BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 14-405

11 MAY 2020

Intelligence

MULTIPLE SOURCE, DISCIPLINE, AND DOMAIN INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2/6OM

Certified by: AF/A2/6O
(Brig Gen Julian C. Cheater)

Supersedes: AFI 14-125, 12 January 2015; AFI 14-128, 2 August 2011; AFI 14-130, 2 April 2014; AFI 14-132, 23 December 2016; AFI 14-135, 22 May 2014

Pages: 13

This publication implements Air Force Policy Directive 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 Regular Air Force, Air Force Reserve, and Air National Guard, except as exempted by **paragraph 1.1** Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Instruction 33-322, *Records Management and Information Governance*, and disposed of IAW the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Refer recommended changes to this publication to the Office of Primary Responsibility using the Air Force Form 847, *Recommendation for Change of Publication*. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility 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 Air Force Instruction (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 requestor's commander for non-tiered compliance items.

SUMMARY OF CHANGES

This publication is new and consistent with the publication reduction effort objectives; it consolidates five instructions in the Intelligence series of publications. This manual should be completely reviewed. To encourage innovation at all echelons, members may refer to DoD issuances instead of specific direction provided in the superseded AFIs.

1. OVERVIEW.

1.1. **Purpose.** This guidance contains 10 tiered compliance statements: 7 (T-0); 2 (T-1); 1 (T-2); 0 (T-3). It includes guidance for conducting multi-source, multi-discipline ISR operations to enable the Air Force ISR Enterprise's continuing transformation into an integrated, flattened organization. This manual provides decision makers within the National Command Authority, combatant commands, Intelligence Community, and warfighters with the most complete intelligence picture through next-generation ISR dominance across multiple domains. Also, this manual promotes commanders' good judgment to empower Airmen at all levels, within the limits of the law, ethics, morality, and their experience. Provisions of this publication do not apply to persons who conduct law enforcement and/or counterintelligence activities.

1.2. **Intelligence Oversight and Operations Security.** All Airmen involved in the conduct of 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. **Multi-INT** is integrated multi-source and collaborative multi-discipline (i.e. geospatial intelligence (GEOINT), human intelligence (HUMINT), signals intelligence (SIGINT), etc.) ISR that enables sensing, identification, attribution and sharing of intelligence, in turn providing decision advantage across all domains.

1.4. **Domains** .

1.4.1. ISR from/for the Air domain synchronizes and integrates the planning and operation of sensors; assets; and processing, exploitation, and dissemination systems in order to produce intelligence products that support the mission of the Air Force.

1.4.2. ISR from/for the Cyberspace domain is an integrated intelligence and operations function, focusing on tactical and operational information gathering and mapping of enemy and adversary networks, systems, capabilities, and activity to support military planning, as described in Joint Publication 3-12, *Cyberspace Operations*.

1.4.3. ISR from/for the Space domain provides an ISR collection vantage point and is a warfighting domain that requires ISR support to ensure space superiority as described in Joint Publication 3-14, *Space Operations*. The Air Force conducts space ISR IAW DoDD 3100.10, *Space Policy*.

1.4.4. ISR from/for the Land and Maritime domains provides additional vantage points to characterize the battlespace.

2. ROLES AND RESPONSIBILITES.

2.1. **Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6)** leads the development of ISR strategy, guidance, standards, concepts of operations and continuity of operations to ensure all collection and intelligence capabilities and disciplines are integrated and interoperable. AF/A2/6 is the Head of an Intelligence Community element and responsible for coordinating all policy affecting Air Force intelligence matters.

2.2. **Director for Intelligence, Surveillance, Reconnaissance Operations (AF/A2/6O)** aligns multi-INT capabilities with National Defense Strategy priorities. AF/A2/6O:

2.2.1. Ensures integrated capability-based planning with, and provides Intelligence Certification for Joint Information programs to the Deputy Chief of Staff for Plans and Programs (AF/A5); coordinates acquisition intelligence with Assistant Secretary of the Air Force for Acquisition, Technology & Logistics (SAF/AQ); develops and coordinates the overarching ISR Enterprise policies and standards with the Intelligence Community, DoD components, and partner nations; develops the future Air Force ISR Enterprise strategy and concepts of operation; advocates for ISR resources via the Planning, Programming, Budgeting, and Execution functions for the Air Force ISR Enterprise; provides ISR program resource management guidance and oversight to major command and field operating agency representatives, and manages and oversees the varied intelligence disciplines to implement national policies in a manner that integrates capabilities and enables fusion warfare.

2.2.2. Represents AF/A2/6 in national, theater, and tactical forums and interfaces with national agencies, Joint Staff, and the Office of the Secretary of Defense. Serves as the ISR Enterprise Image Quality (IQ) Verification Program Functional Manager.

2.2.3. Coordinates with the Air Force Intelligence Oversight Officer, The Office of the Judge Advocate General (AF/JA), and the Air Force General Counsel (SAF/GC) to ensure compliance with Air Force and DoD guidance.

2.2.4. Oversees the Air Force ISR Enterprise’s effort to leverage the advantages of machine intelligence and other advanced technologies to better integrate the intelligence disciplines into a fused, data-centric concept, including sensing, identification, attribution and sharing capabilities.

2.2.5. Coordinates with the Directorate of ISR and Cyber Effects Operations and Warfighter Communications (AF/A2/6C-A/3C) to enable multi-INT capabilities by establishing automated multi-level security interfaces, integrating collection management tools, incorporating intelligence fusion tools into mission planning systems, and standardizing mapping interfaces.

2.2.6. Provides policy and guidance for globally integrated ISR systems, networks, and capabilities that enable ISR Airmen to effectively support execution of fusion warfare; supports a net-centric structure for distributed operations that are integrated across multiple domains; and assists major commands and Field Operating Agencies with technological solutions.

2.2.7. As delegated to the Air Force GEOINT Office, leads and facilitates integration of Air Force GEOINT Enterprise (AFGE) related activities for the AF/A2/6O as the Air Force Service GEOINT Element representative to the National Geospatial Agency and the broader National System for GEOINT (NSG) consistent with DoDD 5105.60, *National Geospatial-Intelligence Agency (NGA)*. The Air Force GEOINT Office coordinates with the NSG elements of the Intelligence Community, DoD, and partner nations on requirements, policy, standards, and mission sharing.

2.3. **Director for Remotely Piloted Aircraft and Airborne Intelligence, Surveillance, Reconnaissance Capabilities (AF/A2/6U)** serves as the focal point for current and emerging airborne platforms, their sensors and interfaces to the emerging sensing grid, providing multi-INT capabilities from multiple domains. Identifies and analyzes ISR capability needs, gaps, and solutions impacting and enabling mission effects. Serves as Deputy Chief of Staff/ISR lead for special and controlled access programs.

2.4. **National Air and Space Intelligence Center (NASIC)** is the Air Force and DoD primary source for foreign air and space threats analysis. NASIC creates foundational, integrated, and predictive intelligence in the Air, Space, and Cyberspace Domains enabling multi-domain operations, force modernization, and policymaking.

2.5. **Commander, Air Combat Command (COMACC)** , except as provided in **paragraph 2.6**, is responsible for organizing, training, and equipping ISR forces and capabilities and presentation of ISR forces to Air Force, joint, and DoD mission partners. COMACC either exercises or delegates the following responsibilities:

2.5.1. Develops and maintains an ISR Fusion Warfare Concept of Operations that addresses integrating 4th, 5th, and future generation weapon systems, Air and Space Operations Centers, the Distributed Common Ground System, and unit-level functions; outlines roles and responsibilities, data flow, tradecraft, and key decision points for advancing fusion warfare.

2.5.2. Leads integration of multiple source and discipline ISR across all domains identifying requirements for sensing, identification, attribution and sharing across all major commands.

2.5.3. Leads the Collections and Processing, Exploitation, and Dissemination Capabilities - ; Analysis Capability - ; and Targeting Capability Working Groups; formulates an integrated approach supporting multi-INT operations executing fusion warfare.

2.5.4. Identifies, in coordination with NASIC, ISR mission areas and tasks that will benefit from machine intelligence and other advanced technologies and proposes the integration of those technologies into programs of record. Organizes data-standardization efforts, algorithm development, and integration of machine intelligence technologies, supporting future multi-INT, multiple domain operations.

2.5.5. Develops sensor-and discipline-agnostic ISR processing, exploitation, and dissemination work centers focused on commander’s priority intelligence requirements.

2.5.6. Procures hardware, software, and information technology services necessary to maximize discovery, access, and use of Air Force ISR data by the Intelligence Community.

2.5.7. Maximizes, in coordination with NASIC, the use of Intelligence Community capabilities, tools, and services to reduce duplication of effort and improve service interoperability.

2.5.8. Collaborates with NASIC and the Intelligence Community functional managers to procure commercial technology, advancing multi-INT capabilities.

2.6. **Commander, Air Force Service Cryptologic Component (AFSCC/CC)** leads the Air Force component to the National Security Agency (NSA), is subordinate to the Chief, Central Security Service (CSS) for all cryptology matters, and is otherwise subordinate within the Department of the Air Force. Air Force Cryptologic Management is led by the AFSCC/CC, working closely with the AF/A2/6, to ensure Air Force cryptologic matters are appropriately governed and operations conducted IAW AFPD 14-4, and other guidance such as DoDI O-3115.07, *Signals Intelligence (SIGINT).* The AFSCC Cryptologic Staff tracks and facilitates cryptologic authorities. While doing so, the staff exercises management, compliance, and oversight of Air Force cryptologic activities. Further, it directs cryptologic operational coordination and execution as well as implements cryptologic planning, programming, budgeting, training, policy, doctrine, and foreign relationships for cryptologic activities. The AF/A2/6 has direct liaison authority with the AFSCC/CC to enable agreements with the National Security Agency/Central Security Service (NSA/CSS), for assigning military personnel to the NSA/CSS and policy support-related cryptologic matters. Organizations authorized to conduct cryptologic activities will coordinate all cryptologic operations, plans, policy, doctrine, governance, foreign relationships, and cryptologic or cryptologic-related training with the AFSCC/CC IAW National Security Council Intelligence Directive 6, *Signals Intelligence*; DoDD 5100.20, *National Security Agency/Central Security Service*; National Security Agency/Central Security Service Policy 1-3 (**https://policy.sp.web.nsa.ic.gov/PolicyDepot**); DoDI O-3115.07, *Signals Intelligence (SIGINT)*; and United States Signals Intelligence Directive SE3000, *SIGINT Mission of the USAF Cryptologic Forces* **(T-2)**. **Note:** AFSCC/CC is the waiver authority for Tier 2 compliance statements related to cryptologic matters. The AFSCC/CC:

2.6.1. Provides guidance on training for Air Force cryptologic personnel and unit external cryptologic intelligence training IAW DoDI 3305.09, *DoD Cryptologic Training* and NSA Policy 4-25, *Cryptologic Training System* (**https://policy.sp.web.nsa.ic.gov/PolicyDepot**).

2.6.2. Publishes guidance/standards for Air Force cryptologic personnel, programs, and activities applicable to all Air Force Cryptologic Forces and entities, regardless of command relationship.

2.6.3. Organizes, trains and equips cryptologic and cryptologic support personnel to maintain the Director NSA's cryptologic tradecraft, compliance, and training standards. Provides functional management of cryptologic Air Force Specialty Codes: 1A8X1X, 1A8X2, 1N2X1X, 1N3X1X, and 1N4X1X.

2.6.4. Coordinates with AF/A2/6 on the planning, programming, budgeting, and execution of the Consolidated Cryptologic Program. Provides manpower management oversight for cryptologic activities to satisfy mission requirements and execution.

2.6.5. Advises the ACC SIGINT Capabilities Working Group on national, sister service, and foreign partner cryptologic systems.

2.6.6. Manages cryptologic Information Technology (e.g., NSA network) capability requirements for Air Force facilities to ensure compliance with NSA/CSS standards. Maximizes the use of capabilities, tools, and services to reduce duplication of effort and improve interoperability within the Intelligence Community; procures hardware, software, and information technology services necessary to maximize data discovery and access.

2.6.7. Facilitates rapid delivery of operational capabilities that generate multi-domain, cross-functional effects through coordination with NSA/CSS cryptologic offices and programs. Provides integration of cryptologic capability development, exploitation tools, and interpretation of authorities.

2.6.8. Assesses Air Force systems that are not developed by the Intelligence Community, to determine the system's ability to perform SIGINT functions. Ensures proper oversight and data protection mechanisms are in place during testing and operations for SIGINT systems not operated by SCC personnel.

2.7. **Commander, Sixteenth Air Force (Air Forces Cyber) (16 AF/CC)** in addition to responsibilities as AFSCC/CC (**paragraph 2.6**), integrates multisource intelligence, surveillance, and reconnaissance, cyber warfare, electronic warfare, and information operations capabilities across the conflict continuum to ensure fast, lethal, and fully integrated effects in both competition and in war. Sixteenth Air Force provides mission integration of Information Warfare at operational and tactical levels. The command also prioritizes Cyberspace Intelligence Requirements and tasks ISR from/for Cyberspace assets via the Cyber Reconnaissance, Surveillance, and Target Acquisition Annex internal to Air Force Cyber. Further, the Sixteenth Air Force coordinates service-retained/reach-back capabilities to support airborne ISR collection platforms, sensors, data links, and associated processing, exploitation, and dissemination and coordinates service retained analysis and production activities via the ISR Operations Directive (IOD) Reconnaissance, Surveillance and Target Acquisition (RSTA) Annex.

2.8. **Commander, Air Force Materiel Command (AFMC/CC)** takes validated and prioritized requirements and translates them into materiel developments. In addition, AFMC/CC ensures continued partnerships between future threat analysts and science and technology developers and integrates ISR concerns into the early stages of weapon system development. The command also serves as lead major command for ensuring image quality requirements are incorporated into systems throughout their life cycle.

2.9. **Commander, Air Force Space Command (AFSPC/CC)** develops, expands, and integrates ISR capabilities from/for space operations from DoD, the Intelligence Community, industry, and allies in coordination with Air Combat Command.

2.10. **Commander, Air Education and Training Command (AETC/CC)** , in coordination with Deputy Chief of Staff for ISR and Cyber Effects Operations, Readiness and Talent Management (AF/A2/6F) and appropriate lead command/lead major command, develops ISR training to support advancements in fusion warfare and updates ISR training curricula to incorporate multi-INT concepts, tactics, techniques, and procedures.

2.11. **Major Command Directors of Intelligence** coordinate unit ISR tool/data requirements and requests, to include licenses and training; provide information on personnel to AF/A2/6, ACC/A2 (Intelligence Directorate), and NASIC to ensure efficient resource use; assess and implement fusion warfare concepts in support of missions; and ensure PAI research and collection activities are accomplished through use of appropriate research methods commensurate with acceptable level of risk.

2.12. **Field Operating Agency/Direct-Reporting Unit/Wing/Unit Commanders** provide Airmen with required resources, training, and certifications to maximize multi-INT activities within assigned mission and resources. Commanders will:

2.12.1. Ensure all ISR collection activities and all use of collected intelligence is within legal guidelines and consistent with unit mission statements IAW DoDD 5240.01, *DoD Intelligence Activities* and DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, **(T-0)**. Ensure tailored mission training **(T-0)**.

2.12.2. Ensure members conduct research and collect PAI for mission purposes, only while on duty, using government-provided information systems, and with government-approved accounts **(T-0)**. Ensure personnel do not search and store PAI related to an intelligence mission on personal devices **(T-0)**. Ensure personnel read and comply with terms-of-service (e.g. websites, PAI tools, etc.); and consult servicing legal counsel should there be questions with regard to mission-related exceptions **(T-0)**.

2.12.3. In order to meet audit obligations outlined in DoDM 5240.01 prohibit members from using non-DoD-controlled information systems or devices to conduct research on behalf of an assigned mission or other duty-related reason. Research conducted on non-DoD-controlled information systems or devices for personal interests and/or professional development shall be permitted. Members may not misrepresent research conducted on non-DoD-controlled information systems or devices on behalf of an assigned mission or other duty-related reason as research conducted for personal interests and/or professional development **(T-0)**.

2.12.4. Ensure personnel receive training on the proper identification and use of technology and tradecraft to mitigate operational security risk when conducting PAI research or collection **(T-1)**.

2.12.5. Comply with the ISR Enterprise Image Quality Verification Program when in the process of acquisition, creation, transmission, exploitation or dissemination of imagery **(T-1)**.

3. ISR COLLECTION AND EXPLOITATON MISSIONS.

3.1. **Geospatial Intelligence (GEOINT)** includes the collection, processing, exploitation, and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. All intelligence

integrates with GEOINT. GEOINT consists of imagery, imagery intelligence, and geospatial information.

3.1.1. GEOINT activities are conducted by personnel assigned, attached, or supporting units with authorized GEOINT missions IAW:

3.1.1.1. DoDD 5250.01;

3.1.1.2. DoDI 3115.15, *Geospatial Intelligence*;

3.1.1.3. DoDI 5000.56, *Programming Geospatial Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems*;

3.1.1.4. National System for Geospatial Intelligence Directive (NSGD) 1501, *Termination or Change of Geospatial Intelligence Products and Services* (**http://nsg.ic.gov/nsg2/library**);

3.1.1.5. NSGD 3201, *The Geospatial Intelligence Functional Manager Standards Assessment Program*; (**http://nsg.ic.gov/nsg2/library**);

3.1.1.6. National System for Geospatial Intelligence Instruction - Analysis and Production 3104, *Military Services Geospatial Intelligence Analysis and Production Program Mission Instruction* (**http://nsg.ic.gov/nsg2/library**);

3.1.1.7. Chairman of the Joint Chiefs of Staff Instruction 3110.08E, *Geospatial Information and Services Supplemental Instruction to Joint Strategic Capabilities Plan (JSCP)*; and

3.1.1.8. Joint Publication 2-03, *Geospatial Intelligence Support in Joint Operations.*

3.1.2. The AFGE is the community of Air Force users and producers of geospatial products and data at all levels of command and functions. These include ISR, logistics, engineering, force protection, NASIC, Air Force Flight Standards Agency, and the 557th Weather Wing. The AFGE ensures that data and services comply with policies specified in NSGD 3201. AFGE develops and resources the GEOINT sensor, systems, and tradecraft that leverages machine learning to synchronize ISR collection and exploitation across the enterprise, leading to fusion of data and information at the point of need.

3.2. **Human Intelligence (HUMINT)** is an ISR collection activity in which humans are both the source and collection platform for information. HUMINT is a key capability undergirding nearly all foundational intelligence collections and understanding of the battlespace. The Air Force is authorized and directed to conduct HUMINT collection operations, reporting, and related intelligence activities IAW DoDD S-5200.37, *Management and Execution of Defense Human Intelligence*. HUMINT activities are conducted by personnel assigned, attached or supporting units with authorized HUMINT missions and appropriate training, qualifications, and leadership IAW:

3.2.1. DoDD S-5200.37;

3.2.2. DoDI S-5200.42, *Defense Human Intelligence and Related Intelligence Activities (U)*;

3.2.3. DHE-M-3301.001, *Defense Human Intelligence Enterprise Manual, Volume 1: Collection Requirements, Reporting, and Evaluation Procedures*;

3.2.4. DCHE-M-3301.002, *Defense Counterintelligence and Human Enterprise Manual, Volume II: Human Intelligence Collection Operations*;

3.2.5. DoDI S-3325.10, *Human Intelligence Activities in Cyberspace (U)*;

3.2.6. DoDI C-5205.01, *DoD Foreign Military Intelligence Collection Activities (FORMICA) (U)*;

3.2.7. DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation (U)*; and

3.2.8. AFI 16-901-S, *Support to Sensitive Activities (U)*.

3.3. **Measurement and Signature Intelligence (MASINT)** is information produced by quantitative and qualitative analysis of physical attributes of targets and events to detect, identify, locate, and characterize them. Advanced MASINT analysis provides algorithms supporting missions and platforms operating across the Air, Land, Sea, and Space domains. Personnel assigned or attached to, or otherwise supporting units with authorized missions IAW DoDI 5105.58, conduct MASINT activities in a manner to optimize sensing, identification, attribution and sharing, aircraft, and space systems in support of mission sets.

3.4. **Publicly Available Information (PAI) and Open Source Intelligence (OSINT).** 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.

3.4.1. Open Source Intelligence (OSINT) is intelligence that is produced from PAI that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement as stated in DoDI 3115.12, *Open Source Intelligence (OSINT)*.

3.4.2. Intelligence organizations and personnel are authorized to conduct PAI research and collection to produce intelligence IAW their mission, DoDD 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)* and DoDM 5240.01. Integrating PAI into analytic workflows supports fusion of information at the speed and point of need. When related to cryptologic matters refer to National Security Agency Policy 2-16, *National Security Agency/Central Security Service Support to the National Open Source Enterprise* (**https://policy.sp.web.nsa.ic.gov/PolicyDepot**).

3.5. **Signals Intelligence (SIGINT)** is a category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted, and includes intelligence derived from communications, electronic, and foreign instrumentation signals. Personnel conduct SIGINT IAW United States Signals Intelligence Directive SE3000.

MARY F. O'BRIEN, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
Reconnaissance and Cyber Effects Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*, 11 July 2019

HAFMD 1-33, *Deputy Chief of Staff of Air Force, Intelligence, Surveillance and Reconnaissance*, 18 September 2015

AFI 10-701, *Operations Security*, 24 July 2019

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

AFI 16-901-S, *Support to Sensitive Activities* (U), 12 October 2018

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 33-322, *Records Management and Information Governance*, 6 March 2020

CJCSI 3110.08E, *Geospatial Information and Services Supplemental Instruction to Joint Strategic Capabilities Plan (JSCP)*, July 17, 2013

DHE-M-3301.001, *Defense Human Intelligence Enterprise Manual, Volume 1: Collection Requirements, Reporting, and Evaluation Procedures* (S/NF), 1 February 2012

DCHE-M-3301.002, *Defense Counterintelligence and Human Enterprise Manual, Volume II: Human Intelligence Collection Operations* (S/NF), 22 June 2015

DoDD 3100.10, *Space Policy*, October 18, 2012

DoDI O-3115.07, *Signals Intelligence*, September 15, 2008

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

DoDI 3115.15, *Geospatial Intelligence*, December 6, 2011

DoDD 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*, June 11, 2019

DoDI 3305.09, *DoD Cryptologic Training*, June 13, 2013

DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation (U)*, June 22, 2009

DoDI S-3325.10, *Human Intelligence Activities in Cyberspace (U)*, June 6, 2013

DoDI 5000.56, *Programming Geospatial Intelligence, Geospatial Information and Services, and Geodesy Requirements for Developing Systems*, July 9, 2010

DoDD 5100.20, *National Security Agency/Central Security Service*, January 26, 2010

DoDI 5105.58, *Measurement and Signature Intelligence*, April 22, 2009

DoDD 5105.60, *National Geospatial-Intelligence Agency*, July 29, 2009

DoDD S-5200.37, *Management and Execution of Defense Human Intelligence (U)*, February 9, 2009

DoDI S-5200.42, *Defense Human Intelligence and Related Intelligence Activities (U)*, December 8, 2009

DoDI C-5205.01, *DoD Foreign Military Intelligence Collection Activities (FORMICA) (U)*, March 9, 2015

DoDD 5240.01, *DoD Intelligence Activities*, August 21, 2007

DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, August 8, 2016

DoDD 5250.01, *Management of Intelligence Mission Data in DoD Acquisition*, January 22, 2013

JP 2-03, *Geospatial Intelligence Support in Joint Operations*, 5 July 2017

JP 3-12, *Cyberspace Operations*, June 8, 2018

JP 3-14, *Space Operations*, 10 April 2018

NSA/CSSP 1-3, *National Security Agency/Central Security Service Governance*, September 10, 2008

NSA/CSSP 2-16, *National Security Agency/Central Security Service Support to the National Open Source Enterprise*, September 28, 2012

NSA Policy 4-25, *Cryptologic Training System*, May 9, 2007

National Security Council Intelligence Directive 6, *Signals Intelligence*, February 17, 1972

NSGD 1501, *Termination or Change of Geospatial Intel Products & Services*, March 17, 2016

NSGD 3201, *The Geospatial Intelligence (GEOINT) Functional Manager Standards Assessment (GFMSA) Program*, June 1, 2015

NSGI AP 3104, *Military Services Geospatial Intelligence Analysis & Production Program Mission Instruction*, March 27, 2013

USSID SE3000, *SIGINT Mission of the USAF Cryptologic Forces*, November 10, 2009

Adopted Forms

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

Abbreviations and Acronyms

AF/A2/6—Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations

AFGE—Air Force Geospatial Intelligence Enterprise

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC/CC—Commander, Air Force Materiel Command

AFSCC/CC—Commander, Air Force Service Cryptologic Component

AFSPC/CC—Commander, Air Force Space Command

COMACC—Commander, Air Combat Command

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

GEOINT—Geospatial Intelligence

HUMINT—Human Intelligence

IAW—In Accordance With

ISR—Intelligence, Surveillance, and Reconnaissance

MASINT—Measurement and Signature Intelligence

Multi-INT—Multiple-Source, Multiple-Discipline Intelligence, Surveillance, and Reconnaissance

NGA—National Geospatial-Intelligence Agency

NASIC—National Air & Space Intelligence Center

NSA/CSS—National Security Agency/Central Security Service

NSG—National System for Geospatial Intelligence

NSGD—National System for Geospatial Intelligence Directive

OSINT—Open Source Intelligence

PAI—Publicly Available Information

SIGINT—Signals Intelligence