BY ORDER OF THE COMMANDER
AIR FORCE RESERVE COMMAND

AIR FORCE RESERVE COMMAND
INSTRUCTION 14-101

4 JANUARY 2024

Intelligence

OPEN-SOURCE INTELLIGENCE AND PUBLICLY AVAILABLE INFORMATION PROGRAM MANAGEMENT

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**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFRC A2/A2OP

Certified by: AFRC/A2O

Pages: 7

This Instruction implements AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*. It applies to all Airmen supporting or conducting multiple source (multi-source), multiple discipline (multi-discipline) intelligence or intelligence-related activities, including civilian employees and uniformed members of the Air Force Reserve, except members supporting cryptologic missions, where National Security Agency Policy 2-16, *National Security Agency/Central Security Service Support to the National Open-Source Enterprise*, takes precedence. It does not apply to ANG, or USSF. 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 Department of the Air Force Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the OPR using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all 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 DAFMAN 90-161, *Publishing Processes and Procedures*, 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 Office of Primary Responsibility for non-tiered compliance items.

1. OVERVIEW

1.1. Purpose. This guidance contains 13-tiered compliance statements. 1 (T-0); 0 (T-1); 2 (T-2); 0 (T-3). It includes guidance for conducting publicly available information (PAI) research and open-source intelligence (OSINT) analysis, production, and dissemination. This publication does not apply to persons conducting law enforcement and/or counterintelligence activities.

1.2. Intelligence Oversight and Operations Security. All Airmen involved in the conduct of Intelligence, Surveillance, and Reconnaissance (ISR) activities also comply with AFI 14-404, *Intelligence Oversight* and AFI 10-701, *Operations Security*, in the execution of mission and duties. For cryptologic matters, Airmen coordinate Intelligence Oversight reports to the Air Force Cryptologic Office. Airmen must comply to protect the constitutional/legal rights and the privacy/civil liberties of U.S. Persons as defined by AFI 14-404. **(T-0)**

1.3. Definitions:

1.3.1. Open-Source Intelligence. OSINT is intelligence produced from PAI that is collected, exploited, and disseminated to address an intelligence requirement. AFRC intelligence personnel are authorized and encouraged to conduct PAI research and collection and include OSINT as a tool to support the unit mission and answer commanders' intelligence requirements.

1.3.2. Publicly Available Information. PAI is "information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public" as stated in DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities.*

1.3.3. Collection. The Defense Intelligence Enterprise defines collection as information received by and Defense Intelligence component, whether or not it is retained by the component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the component. Collected information does not include: Information that only momentarily passes through a computer system of the component; Information on the Internet or in an electronic forum or repository outside the component that is simply viewed or accessed by a component employee but is not copied, saved, supplemented, or used in some manner; Information disseminated by other components or elements of the Intelligence Community; or Information that is maintained on behalf of another U.S. government agency and to which the component does not have access for intelligence purposes.

2. ROLES AND RESPONSIBILITIES

2.1. Director, HQ AFRC, Intelligence Surveillance, Reconnaissance (AFRC/A2) will:

2.1.1. Provide policy and guidance supporting the AFR ISR enterprise effort to leverage OSINT and PAI.

2.1.2. Oversee AFR ISR enterprise effort to leverage OSINT and PAI.

2.1.3. Ensure adherence to AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR).*

2.1.4. Appoint, in writing, a primary and alternate OSINT/PAI program manager.

2.1.5. Direct and ensure the inspection of OSINT and PAI use and products, including adherence to this Instruction during Unit Effectiveness Inspections.

2.2. HQ AFRC OSINT/PAI Program Managers will:

2.2.1. Implement DoD, USAF, and AFRC policy and guidance.

2.2.2. Manage/provide access to PAI systems, and licenses.

2.2.3. Monitor and audit the AFRC ISR enterprise PAI tools, systems, and license use for compliance with DoD, USAF, and AFRC policy and guidance.

2.2.4. Maintain a list of available training opportunities and advertise these options to units through AFRC/A2 MilSuite and SharePoint™ sites, and during working groups.

2.3. HQ AFRC/A2OP will:

2.3.1. Ensure inspection criteria is developed to accurately assess unit level implementation of this guidance.

2.3.2. Ensure all inspections include an assessment of unit level implementation of DoD, USAF, and AFRC policy and guidance.

2.4. Commanders and Senior Intelligence Officers will:

2.4.1. Ensure compliance with AFMAN 14-405 Paragraph 3.4.2.

2.4.2. Ensure intelligence products adhere to Intelligence Community Directive 203, *Analytic Standards*, and Intelligence Community Directive 206, *Sourcing Requirements for Disseminated Analytic Products*.

2.4.3. Ensure members conducting OSINT/PAI research and collection receive appropriate training and only utilize authorized tools.

2.4.4. Ensure members conducting OSINT/PAI research and collection utilize approved tradecraft.

2.5. All Airmen who conduct Intelligence and Intelligence-Related Activities for the Air Force, and Any Person Who Conducts Intelligence and Intelligence-Related Activities on Behalf of the Air Force will:

2.5.1. Perform mission related PAI research, only while on duty, and only use authorized managed attribution accounts for researching and collecting OSINT (SILO, Dataminr™, Recorded Future, and PAI Tool Suite). Account request forms are available by contacting AFRC/A2OS.

2.5.2. Maintain appropriate training for the use of managed attribution accounts.

2.5.3. Adhere to ICD 203 and ICD 206.

2.5.4. Adhere to standards directed in the AF PAI Research Handbook.

2.5.5. Adhere to the standards directed in the HQ USAF/A2 *Proper Use of Publicly Available Information (PAI) for AF Intelligence Activities* memorandum.

2.5.6. AFR intelligence analysts are authorized to perform missions related to OSINT research in a telework status if there is an approved research plan on file and must adhere to **paragraph 2.5.1** of this instruction.

2.5.7. PAI research must be conducted in a manner that respects the individual's U.S. Constitutional rights. If an alert contains US Person Information, follow DoDM 5240.01 rules on incidentally or intentionally collected publicly available US Person Information USPI. AFR personnel will not utilize PAI tools to collect information on friends, co-workers, family members, or US persons; or to access sexually explicit or offensive/slanderous material.

2.5.8. Personnel are not authorized to use false personas, research credentials, misrepresent their identity, join, register, or log into any websites, databases or social networks that require authentication as these activities do not constitute passive collection per DoDM 5240.01, Procedure 10.

2.5.9. PAI research using personal social media accounts and/or login credentials is prohibited.

3. TRAINING AND DOCUMENTATION

3.1. All AFR intelligence analysts will, at the minimum, complete the USAF PAI Fundamental Training course prior to conducting PAI research and producing any OSINT product. **(T-2)**

3.2. PAI Tool Suite training requirements:

3.2.1. All AFR intelligence analysts will complete a USAF PAI Tool Suite User Agreement and vendor provided virtual training course prior to obtaining a license and system access.

3.3. SILO (Managed Attribution)

3.3.1. All AFR intelligence analysts will complete SILO account training prior to obtaining a license and system access.

3.4. Dataminr™ First Alert

3.4.1. All AFR intelligence analysts will complete vendor provided telecon training or locally produced training course prior to obtaining a license and system access.

3.5. Recorded Future

3.5.1. All AFR intelligence analysts will complete Recorded Future webinar series training prior to obtaining a license and system access.

3.6. Additional Optional Training Opportunities.

3.6.1. General OSINT Awareness Training (Course DIA-INC-2025)

3.6.2. Introduction to the Open-Source Enterprise (Course OSC-OSE1106)

3.6.3. Introduction to Social Media for Intelligence Professionals (Course OSC-OSE1212)

3.6.4. Analysts should consider completing Certified Analyst Lab training to enhance OSINT capabilities.

3.7. Research plans are locally generated and should be maintained by the unit and should include essential elements of information which websites, tools, and search terms the analysts intend to use, at a minimum. See **Figure A2.1** for a sample research plan.

3.8. The USAF OSINT MilSuite site provides further guidance on training, best practices, PAI tool descriptions, Air Force PAI Research Handbook, and Proper Use Memorandums. **https://www.milsuite.mil/books/groups/air-force-osint/overview**

SIVULKA, ADAM, Colonel, USAF

Director, Intelligence, Surveillance, Reconnaissance

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 12333, *United States Intelligence Activities*

DoDD 5148.13, *Intelligence Oversight*, 26 April 2017

DoDI 3115.12, *Open-Source Intelligence (OSINT)*, 16 July 2020

DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*

AFPD 14-4, *Management of AF ISR and Cyber Effects Operations Enterprise*, 11 July 2019

AFI 10-701, *Operations Security*, 14 July 2019

AFI 14-404, *Intelligence Oversight*, 3 September 2019

AFI 33-322, *Records Management and Information Governance*, 28 July 2021

DAFMAN 90-161, *Publishing Processes and Procedures,* 18 October 2023

AFMAN 14-405 *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, 11 May 2020

ICD 203, *Analytic Standards*, (Current Edition)

ICD 206, *Sourcing Requirements for Disseminated Analytic Products*, (Current Edition)

Prescribed Forms

None

Adopted Forms

AF IMT 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ICD—Intelligence Community Directive

ISR—Intelligence, Surveillance, and Reconnaissance

OSINT—Open-Source Intelligence

PAI—Publicly Available Information

Office Symbols

AFRC/A2—Director, HQ AFRC, Intelligence Surveillance, Reconnaissance

AFRC/A2OS—HQ AFRC/A2 Special Security Office

HQ AFRC A2/A2OP—HQ AFRC/A2 Policy Integration and Assessments

Attachment 2

SAMPLE RESERCH PLAN

Figure A2.1. Sample Research Plan

Classification: _____ **Report ID**: _____

(U//FOUO) OSINT & Managed Attribution Collection and Research Plan Worksheet

Analyst Name (Last, First MI): _____ **Unit/Office Symbol:** _____

Information Requirement/Research Question/Essential Element of Information (EEI):			
Mission Alignment: (What is your unit responsible for researching/supporting/solving)			
Sources: Websites Utilized			**Resources: Tools Utilized**
1. **2.** **3.**			**1.** **2.** **3.**
Search Terms/Keywords	**Search Terms/Keywords**		**Search Terms/Keywords**
1. **2.** **3.**	**4.** **5.** **6.**		**7.** **8.** **9.**
Parallel Process: (Additional Personnel Completing Requirement)	**Name:** **Unit:**		**Name:** **Unit:**
Date of Research (DD/MMM/YYYY):	**Time of Research** (24-Hour Time):		**Time Zone:**
Target Data: (Country, Region, Org., Topic, OP Name, etc.)		**Justification:**	
Result Evaluation: Was the question answered? **YES | NO** **1.** Incorrect search terms/keywords **2.** Research question not focused enough **3.** No references in language(s) searched **4.** No results available **5.** Other:		**USPI:** YES | NO **Exclusion ID:** _____ **Saved Data:** YES | NO **File Name:** **Location:**	
Additional Information:			

Classification: _____