

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

AIR FORCE INSTRUCTION 14-130

18 MAY 2012

Incorporating Change 1, 2 APRIL 2014



Intelligence

**AIR FORCE OPEN SOURCE
INTELLIGENCE (OSINT)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2CH

Certified by: AF/A2C
(Maj Gen Morris E. Haase)

Pages: 6

This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning Resources and Operations* and is consistent with Department of Defense (DoD) Instruction 3115.12, *Open Source Intelligence (OSINT)*. This publication establishes standards and procedures for the operational-level conduct of OSINT training and operations for all major commands (MAJCOMs) within the Department of the Air Force (AF). This publication applies to Regular Component, Air Force Reserve (AFR), Air National Guard (ANG), and Department of the Air Force (DAF) Civilians. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items.

SUMMARY OF CHANGES

This interim change adds risk factors, known as “tiers” to tasks assigned to organizations below MAJCOM level to depict the assessed risk of non-compliance and updates the certifying official. A margin bar (|) indicates newly revised material.

1. Overview. This publication provides guidance for successfully accomplishing the AF OSINT activities. It details guidance and fundamentals, provides an overview of organizational responsibilities, and establishes a framework within which to generate requirements for the acquisition and exploitation of open source material. The Air Force Office of Special Investigation (AFOSI) should comply with this instruction except when the instruction conflicts with the legal governance of AFOSI law enforcement and counterintelligence activities. Provisions of this publication do not apply to persons performing open source activities conducted for law enforcement and/or counterintelligence as part of AFOSI missions.

1.1. Title 50, USC, Section 403-5, defines Open Source Information as "publicly, available information that anyone can lawfully obtain by request, purchase, or observation" and defines Open Source Intelligence (OSINT) as "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

1.2. In addition to the definition in Title 50, USC, Section 403-5, OSINT is defined by the AF as intelligence obtained from publicly, privately, or commercially available information. OSINT is also the process of applying tradecraft in the collection or acquisition of open source information and in the exploitation of open source information. OSINT tradecraft includes but is not limited to the application of appropriate Operational Security (OPSEC) when using the internet and other digital sources, the use of non-attribution software, and the use of a variety of search techniques and software to translate and analyze open source information.

1.3. The AF shall conduct OSINT activities in a coordinated, collaborative manner, and pursue full integration and exploitation of open sources for intelligence purposes. (T-2)

1.4. OSINT collection, acquisition, exploitation, analysis, and dissemination will support prioritized specific intelligence requirements. Requirements will be entered into the intelligence community's formal OSINT requirement system, Open Source Collection & Acquisition Requirements-Management System (OSCAR-MS) or the current system of record. (T-2)

1.5. **Intelligence Oversight Compliance.** All OSINT activities will be conducted in compliance with applicable laws, policies, and directives. They will be conducted in a manner that ensures legality and propriety and that preserves and respects privacy and civil liberties. All personnel involved in the conduct of OSINT activities will comply with intelligence oversight procedures IAW DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons* and AFI 14-104, *Oversight of Intelligence Activities*. (T-1)

2. Responsibilities.

2.1. **Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2) will:**

2.1.1. Program funds through the Department of Defense (DoD) Intelligence Planning, Programming, Budgeting, and Execution (IPPBE) process to support AF OSINT requirements. This will include, but is not limited to, the baseline funding to support the open source collection platforms, open source material data acquisition, analytical tool development, and support resources as required.

2.1.2. Designate the appropriate staff element to oversee development, coordination, and implementation of fiscal and information support plans and programs supporting OSINT activities.

2.1.3. Be responsible for the effective integration of intelligence oversight into OSINT activities.

2.2. Director, Intelligence, Surveillance and Reconnaissance Capabilities (AF/A2C) will:

2.2.1. Maintain oversight of the AF OSINT capability and OSINT activities across the AF.

2.2.2. Execute AF OSINT funds in acquiring content, developing analytical tools, and producing OSINT with the goal of minimizing duplication of effort and streamlining activities across the AF.

2.2.3. Provide appropriate AF representation to the National Open Source Committee (NOSC) and the DoD Open Source Council (DOSC).

2.2.4. Conduct surveys, as needed, of all AF units acquiring open source material for intelligence purposes, producing OSINT based on specific intelligence requirements, or developing tools that facilitate discovering, analyzing, disseminating, or exploiting open source material.

2.2.5. Designate National Air and Space Intelligence Center (NASIC) the AF/A2C agent on all matters related to the execution of the OSINT activities.

2.3. MAJCOMs, Field Operating Agencies, and Direct Reporting Units will:

2.3.1. Ensure that collection, acquisition and exploitation of open sources, to include searches of the open internet, are accomplished IAW the constraints of this Instruction.

2.3.2. Reach back to NASIC for support including but not limited to OSINT tradecraft training and access to distributed OSINT products. (T-2)

2.3.3. Establish, as required, OSCAR-MS accounts on their own behalf for the purpose of submitting OSINT requirements. (T-2)

2.4. Units conducting OSINT operations will:

2.4.1. Coordinate with NASIC prior to executing funds to acquire open source content, develop analytical tools, or conduct OSINT research or production in order to increase efficiencies. (T-2)

2.4.2. Submit OSINT requirements via OSCAR-MS, or the current system of record, as appropriate and available. (T-2)

2.4.3. Execute assigned OSINT activities IAW Director of National Intelligence, DoD, and AF established OSINT tradecraft standards. (T-2)

2.4.4. Assess facilities, IAW AFMAN 32-1084, *Facility Requirements*, to ensure they adequately support the assigned OSINT activities. Identify and correct deficiencies by submitting an AF Form 332, *Base Civil Engineer Work Request*, to the host base. All facility requirements will be tracked according to local command procedures and funding allocated. (T-2)

LARRY D. JAMES, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
and Reconnaissance

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

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning Resources and Operations*, 2 April 2004

AFI 14-104, *Oversight of Intelligence Activities*, 23 April 2012

AFI 33-360, *Publications and Forms Management*, 25 September 2013

AFMAN 32-1084, *Facility Requirements*, 20 April 2012

AFMAN 33-363, *Management of Records*, 1 March 2008

AFH 32-1084, *Facility Requirements*, 1 September 1996

DoDI 3115.12, *Open Source Intelligence (OSINT)*, August 24, 2010

DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, December 1, 1982

Title 50, United States Code, Section 403-5, January 7, 2011

Adopted Forms

AF Form 332, *Base Civil Engineer Work Request*, 1 January 1991

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

Abbreviations and Acronyms

AD—Active Duty

AF—Air Force

AF/A2—Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance

AF/A2C—Director, Intelligence, Surveillance, and Reconnaissance Capabilities

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigation

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

ANG—Air National Guard

DAF—Department of the Air Force

DoD—Department of Defense

DoDI—Department of Defense Instruction

DOSC—DoD Open Source Council

IPPBE—Intelligence Planning, Programming, Budgeting and Execution

ISR—Intelligence, Surveillance, and Reconnaissance

MAJCOM—Major Command

NASIC—National Air and Space Intelligence Center

NOSC—National Open Source Committee

OPR—Office of Primary Responsibility

OPSEC—Operational Security

OSCAR—MS—Open Source Collection and Acquisition Requirements-Management System

OSINT—Open Source Intelligence

RDT&E—Research, Development, Test, and Evaluation

T-1—Tier 1

T-2—Tier 2

USC—United States Code

Terms

Open Source Information—Publicly available information that anyone can lawfully obtain by request, purchase, or observation.

Open Source Intelligence (OSINT)—As defined by Title 50, United States Code. Intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

Tier 1 (T-1)—Non-compliance puts Airmen, commanders or the USAF strongly at risk of mission or program failure, death, injury, legal jeopardy or unacceptable fraud, waste or abuse. T-1 waiver requests may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director, with the concurrence of the publication's approving official. (AFI 33-360)

Tier 2 (T-2)—Non-compliance has the potential to create moderate risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director. (AFI 33-360)