements. The list below identifies some of the tools that should be used by the S2s in its day-to-day operations.

3.2.4.4.1. Pattern Analysis (See Attachment 3). A generic term for a number of related disciplines such as crime or incident series identification, crime trend analysis, hot spot analysis and can include mapping.

3.2.4.4.2. Analysis of Competing Hypotheses (ACH). The S2 will explicitly identify all the reasonable alternatives for a particular situation and have them “compete” against each other to determine the most plausible option.

3.2.4.4.3. Activity flow. Activity flow shows the steps a criminal or terrorist enterprise uses, indicating exact incidents, dates, and a description of the activities that occurred. The incidents are linked in a flow chart to help understand the progression of the enterprise. The activity flow pieces together a complex organization and may be used for intervention in the enterprise as well as to determine where gaps exist. If gaps are identified, intelligence requirements are used to fill the gaps so that the activity of the enterprise can be fully mapped to aid in prevention and prosecution.

3.2.4.5. An Explanation of Estimative Language.

3.2.4.5.1. Estimative language is designed to convey judgments rather than certainty. Additionally, estimative language often conveys: 1) assessed likelihood or probability of an incident; and 2) the level of confidence ascribed to the judgment.

3.2.4.5.1.1. Estimates of Likelihood. Because analytical judgments are not certain, we use probabilistic language to reflect the S2’s estimate of the likelihood of developments or incidents. Terms such as *probably, likely, very likely* or *almost certainly* indicate a greater than even chance. The terms *unlikely* and *remote* indicate a less than even chance that an incident will occur; they do not imply that an incident will not occur. Terms such as *might* or *may* reflect situations in which we are unable to assess the likelihood, generally because relevant information is unavailable, sketchy, or fragmented. Terms such as *we cannot dismiss, we cannot rule out, or we cannot discount* reflect an unlikely, improbable, or remote incident whose consequences are such that it warrants mentioning.

3.2.4.5.1.2. Level of Confidence in Assessments. The S2’s assessments and estimates are supported by information that varies in scope, quality, and sourcing. Consequently, ascribe *high, moderate, or low* levels of confidence to assessments, as follows:

3.2.4.5.1.2.1. High confidence generally indicates that judgments are based upon high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A “high confidence” judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.

3.2.4.5.1.2.2. Moderate confidence generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. Sufficient corroboration is an analytical judgment that is dependent upon a composite of source reliability, credibility, and number of sources.

3.2.4.5.1.2.3. Low confidence generally means that the information’s credibility and/or plausibility is questionable, or the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have significant concerns or problems with the sources.

3.2.5. Step 5 – Dissemination/Reporting . The S2 will provide credible information to the Installation Commander through their respective chain of command when such information reflects a credible threat to installation resources. Depending upon the level of threat activity, the Installation Commander may convene a TWG to develop and refine threat information, coordinate and disseminate threat warnings, reports, and summaries. Once convened the TWG is responsible for developing and recommending appropriate COAs and briefing installation key leadership based on information received through the TII process. The reporting format will be determined by the criticality of the information, its time sensitivity, and the length of additional analysis required to make it most useful. No matter the format, the overall quality of the respective product is crucial to ensure maximum usability and to ensure credibility.

3.2.5.1. The characteristics described below represent the standard against which S2’s products should be continuously evaluated.

3.2.5.1.1. Timely. Integrated data must be available when the recipient (e.g., Installation Commander, DFC, Antiterrorism Staff, etc.) requires it. Timely intelligence/information/data enables the recipient to anticipate incidents and take proactive measures to mitigate threats.

3.2.5.1.2. Accurate. Intelligence must be factually correct, convey an appreciation for facts and the situation as it actually exists, and provide the best possible estimate of the threat environment and possible enemy COAs based upon sound judgment of all information available.

3.2.5.1.3. Usable. Intelligence must be tailored to the specific needs of the recipient, and must be provided in forms suitable for immediate comprehension. The recipient must be able to quickly apply intelligence to the task at hand. Providing useful intelligence requires the producers to understand the circumstances under which their products are used. For example, commanders operate under mission, operational, and time constraints that will shape their intelligence requirements and determine how much time they will have to study the intelligence they are provided. Commanders may not have sufficient time to analyze intelligence reports that are excessively

complex and difficult to comprehend. The “bottom line” must be up front and easily understandable. Oral presentations should be simple and to the point.

3.2.5.1.4. Relevant. Intelligence must be relevant to the mission. It must aid the recipient in the accomplishment of their respective tasks. Intelligence must contribute to the recipient’s understanding of the threat environment, but not burden them with intelligence that is of minimal or no importance to the current mission.

3.2.5.1.5. Objective. For intelligence to be objective, it should be unbiased, undistorted, and free of prejudicial judgments. The objective analyst must remain open-minded to all hypotheses and should never attempt to make the facts fit preconceptions of a situation or an adversary. In particular, intelligence should recognize each adversary as unique, and should avoid mirror imaging. Red teams can be used to check analytical judgments by ensuring assumptions about the aggressor are valid and intelligence assessments are free from mirror imaging and cultural bias.

3.2.5.1.6. Available. Intelligence must be readily accessible to the commander. Availability is a function of not only timeliness and usability, but also appropriate security classification, interoperability, and connectivity. Intelligence producers must strive to provide data at the lowest level of classification with the least restrictive releasability caveats, thereby maximizing the consumers’ access, while ensuring that sources of information and methods of collection are fully protected.

3.2.5.2. S2 authored products containing outside agency information, other than general awareness bulletins, intended for distribution outside of SF channels are coordinated with the local AFOSI and FPI representative prior to release. The most frequently used report formats are detailed below.

3.2.5.2.1. Situational Awareness Bulletins/Alerts (see Attachment 3). Situational awareness bulletins/alerts are the most concise and frequently used format and are simply a concise update typically forwarded via e-mail regarding a developing situation.

3.2.5.2.1.1. Situational Awareness alerts can be distributed as directed by the installation commander, the DFC or designee. These alerts are for notification purposes and are not considered directive in nature. Specific details such as sources and operational security information will usually be omitted from these alerts. The distribution list for situational awareness notifications will be determined by the same authority used to direct the alert. It is advisable to share Situational Awareness alerts with other local DoD installations as well as local/state law enforcement agencies. Additionally, the type of information being released (e.g., For Official Use Only, Law Enforcement Sensitive, etc.) will determine the distribution list. Situational awareness alerts will be distributed as soon as possible in order to ensure the information is distributed prior to the subject of the alert.

3.2.5.2.1.2. Local policy and procedures should be established that directs whether pre-coordination with key leadership or peer review is required, particularly if the material in question is time sensitive. In cases where information is time sensitive, commanders should focus on the need to

disseminate information in a timely manner rather than the need to review.

3.2.5.2.2. Incident Bulletins. Event bulletins are more comprehensive than situational awareness emails and may consist of a one- or two-page document.

3.2.5.2.2.1. Incident bulletins are distributed due to threat information or recent significant incidents of interest or potential impact to the installation. This kind of bulletin will often be published following a physical or telephonic TWG. The bulletin may be issued in conjunction with or in addition to official force protection measure recommendations from the DFC or installation commander.

3.2.5.2.2.2. May include original assessment or comments made by the TII collaborators, extracts from source documents, and references with hyperlinks or attachments.

3.2.5.2.2.3. Distribution of incident bulletins by the S2 will be determined by the directing authority and may be limited based upon whether or not direct instructions are included.

3.2.5.2.2.4. These alerts will be distributed as rapidly as possible allowing for appropriate development of analytical comments.

3.2.5.2.3. Information Bulletins. Informational summaries can be produced in various formats. The intent of the bulletin is to distill the most significant reporting available during a given time period. The bulletins are designed to provide situational awareness to customers who have minimal time to devote to filtering threat reporting or significant intelligence on a regular basis and therefore do not necessarily target individuals who work in a full time analytical capacity. Articles in an information summary may be sorted by criticality of the information, topic, geographic area of interest addressed, or other headings.

3.2.5.2.3.1. May include brief summaries of relevant reporting, original comments on the importance of the topic, hyperlinks to original source documents and source document, and publication date information.

3.2.5.2.3.2. Topics for these bulletins may include headings for TTP development, suspicious activity (eGuardian reporting), and homeland or external terrorist planning. Note: Per AFI 71-101, Volume 1, *Criminal Investigation Program*, eGuardian reporting is cleared with the installation AFOSI Detachment Commander or designee prior to dissemination.

3.2.5.2.3.3. For general situational awareness bulletins, widest possible dissemination is encouraged; however, the situation and classification of the information will dictate the distribution list.

3.2.5.2.3.4. There is no specific time frame for these types of bulletins; however, these bulletins should be completed and distributed as soon as possible to detect or delay possible future incidents.

3.2.5.2.4. Storyboards (See Attachment 5). These products assist the S2 in establishing a timeline of incidents and capturing pertinent information about an incident. The incidents are captured in chronological order similar to a blotter entry.

3.2.5.2.4.1. Following the description of the incident, the S2 documents their assessment of the incident and what possible impacts or significance the incident could have.

3.2.5.2.5. Threat Briefings/Working Groups.

3.2.5.2.5.1. The S2 may occasionally be asked to provide topic or information briefs to specialized gatherings within their unit such as guardmount briefings, Security Forces Staff Meetings, etc . These briefs may consist of general threat information or awareness of how to contact the TII members and the support the TII can provide. Threat briefings are conducted by AFOSI and FPI representatives.

3.2.5.2.5.2. May include formal standup briefings, informal tabletop briefings, other forms of presentation as required, as well as question and answer periods. Formal standup briefing slide presentations should use a consistent slide format. Great care must be paid to the highest classification that can be discussed in a particular facility and whether the audiovisual equipment in the assigned room will support a visual presentation at that classification.

3.2.5.2.5.3. Example topics may include: general terrorist threat trends; case studies of interest; developments in enemy attempts to bypass security measures; TII structure, capabilities, and contact information.

3.2.5.2.5.4. Peer review and input from each TII member is highly desired.

**3.3. Ground Tasking Order Process.** Ground Tasking Orders (GTO) should be considered at the installation level in order to synergize IPB efforts with the DFC's risk-based security operations. While the previous sections of this document provide the framework for information-sharing, and the S2's collaboration within TII, as well as the Organizing/Training/Equipping (OT&E) for the S2, the GTO process outlined here provides a framework for how the S2 can conduct daily operations in support of the DFC's ID efforts. This process takes the outputs from previously described processes and focuses the scope of effort towards achieving specific ID effects.

3.3.1. The GTO process is a 7-step, 7-day continuous cycle that enables the DFC to tailor forces and resources according to the local threat environment. Figure 3.2. depicts this process.

3.3.1.1. Step 1 – Information/Intelligence received from sources. This step is facilitated through normal information sharing processes outlined in paragraph 3.2.

3.3.1.2. Step 2 – Relevant trend data evaluated. This step is facilitated through normal information sharing processes outlined in paragraph 3.2.

Figure 3.2. Ground Tasking Order Process.



3.3.1.3. Step 3 – Threat evaluated and Information fused. This step is facilitated through normal information-sharing processes outlined in paragraph 3.2.

3.3.1.4. Step 4 – GTO is created and approved (see Attachment 6). The GTO should be created using a standardized template that will be user-friendly for flight operations and easily repeatable. A standardized database that uses canned GTO entries could facilitate this process; however, caution should be used to avoid stagnation and/or watering down the GTO process. Once the appropriate GTO template is selected for use, it should be approved by the Security Forces Staff Function S3 prior to implementation. For this process to be effective, it must be done on a near real-time basis without undue delay due to coordination and staffing processes.

3.3.1.5. Step 5 – GTO executed in support of DFC’s ID operations. Upon approval of the GTO by the DFC, the S3 implements the order in daily operations. As part of the GTO execution process, patrols should be provided with a list of information that can contribute to the S2’s overall situational awareness. Examples of this information include changes in terrain, disposition of the local populace, etc.

3.3.1.6. Step 6 – Patrol After Action Report (PAAR) (See Attachment 7). Upon completion of each GTO (per shift/cycle), the responsible patrol should complete a

PAAR capturing the relevant data. The PAAR is sent directly from the on-duty Operations Flight to the S2 for analysis. The on-duty Operations Flight should capture the date/time/title of the GTO in the blotter.

3.3.1.6.1. Completion of PAARs are not necessary for every scenario. For instance, patrols conducted in/around combat areas of operation should produce a PAAR after every patrol; however, patrols conducted by CONUS-based law enforcement units can document incidents during their shift utilizing the standard AF Form 3545, Incident Report or AF Form 3907, Field Interview Card rather than a PAAR. S2 personnel should review the Incident Reports, Field Interview Cards and daily blotter to assess whether additional information is needed from the patrol.

3.3.1.7. Step 7 – GTO effects assessed. Upon receipt of the PAAR, the S2 will evaluate the results and provide analysis, as appropriate. This final step results in new raw intelligence to be combined with existing information to begin the cycle over again.

## Chapter 4

### INTELLIGENCE PREPARATION OF THE BATTLESPACE

**4.1. Introduction.** Intelligence Preparation of the Operating Environment (IPOE) is generally performed at the operational and strategic levels (macro approach), while IPB is performed to support the component commands (micro approach) at the tactical level. IPOE and IPB products generally differ only in terms of their relative purpose, focus, and level of detail. The purpose of IPOE is to support the Joint Force Commander by determining the adversary's probable intent and most likely COA for countering the overall friendly joint mission, whereas IPB is specifically designed to support the individual operations of the component commands. This handbook will use the most appropriate term of IPB.

4.1.1. Throughout the spectrum of operations, IPB is a process interwoven into all levels of the military decisions making process, the IDRMP and contingency planning. The process itself involves thought, knowledge of the threat, and visual techniques to create and communicate the necessary information to the commander regarding the battlespace and the unit's mission within the integrated battlespace. It is a continuous process, enabling the commander to visualize the spectrum of friendly and adversarial capabilities/tactics and weaknesses within the operational environment; how they are affected by a variety of environmental factors (e.g., weather, light, terrain, political and social conditions); and the logical predictions of the most likely and most dangerous enemy COAs toward an installation or an installation's operations. In turn, these predictions are fed to the DFC's staff to shape and support ID plans designed to obtain information superiority while mitigating the threat.

4.1.2. Time permitting, the IPB process is refined to include the analysis of the branches and sequels to an operation and for each individual threat COA. This analytical process builds an extensive database for each potential area in which a unit may be required to operate. This is performed to determine the impact of the threat, environment, and terrain on operations. It is ultimately presented in a graphic format.

4.1.3. The IPB process consists of four steps. Step 1 is to *define the battlespace environment*. In Step 2, you will *describe the battlespace's effects*. You *evaluate the threat* in Step 3. Finally, in Step 4, you will *determine threat COAs*.

**4.2. Step 1 – Define The Battlespace Environment.** Identify for further analysis specific features of the environment or activities within it, and the physical space the mission will occupy within a particular operation. IAW AFPD 31-1, *Integrated Defense*, IPB will focus on the BSZ as this is the area from which the base may be vulnerable to standoff threats. This area is controlled either directly or indirectly by security forces, in a manner consistent with legal and jurisdictional limitations.

4.2.1. Identify significant characteristics of the environment. The focus of this step is to identify what aspects of the environment will have a clear impact on enemy and/or friendly COAs. Initial requirements for this step include available map sheets, city studies, and detailed specialized products. Physical characteristics include mountains, rivers, forest, high speed avenues of approach, etc. Additional documents may include history of the

environment, demographics of area surrounding the installation, ethnic issues, economics, religion, and operation-specific information.

4.2.1.1. Consider threat forces and all other aspects of the environment that may have an effect on accomplishing the unit's mission such as: weather, infrastructure (including transportation, electricity and telecommunications), as well as threat forces and their capabilities. The focus of the S2 during this phase will be the aspects that affect the installation's mission.

4.2.2. Identify the limits of the installation's AOI and BSZ. Usually, the limits of an installation's BSZ are determined by the maximum capabilities of the enemy to engage and disrupt the installation's operations. Research during this phase includes the BSZ and should include the AOI, as the AOI may be used to stage operations prior to entering the BSZ (See Attachment 8). It may be useful during this phase to create maps or overlays of an installation map that identifies the physical and legal boundaries of the installation, the BSZ and the AOI. The format or type of product is determined by the S2, the DFC, or the installation commander. S2s are encouraged to use any/all technology at their disposal (e.g., SIPRNet, Google Earth) in order to produce requested products).

4.2.3. Establish the limits of the AOI. The AOI for an installation extends beyond the BSZ as enemies can move into the BSZ from surrounding areas without being detected. The area of interest encompasses areas about which the installation needs to maintain situational awareness. The AOI around an installation may encompass surrounding major cities. The extent to which an AOI extends is determined by the DFC. Coordination with local law enforcement agencies should include information from locations within your AOI in accordance with applicable policy and law.

4.2.4. Identify the amount of detail required and feasible within the time available for IPB. The time available for completion of the IPB process may not permit the luxury of conducting each step in detail. You can overcome this by focusing on the parts of the IPB that are most important to the commander in planning and executing the mission. For example, the situation may not require an in-depth analysis of all threat forces within the AOI. Perhaps only certain threats (e.g., terrorist threats rather than criminal threats) may require a complete evaluation rather than a summary of their effects or capabilities. Allow the commander to prioritize your efforts in order to produce the amount of detail required within the available time. To assist in this task, create a visible timeline with major milestones and expectations identified.

4.2.5. Evaluate existing databases and identify intelligence gaps. Not all the intelligence and information required to evaluate the effects of each characteristic of the battlespace and each threat will be in the current database or available to you. Identify the gaps for the current operation and submit requests for information (RFIs) for the specific intelligence required to fill them. In order to ensure the request meets the format and/or requirements of the MAJCOM, consider coordinating creation/drafting of the RFIs with AF Intelligence and/or AFOSI personnel. Once the intelligence gaps have been identified, prioritize the information requests using the DFC's intent to prioritize.

4.2.6. Collect the information and intelligence required to conduct the remainder of IPB. S-2 personnel do not collect intelligence; however, this does not stop you from tapping into sources/products which are already deployed/published such as Air Force Intelligence,

AFOSI, local law enforcement, etc. Identify sources of information that can assist you while conducting IPB. Additionally, submit RFIs to fill intelligence gaps. Ideally, intelligence operations enable one to develop the perception of the battlespace and the threat to completely match the actual situation on the battlespace. In reality, intelligence will never eliminate all the unknown aspects that concern a commander and his/her staff. Be prepared to fill gaps with reasonable assumptions and continually send out RFIs to update information on unknown criteria. The references located at the HQ AFSFC SmartNet website <https://afsmil.lackland.af.mil/> can be useful sources of information.

**4.3. Step 2 – Describe The Battlespace’s Effects.** The definition for describing the battlespace’s effects is the determination of how the battlespace environment affects both threat and friendly operations. Evaluate and integrate the various factors of the battlespace environment that affect both threat and friendly operations. Begin the evaluation with an analysis of the existing and projected conditions of the battlespace environment, and then determine their effects on both friendly and threat operations.

4.3.1. The goal of this step is to describe how the factors affect operations, equipment and personnel. Whenever possible, it is recommended to use color-coded “stoplight charts” to describe aspects of operations or effects on personnel and equipment. Use Mission Capable (green), Partially Mission Capable (yellow), or Non-Mission Capable (red) to denote capabilities. For example, vehicle movement through a swamp would most likely be identified as red (denoting non-mission capable) while personnel movement through a swamp would be yellow, identifying slowed movement.

4.3.2. Evaluate the battlespace environment, to include terrain and weather analysis. Certain areas, or sectors of the installation, will affect various types of operations in differing degrees. During the evaluation, identify the areas that favor each type of operation. Terrain analysis within an urban area may focus on high-speed avenues of approach for vehicles to the installation perimeter; whereas, rural or desert areas may not have high-speed avenues of approach. Instead you may focus on portions of the installation perimeter fence that can easily be climbed or cut without detection or identifying likely locations where surface-to-air missiles may be employed against friendly aircraft. Additional evaluation may focus on low-lying areas of an installation that are prone to flooding or critical assets near the installation perimeter.

4.3.2.1. Terrain and weather analysis are inseparable. You should have already included the weather’s effects on terrain during terrain analysis. In this sub step, weather analysis evaluates the weather’s direct effects on operations, such as making certain areas of the installation inaccessible or creating unsafe driving conditions. If time and resources permit, obtain climatology-based overlays for planning purposes through your supporting Air Force weather unit.

4.3.2.2. Take the time to coordinate with trained Air Force weather personnel in order to analyze the military aspects of weather. For instance, low visibility hinders defensive operations because cohesion and control becomes difficult to maintain and detection efforts become impeded. The variability of weather can also have a major impact on your operations if the installation is potentially in the downwind range of nearby toxic industrial chemical/toxic industrial chemical (TIC/TIM) locations. Under some circumstances a hazard plume from a release would affect the installation while in other

situations it would not. These weather conditions can change frequently throughout the response effort. Because of this, it is important to integrate your supporting weather unit into the planning process for weather data, forecasts and weather effects.

4.3.3. Analyze other characteristics of the battlespace. Other characteristics include all aspects of the battlespace environment that affect threat or friendly COAs not already incorporated into the terrain and weather analysis. These may include:

4.3.3.1. The presence of criminal involvement around the installation.

4.3.3.2. Demographics of the local population.

4.3.3.3. Influence of gangs or other unofficial political elements.

4.3.3.4. Logistical or network infrastructure on or off the installation which contributes to the installation's mission.

4.3.3.5. Once you have identified the other characteristics of the battlespace, you must express it in terms of how it affects friendly and enemy COAs. For this task you may use a Modified Combined Obstacle Overlay (MCOO) which will help you depict the battlespace's effects on operations. This will identify such key items as objectives, defensible terrain, likely engagement areas and key terrain (see Attachment 9).

4.3.4. Describe the battlespace's effects on threat and friendly capabilities and broad COAs. Accomplish this step by combining the evaluation of the effects of terrain, weather and other characteristics of the battlespace into one integrated product. Address the battlespace's effects on threat as well as friendly COAs. A good technique for accomplishing this is to completely place yourself in the perspective of the threat's S2 position who must also recommend a set of COAs to his/her commander. Evaluate the effects of the battlespace environment on threat COAs considering the specific threat your installation is facing. Following are some examples to consider:

4.3.4.1. Weather may affect threat equipment differently than US equipment. For example, an AK-47 is more resistant to moisture than an M-16. Likewise, fog will affect US thermal sights less than it will affect vehicles with optical sights only.

4.3.4.2. Engagement areas and ambush sites. Using the results of evaluating cover and concealment, identify areas where maneuvering forces are vulnerable to fires. Consider weapon ranges, missile flight times and the likely speed of maneuvering forces. If your command is attacking, these are areas where it will be vulnerable to enemy fires. If your command is defending, these are potential engagement areas.

**4.4. Step 3 – Evaluate The Threat.** The third step in the IPB process is to evaluate the threat in terms of the commander's requirements. In this step, the threat is determined, information gaps are identified, and additional RFIs are forwarded to attempt to fill the gaps. The end result produces a threat model that describes threat actors and their associated capabilities and tactics. See DOD ATO Guide for information regarding compiling the threat matrix and utilizing that information to formulate the most likely and most dangerous COAs. This information should be used in the IDRMP in order to determine the amount of risk posed to installation assets/operations. Unanswered questions and gaps in intelligence greatly hinder future planning and analysis.

4.4.1. You may begin this step by obtaining DIA country reports or the AFOSI installation LTA of the operating environment, or other reports about the adversaries capable of operating in your AOI. However, it should not stop with these reports. You must utilize the elements of these reports to guide you when seeking additional information in order to determine the on-the-ground possibility of the enemy's presence and intentions. Often this is dependent upon the operational environment (CONUS, OCONUS and expeditionary) and is normally provided through your local AFOSI detachment. Consider the capabilities and weaknesses of each specific group without assuming that all enemy forces collaborate. Consider and evaluate the effects of the operating environment (gathered in Part 1 and evaluated in Part 2) on each individual adversary.

4.4.2. The desired end result is to know the threat and to determine their capabilities, given the current situation. Develop threat models which accurately portray aggressor TTPs under normal conditions. All threat actors can be evaluated through doctrine, patterns of behavior, historical references, and reactions to similar situations.

4.4.3. Identify the threat. First, identify and evaluate threat databases for complete and accurate threat compositions, strengths, and dispositions. Intelligence gaps should be identified immediately, allowing time to develop and submit requests for information to outside agencies. This step involves in-depth and continuous coordination with outside agencies and normally accomplished through AFOSI and AF Intelligence for the information needed. Sources of information can include, but are not limited to:

4.4.3.1. Department of Homeland Security (DHS) Intelligence

4.4.3.2. DIA

4.4.3.3. National Geospatial- Intelligence Agency (NGA)

4.4.3.4. National Center for Medical Intelligence (NCMI)

4.4.3.5. INTELINK

4.4.3.6. USNORTHCOM

4.4.3.7. AFNORTH

4.4.3.8. AFSOUTH

4.4.3.9. Global Terrorism Database

4.4.3.10. National Counterterrorism Center

4.4.3.11. Defense Counterterrorism Center

4.4.3.12. CJCS/J2

4.4.3.13. USSTRATCOM SkiWeb

4.4.3.14. Naval Criminal Investigative Service (NCIS)

4.4.3.15. National Center for Medical Intelligence (NCMI)

\*NOTE: Sources referenced in 4.2.6 may also be helpful during this step.

4.4.4. Update and create threat models. Threat models depict how threat actors prefer to conduct operations under ideal conditions. They are based upon the identified threat's normal

organization, equipment, doctrine, and TTPs. Threat models result from a detailed study of the aggressor. Ideally, threat models are constructed and evaluated prior to deployment. After deployment, continuous evaluation of the threat and updating the threat models are required.

4.4.4.1. The threat model should include preferred tactics and targets of threats to the installation, i.e., local threat actors that are present and have the capability and intent to negatively impact installation mission, personnel and resources. Any/all historical information should be included so as to contribute to the most accurate prediction. This information should be constantly updated to reflect any changes and can/should include:

4.4.4.1.1. Composition. What is the make-up of the enemy force? Does it include active cadre, recruiters, supporters, etc.?

4.4.4.1.2. Disposition. What are the tendencies of the enemy force? Do they have a history of targeting US interests?

4.4.4.1.3. Strength. How many members belong to the enemy force?

4.4.4.1.4. Tactics. What type of tactics does the enemy force employ?

4.4.4.1.5. Training Status. Does the enemy force have an active training program? Do they have the capability to train new recruits in order to replenish their numbers?

4.4.4.1.6. Logistics. Does the enemy force have the capability to procure, maintain, and transport equipment and personnel in order to facilitate an attack?

4.4.4.1.7. Effectiveness. Can the enemy force produce the intended results of their mission?

4.4.5. Identify threat capabilities. At the installation level, concern regarding threat capabilities is usually focused down to what tactics an aggressor is capable of employing (e.g., sniping, Vehicle Borne Improvised Explosive Device (VBIED), drive-by shooting, etc.).

4.4.5.1. Threat capabilities are the broad COAs and support operations which aggressors take to influence the accomplishment of friendly operations. They take the form of statements, such as:

4.4.5.1.1. The threat has the capability to launch Surface-to-air-missiles (SAM) attacks.

4.4.5.1.2. The threat has access to CBRN weapons.

4.4.5.1.3. The protestors can effectively block traffic at no more than seven different intersections.

4.4.5.2. Begin with the full set of tactics and consider the threat's ability to conduct each operation based upon the current situation. Example: A terrorist group's normal TTPs may call for the use of car bombs or similar devices to tie down emergency services while they conduct raids in other parts of town. Your evaluation of the threat's current logistics status, however, might indicate a critical shortage of explosive materials.

4.4.5.3. Disseminate the results of evaluating the threat as widely as possible. At the very least, this information should be shared with S-3 personnel, and TII contributors (as

applicable). This allows other staff sections and units to include them in their own assessments.

**4.5. Step 4 – Determine Threat COAs.** The final step of the IPB process is to determine the various threat COAs that will influence the accomplishment of friendly operations. The goal of this entire exercise is to replicate the set of COAs that the aggressors are considering based upon the friendly situation. The majority of your focus during this step should be applied to the most likely and most dangerous enemy COAs. Utilize the resulting threat COAs, along with other facts and assumptions about the battlespace environment, to drive the wargaming process and to develop friendly COAs.

4.5.1. Identify the threat's likely objectives and desired end state. Begin this step by attempting to identify what the goal of the enemy is (desired end state). The next step is to consider the threat COAs that could significantly influence the installation's mission, even if the threat's doctrine considers them infeasible or sub-optimum under current conditions.

4.5.1.1. Consider any indirect or "wildcard" COAs that the threat is capable of executing.

4.5.1.2. Consider the threat COAs indicated by recent activities and incidents.

4.5.1.3. Consider all possible explanations for the threat's activity in terms of possible COAs to avoid surprise from an unanticipated COA.

4.5.1.4. Consider each subset of COAs independently to avoid forming biases that restrict the analysis and evaluation. Once each subset is evaluated separately, combine them to eliminate redundancy and minor variations.

4.5.1.5. Compare the consolidated list of threat capabilities identified in Step 3 of the IPB process and eliminate any COA the threat is incapable of executing.

4.5.1.6. Once you have identified all of the COAs above, consider the suitability of each COA to the desired end states of the threat. If the COA is successfully executed, will it accomplish the threat's objectives?

4.5.1.7. Consider the feasibility of each threat COA to determine if the COA is feasible. Does the threat possess the capability, time, and resources to carry out the COA?

4.5.2. Once you have identified all probable COAs, the next step is to mold intelligence collection requests in order to answer specific questions that, when observed, reveal which COAs the aggressor has chosen. These activities are called indicators.

4.5.3. Once persistent threat information has been developed it should be applied to the commander's IDRMP to identify any changes to risk. IAW AFI 31-101 and AFI 10-245, *Antiterrorism*, the commander's ForcePRO tool should also be updated to reflect current threat information.

4.5.4. The SIO will be able to provide the S2 with many of the documents/information required for the S2 to accomplish their mission. This may include the following:

4.5.5. Indications and warnings (emerging crisis situations).

4.5.6. Current intelligence (adversary intentions and/or courses of action).

4.5.7. General military intelligence (adversary Order of Battle (OB), cultural awareness information).

4.5.8. Adversary capabilities, TTPs, terrorist group historical background and intent, finished intelligence, terrain analysis, route analysis, man-portable air defense system (MANPADS)/stand-off weapons footprints, cyber threat, etc.

#### **4.6. Tips for Success.**

4.6.1. Work ahead. The best solution is to complete as much work ahead of time as possible. Establish a series of base products, particularly those that deal with the battlespace environment's effects on operations. Keep them updated by periodic review instead of waiting until receipt of a new mission or threat.

4.6.2. Become familiar with the support available to you from intelligence systems and support agencies. Know how to get what you need before you need it by networking and educating yourself with the support available. Think through methods to get support before, during, and after an incident.

4.6.3. Focus on essentials. Decide which products will be developed and to what degree of detail. Focus on the products most important to the mission. Rather than fully developing one threat COA at the expense of others, identify the full range of available COAs. Determine the degree of detail required and then develop all COAs to that level of detail.

4.6.4. Ensure your information is vetted. Never assume data provided or gleaned from open sources is factual. Always try to vet information through second and third sources wherever possible. Use classified sources and information to validate information whenever available; however, reference unclassified sources as often as possible to allow for wider distribution of information. Use validation (i.e., possible, probable, actual) so as not to compromise your assessments and COAs.

4.6.5. Know what you know, what you don't, and what you need to fill in the intelligence gaps. Keep in mind that the first and foremost source for building your product and assessment is the intelligence community. The majority of the time, the intelligence community has already built IPOE or IPB for every AOI around the globe. Work smarter, not harder. Try to never "recreate the wheel" and attempt to build your products from scratch. The relationship developed between the TII partners is essential to building factual, concise, and relevant products for the decision makers. It is essential to know available sources of information and how to gain vital information from stakeholders via RFIs.

4.6.6. When developing the IPB, AOI, and/or COAs, focus on the operating environment, terrain, demographics, and known and suspected adversarial TTPs. Once developed, continuously evaluate and update, as some factors (e.g., TTPs) will change and some (e.g., terrain) will mostly remain constant, but the operating environment itself constantly evolves.

4.6.7. Your most critical asset in the process will be your battle partners within the TII community. They will aid, assist, and oftentimes author the initial product along with updates if asked. If you don't ask, you are severely hampering your assessment and COAs, and likely endangering friendly forces. The more information, the better. If all else fails, get operations and intelligence experts together to help you develop your product.

JUDITH A. FEDDER, Lieutenant General, USAF  
DCS/Logistics, Installations & Mission Support

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

Defense Intelligence Agency (DIA), Analytic Standards

Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World, July 2005

Intelligence Community Directive Number 203, Analytic Standards, June 2007

Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies, January 2009

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing, October 2007

Annex 3-10, *Force Protection*, August 2014

AFPD 31-1, *Integrated Defense*, Oct 2011

AFI 10-206, *Operational Reporting*, September 2011

AFI 10-245, *Antiterrorism*, 21 September 2012

AFI 14-119, *Intelligence Support to Force Protection*, May 2012

AFI 15-128, Air Force Weather Roles and Responsibilities, 7 February 2011

AFI 31-101, *Integrated Defense, Incorporating Through Change 2*, March 2013

AFI 31-401, *Information Security*, March 2009

AFI 71-101, Volume 1, *Criminal Investigations Program*, 8 April 2011, Incorporating Change 1, 16 May 2013

AFI 71-101, Volume 4, *Criminal Investigations Program*, 8 April 2011, Incorporating Change 1, 5 September 2012

DoD 5240.1-R, Activities of DoD Intelligence Components that Affect United States Persons, December 1982

DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, January 7, 1980

DoDI 2000.26, *Suspicious Activity Reporting*, November 2011

DoDI 5505.17, *Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities*, December 19, 2012

DoDI 5525.18, *Law Enforcement Criminal Intelligence (CRIMINT) in DoD*, October 2013

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, March 2014

JP 2.0, *Joint Intelligence*, June 2007

JP 2-01.3, *Intelligence Preparation of the Operating Environment*, June 2009

Office of the Director of National Intelligence, Intelligence Community Directive (ICD), 203, *Analytic Standards*, 21 June 2007

Executive Order 12333, 2008, *United States Intelligence Activities*, December 4, 1981, as amended

International Association of Law Enforcement Intelligence Analysts (IALEA), National Law Enforcement Analytic Standards, April 2012

### ***Abbreviations and Acronyms***

**ACH**—Analysis of Competing Hypothesis

**ADCON**—Administrative Control

**AFNORTH**—Air Forces North

**AFOSI**—Air Force Office of Special Investigations

**AFSOUTH**—Air Forces South

**AKO**—Army Knowledge Online

**AO**—Area of Operations

**AOI**—Area of Interest

**ATO**—Antiterrorism Officer

**BSZ**—Base Security Zone

**CBRN**—Chemical, Biological, Radiological and Nuclear

**CCIR**—Commander's Critical Information Requirement

**CJCS**—Chairman, Joint Chiefs of Staff

**COA**—Course of Action

**DEA**—Drug Enforcement Agency

**DFC**—Defense Force Commander

**DHS**—Department of Homeland Security

**DIA**—Defense Intelligence Agency

**DSS**—Defense Security Service

**FBI**—Federal Bureau of Investigations

**FFIR**—Friendly Forces Information Requirement

**FIR**—Field Investigations Region

**FLETC**—Federal Law Enforcement Training Center

**FPI**—Force Protection Intelligence

**FP IFTU**—Force Protection Intelligence Formal Training Unit

**GTO**—Ground Tasking Order  
**HSIN**—Homeland Security Information Network  
**HQ**—Headquarters  
**ID**—Integrated Defense  
**IDP**—Integrated Defense Plan  
**IDRMP**—Integrated Defense Risk Management Process  
**IPB**—Intelligence Preparation of the Battlespace  
**JIPOE**—Joint Intelligence Preparation of the Operating Environment  
**LEO**—Law Enforcement Online  
**LTA**—Local Threat Assessment  
**MAJCOM**—Major Command  
**MCOO**—Military Combined Obstacle Overlay  
**MDMP**—Military Decision Making Process  
**NAF**—Numbered Air Force  
**NCIC**—National Crime Information Center  
**NCIS**—National Criminal Investigative Service  
**NIMA**—National Imagery and Mapping Agency  
**NIPRNet**—Non-classified Internet Protocol Router Network  
**OPCON**—Operational Control  
**OTE**—Organize, Train, Equip  
**PAAR**—Patrol After Action Report  
**PIR**—Priority Intelligence Requirement  
**RFI**—Request for Information  
**RISS**—Regional Information Sharing System  
**SIPRNet**—Secure Internet Protocol Router Network  
**SFMIS**—Security Forces Management Information System  
**SITREP**—Situation Report  
**SLATT**—State and Local Antiterrorism Training  
**SME**—Subject Matter Expert  
**SAM**—Surface-to-Air Missile  
**TACON**—Tactical Control  
**TIC/TIM**—Toxic Industrial Chemical/Toxic Industrial Material

**TII**—Threat Information Integration

**TTP**—Tactics, Techniques, and Procedures

**TWG**—Threat Working Group

**USNORTHCOM**—United States Northern Command

**USSTRATCOM**—United States Strategic Command

**VBIED**—Vehicle Borne Improvised Explosive Device

### *Terms*

**All-source Intelligence**—Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. See also intelligence. (JP 2-0)

**Analysis and Production**—In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 2-01)

**Area of Interest**—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. This area also includes areas occupied by enemy forces that could jeopardize the accomplishment of the mission. Also called AOI. See also **area of influence**. (JP 1-02)

**Base Security Zone**—The Base Security Zone (BSZ) is an Air Force unique concept and term to be used intra-Service only. The Air Force uses the planning term BSZ to describe the area of concern around an air base and to support the establishment and adjustment of the Base Boundary. The BSZ is the area outside the base perimeter from which the base may be vulnerable from standoff threats (e.g., mortars, rockets, man portable air defense systems [MANPADS]). The Installation Commander should identify the BSZ and coordinate via their operational chain of command with local, state, federal agencies (CONUS) or host nation or area commander (OCONUS) for the BSZ to be identified as the Base Boundary. If the Base Boundary does not include all of the terrain of the BSZ, the Installation Commander is still responsible for either mitigating (through coordination with local, state, federal agencies [CONUS] or the area commander or host nation [OCONUS] or accepting the risks of enemy attack from the terrain outside the Base Boundary. (AFPD 31-1)

**Collection**—In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 2-01)

**Concept of Intelligence Operations**—A verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations. The concept of intelligence operations, which supports the commander's concept of operations, is contained in the intelligence annex of operation plans. The concept of intelligence operations is designed to give an overall picture of intelligence support for joint

operations. It is included primarily for additional clarity of purpose. See also **concept of operations**. (JP 1-02)

**Counterintelligence**—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 2-0)

**Dissemination and integration**—In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (JP 2-01)

**Evaluation and feedback**—In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (JP 2-01)

**Fusion**—In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 2-0)

**Indicator**—In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 1-02)

**Information**—Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1)

**Integrated Defense**—The integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations. (AFPD 31-1)

**Intelligence**—The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (JP 1-02)

**Intelligence Community**—All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called IC. (JP 1-02)

**Intelligence Estimate**—The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 1-02)

**Intelligence Preparation of the Battlespace (IPB)**—The analytical methodologies employed by the Services or joint force component commands to reduce uncertainties concerning the enemy, environment, time, and terrain. Intelligence preparation of the battlespace supports the individual operations of the joint force component commands. Also called IPB. (JP 1-02. SOURCE: JP 2-01.3) (This term and its definition modify the existing term and its definition and are approved for inclusion in JP 1-02.)

**Joint Intelligence Preparation of the Environment (IPOE)**—A systematic, continuous process of analyzing the threat and environment in a specific geographic area. It is designed to support staff estimates and military decision-making. (JP 2-03.1)

**Law Enforcement Sensitive Information**—Law Enforcement Sensitive is a marking sometimes applied, in addition to/conjunction with the marking FOR OFFICIAL USE ONLY, by the Department of Justice and other activities in the law enforcement community. It is intended to denote that the information was compiled for law enforcement purposes and should be afforded appropriate security. (AFI 31-401)

**Need-to-Know**—A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 1-02)

**Open-Source Information (or Intelligence)**—Information of potential intelligence value that is available to the general public. Also called **OSINT**. (JP 2-0)

**Planning and Direction**—In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (JP 2-01)

**Priority Intelligence Requirement**—An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment. Also called PIR. (JP 2-0)

**Processing and Exploitation**—In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (JP 2-01)

**Sensitive But Unclassified (SBU) Information**—SBU information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA. When SBU information is included in DOD documents, it shall be marked as if the information were FOUO. (AFI 31-401)

**Threat Assessment**—In antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations, as well as the security environment within which friendly forces operate to determine the level of threat. Also called **TA**. (JP 3-07.2)

**Attachment 2****REQUEST FOR INFORMATION (RFI) EXAMPLES**

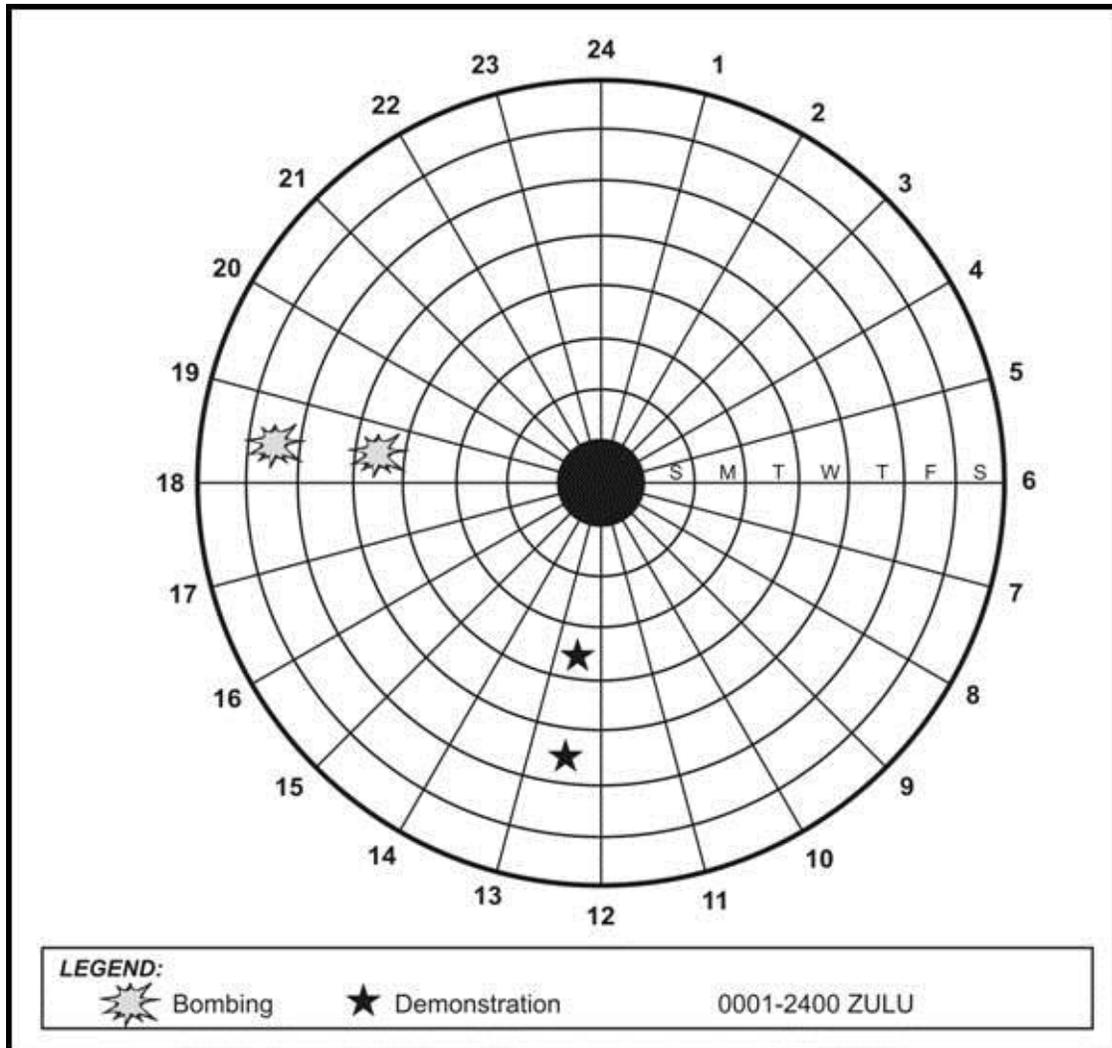
The following information requirements look for indications of threats to AF assets. Some examples of specific indicators are identified in DODI 2000.26, Suspicious Activity Reporting

1. Are there indications of a planned or impending kinetic or cyber-attack by malevolent actors (for example from international, domestic, or self-selected lone wolf terrorists) against AF personnel or dependents, facilities, assets, or critical infrastructure?
2. Are there indications of a planned or impending kinetic or cyber-attacks against the USNORTHCOM AOR that may require support from AF personnel and assets or that may impact AF operations?
3. Are there indications of criminal activity in the vicinity of AF personnel or dependents, facilities, assets, or critical infrastructure that may endanger welfare or disrupt operations?
4. Are there indications of a manmade or natural disaster that may endanger the welfare or disrupt operations of AF personnel and assets?
5. Are there indications of actual or manmade incidents, natural disasters, or other incidents causing significant loss of life and/or large-scale evacuations that may require AF support (force provisioning/DSCA)?
6. Are there indications of interest or intent from drug trafficking organizations, third generation criminal organizations, or other entities in disrupting or compromising the AF counter-narcotics mission?
7. Is there information on a counterintelligence threat to AF that has come into the AF's possession through intelligence or law enforcement reporting channels that should be passed to AFOSI Field Investigative Region (FIR) for appropriate attention?
8. Are there indications of a threat to the USAF nuclear enterprise of interest to the AF?
9. Are there indications of an impending incident/threat that may initiate a COOP response at an AF installation?
10. What current or developing terrorist or criminal tactics, techniques, and procedures pose a prospective threat to AF personnel, facilities, or assets?

## Attachment 3

## PATTERN ANALYSIS EXAMPLE

Figure A3.1. Pattern Analysis Example.



**A3.1.** The above illustration is a depiction of a weekly timeline chart developed in order to identify patterns based on day of the week and time of the day.

A3.1.1. The numbers outside of the circle are the 24 hours within a single day. The days of the week are identified inside the circle starting with Sunday and ending with Saturday. Significant incidents are marked on the specific day of the week and time of the day the incident occurred.

A3.1.2. As identified in the illustration above, two demonstrations occurred on Tuesday and Thursday between 1200 and 1300 hours, respectively. Additionally, two separate bombings occurred on Wednesday and Friday between 1800 hours and 1900 hours.

## Attachment 4

## SITUATIONAL AWARENESS BULLETIN EXAMPLE

Figure A4.1. Situational Awareness Bulletin Example.

**XXX Security Forces Squadron  
Security Forces Investigations  
SITUATIONAL AWARENESS  
DD MMM YY**

This message is being disseminated to achieve maximum situational awareness at all levels within the Chain of Command for personnel assigned to, operating in, or transiting through the XXX XX AOR.

**1. Source:** MSgt John Smith, XXX AFB S2, XXX Security Forces Squadron  
Comm: (123) 456-7891, DSN: 123-4567, [john.smith@us.af.mil](mailto:john.smith@us.af.mil).

**2. Summary of Incidents:** On 4 Feb 13, XXX County Sheriff's Office executed a narcotics search warrant for JOHN Q. PUBLIC in Happy Days Subdivision. PUBLIC was in possession of methamphetamines and several Improvised Explosive Devices (IEDs). The IEDs were described as PVC pipes filled with powder and .223 shells attached to the outside of the pipe, a silicone-type wrap around the PVC pipe and shells with a fuse extending out from the top. Upon further investigation, PUBLIC's criminal record revealed numerous encounters with law enforcement officials in the XXX city/county. Charges included disorderly conduct, domestic abuse, terroristic threats, and IRS charges along with various traffic warrants. Per XXXPD, PUBLIC has a strong dislike for government officials, law enforcement, and the government infringing on his rights.




**NOTE:** Due to the limited availability of information at the time of this report, further information or questions about the suspect's affiliation with an organized group is unknown.

**3. Overall Impact:** There is no information of a threat against XXX AFB personnel and/or assets based upon the information being provided.

**4. Recommended Actions:** Report any suspicious activity to a XXX AFB Law Enforcement entity (SFS/AFOSI) for situational awareness. Incorporate potential threat in any upcoming threat assessment for all open base events. Report similar incidents to your individual Base Defense Operations Center at (123) 456-7891, for immediate response.

**5. POC:** MSgt John Smith (see para 1 for contact info)

Figure A4.2. Situational Awareness Bulletin Example (continued).

*XXX SFS Comment: This information is Law Enforcement Sensitive and shall not leave the LE Community without confirmed consent from the Originator/Source. XXX SFS Squadron is the originator of the provided information and is disseminating this message solely for Situational Awareness purposes.*

**THE INFORMATION CONTAINED IN THIS MESSAGE IS NOT SUFFICIENT PC FOR  
ARREST.**

**XXXX AFB SFS S2  
DSN: XXX-XXXX  
Comm: (XXX) XXX-XXXX**

**Attachment 5**  
**STORYBOARD EXAMPLE**

**Figure A5.1. Storyboard Example.**

<u>UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE</u>				
<u>S2 STORYBOARD – Seymour-Johnson AFB (SJAFB)</u>				
DTG: 0438 (Local) 17May13	LOCATION: Gate P6, SJAFB Southside Perimeter	WEAPONS: White Ford XXX XX/XXXXX	INJ/FAT: N/A	Prelim: X  Final:
<p><b>INCIDENT SUMMARY:</b> At 0438L, XX May XX, SJAFB BDOC received a notification, from XXXXX County 911 Dispatch, of a reported vehicle accident at Gate P6 (seldom used special purpose gate), XXXX Road on the South perimeter of the base. SF patrols were briefed and dispatched along with local authorities. 0445L, SF confirmed a white XXXX pickup (XX/XXXXX) had impacted the XX chain link fence gate. No personnel present in vicinity, but the vehicle showed damage consistent with vandalizing (broken windows and taillights). At 0451L, SF conducted sweeps of the base perimeter and resources with no further findings. It was later discovered that the removable hitch from the truck was utilized to wedge the accelerator to the seat to propel the unmanned vehicle into the fence line gate at relatively low speed. Investigation revealed the vehicle was reported stolen the night before. Approximately 100 feet outside of Gate P6 on XXXXXXX Lane, SF found two hammers, broken glass and pieces of tail light, presumably from the subject truck. During the time of this incident, the SJAFB flight line was inactive and there were no other known sensitive activities occurring on SJAFB. NFI (1330 Local, 17May13)</p>				
				
		<p><b>S2 Assessment:</b> Although the use of an object to wedge the throttle in an attempt to ram the truck into the base perimeter gate is not a typical TTP seen when a stolen vehicle is being discarded, in the absence of any additional information or intelligence to suggest otherwise, this appears to simply be a case of stolen vehicle disposal. While we cannot rule out the possibility that this act was an attempt to breach the installation or test security, the fact that the road and gate in question are both officially closed with bollards in place just inside of the gate, coupled with the fact that the fence line to the left and right of the gate is not equipped with anti-ram cabling, yet the subject(s) chose not to attempt to breach in those areas lead us to believe this was likely just an act of vandalism/destruction of property.</p>		
<u>UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE</u>				

## Attachment 6

## GROUND TASKING ORDER EXAMPLE

Figure A6.1. Ground Tasking Order Example.

Ground Tasking Order Example	
<b>Ground Tasking Order: S-1 (S=Speed Selective)</b>	
RADAR/LIDAR certified Selective Presence patrol at the Beacon Beach/Eagle Dr. intersection from 0700-0800. (Annotate average speed/enforcement, if necessary) (Alpha)	
RADAR/LIDAR certified Selective Presence patrol at the Beacon Beach/Eagle Dr. intersection from 1600-1700. (Annotate average speed/enforcement, if necessary) (Bravo)	
RADAR/LIDAR certified Selective Presence patrol at the Beacon Beach/Eagle Dr. intersection from 2300-0030. (Annotate average speed/enforcement, if necessary) (Charlie)	
<b>Ground Tasking Order: H-1 (H=Housing)</b> - Neighborhood Watch/Domestic Violence Awareness pamphlet distribution in Felix Lake Housing Area between 1100 and 1300 / 1600-1730 (Community Police)	
<b>Ground Tasking Order: H-2</b> - Neighborhood Watch/Domestic Violence Awareness pamphlet distribution in Felix Lake Housing Area between 1100 and 1300 / 1600-1730 (Community Police)	
<b>Ground Tasking Order: H-3</b> - Presence patrol of Red-Eye Housing Area between 1500 and 1600. 30 minutes on foot on the following streets: Harlow LN, Kiskadee Loop, and Burge Circle (Bravo)	
<b>Presence patrol of Red-Eye Housing Area between 0600 and 0730.</b> 30 minutes on foot on the following streets: Harlow Ln, Kiskadee Loop, and Burge Circle (Alpha)	
<b>Presence patrol of Red-Eye Housing Area between 0600 and 0730.</b> 30 minutes on foot on the following streets: Harlow Ln, Kiskadee Loop, and Burge Circle (Charlie)	
<b>Ground Tasking Order: DR-1:</b> (DR=Driving Under the Influence) Presence patrol on Highway 98 any location. Use GTO matrix identified times. (Alpha Bravo Charlie)	
<b>Ground Tasking Order: DR-2:</b> Presence patrol on Sabre Dr. any location. Use GTO matrix identified times. (Alpha Bravo Charlie)	
<b>Ground Tasking Order: DR-3:</b> Presence patrol on Beacon Beach/Suwannee Rd any location. Use GTO matrix identified times. (Alpha Bravo Charlie)	
<b>Ground Tasking Order: DR-4:</b> Presence patrol at intersection of Class Six Schooner and Illinois Ave. Use GTO matrix identified times. (Alpha Bravo Charlie)	
<b>Ground Tasking Order: AT-1</b> (AT=Antiterrorism/Counter Surveillance) 100% ID checks at the Silver Flag entry gate, as well as ensuring commercial vehicles have been through the Cleveland gate for inspection, if not, annotate how many in a PAAR. 1100-1230 (Alpha) 1400-1530 (Bravo)	
<b>Ground Tasking Order: FP-1:</b> (FP=Force Protection) ATX sweep of wood line/coastal edges in Raptor Circle Housing and 20-minute LPOR within that area. (Community Police)	
<b>Ground Tasking Order: TP-1:</b> (TP=Theft Prevention) Single Vehicle Searches (to include the trunk) of every seven (7) vehicles exiting Illinois Gate for one (1) hour. Scan for any potential stolen/unaccounted for military/contracted equipment, suspicious activity and/or surveillance media. (Alpha Bravo Charlie) NOTE: If traffic begins to accumulate, clear the lanes, then select the next vehicle for the search.	
<b>Ground Tasking Order: EC-1:</b> (EC=Entry Control) Two forms of identification check at all installation entry control points, to include Cleveland gate.	
<b>Ground Tasking Order: DV-1:</b> (DV=Disinformed Visitor/Event) Realtime sweep of Hangar 1 the day prior to the Change of Command Ceremony with an Explosives Certified K-9 and Handler. Times will be determined and listed on the GTO matrix. (K-9)	

## Attachment 7

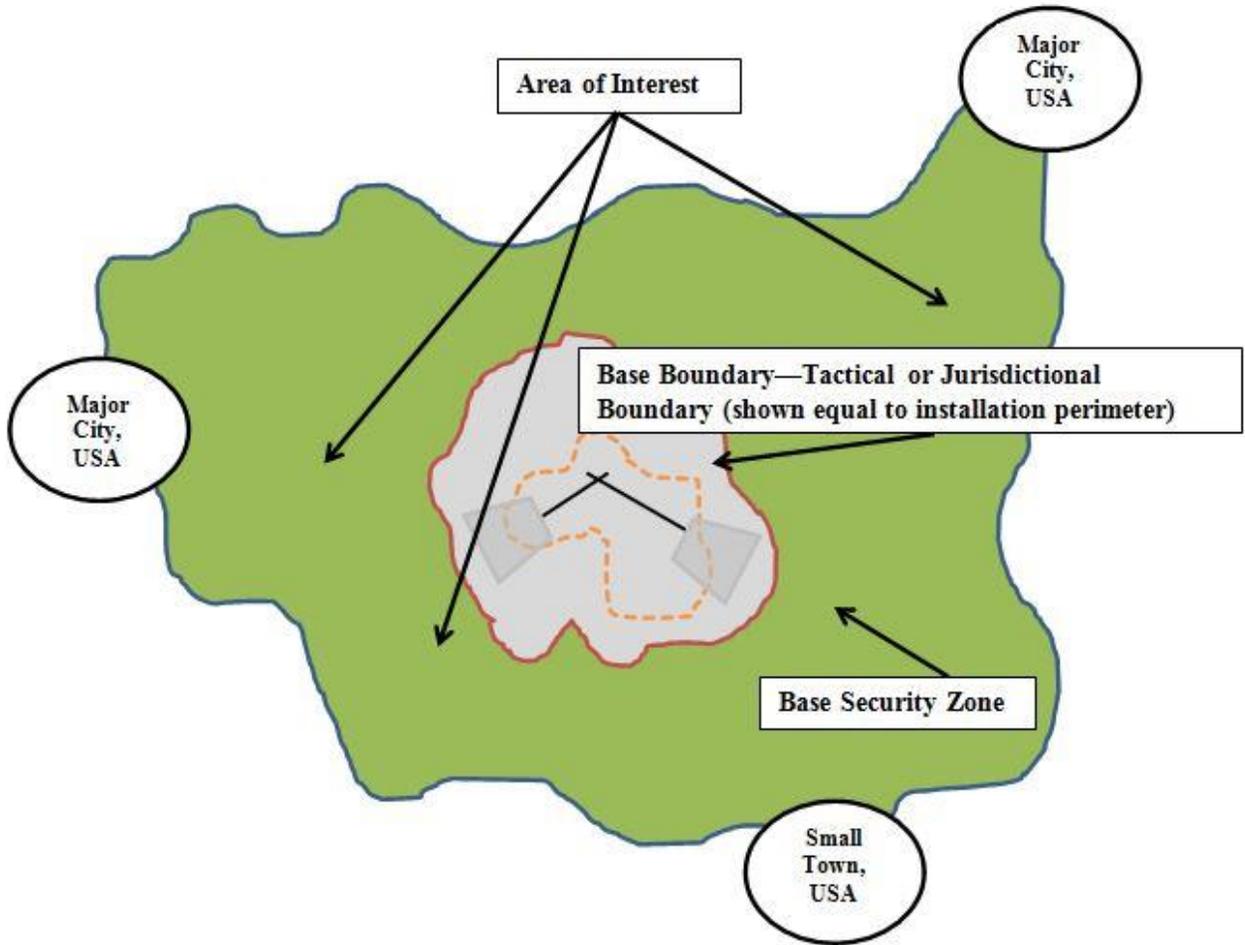
## PATROL AFTER ACTION REPORT (PAAR)

Figure A7.1. Patrol After Action Report (PAAR).

Patrol After Action Report
<u>Date: 13 Sep 12</u>
<u>Flight: Alpha</u>
<u>Time: 1100-1230 Hours</u>
<u>Location: Silver Flag Gate</u>
<u>GTO Completed: (i.e. AT-1): AT-1</u>
<p>Patrolman Summary (who, what, why): While conducting GTO AT-2, I, SrA Public, John Q. (acting as Romeo-1), came in contact with 24 vehicles. Two (2) of these vehicles were commercial vehicles that weren't searched by VACIS personnel prior to gaining entry. When questioned as to why they did not go through the proper procedures, the drivers of both vehicles stated they had never done it before because there isn't usually someone there to check. Both drivers further stated they did not know that those were the procedures required to properly access the Silver Flag area. SrA Public also encountered a vehicle containing two individuals that had an escort, but did not have an AF Form 75/Visitor's Pass on their persons. When asked why they were missing these required items, the driver/escort stated they never had to have them to access that part of the installation before. //Nothing further to report//</p>
<p>S2 Analyst Comment: Multiple reports have concluded that personnel are entering the Silver Flag training site without going through the proper search procedures. (PAARs: AT-1 26 Sep 12, AT-1 28 Sep 12) have reported this same vulnerability. The S2 concluded that unsearched vehicles pose the most dangerous threat to Tyndall AFB, being a VBIED attack. Further GTOs will be used for deterrence and documentation to support a resolution.</p>

Attachment 8  
AREA OF INTEREST MAP

Figure A8.1. Area of Interest Map.



Attachment 9

MODIFIED COMBINED OBSTACLE OVERLAY

Figure A9.1. Modified Combined Obstacle Overlay.

