BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 14-4

11 JULY 2019

Intelligence

MANAGEMENT OF THE AIR FORCE INTELLIGENCE, SURVEILLANCE, RECONNAISSANCE AND CYBER EFFECTS OPERATIONS ENTERPRISE

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 or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2/6E

Certified by: AF/A2/6
(Lt Gen VeraLinn Jamieson)

Supersedes: AFPD 14-1, 2 April 2004,
AFPD 14-2, 29 November 2007,
AFPD 14-3, 1 May 1998

Pages: 6

This Directive establishes the management and integration of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise. It implements Executive Order Number 12333, *United States Intelligence Activities*, Department of Defense Instruction (DoDI) O-3115.07, *Signals Intelligence (SIGINT)*, DoDI 3115.12, *Open Source Intelligence (OSINT)*, DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis*, DoDI 3305.02, *DoD General Intelligence Training and Certification*, DoDI 3305.09, *DoD Cryptologic Training*, DoDI 3305.10, *Geospatial-Intelligence (GEOINT) Training*, DoDI 3305.15, *DoD Human Intelligence (HUMINT) Training and Certification*, DoDI 3305.16, *DoD Measurement and Signature Intelligence (MASINT) Training and Certification*, DoDI 5000.02, *Operation of the Defense Acquisition System*, DoDI 5000.56, *Programming Geospatial-Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems*, Department of Defense Directive (DoDD) 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*, DoDD 5105.60, *National Geospatial-Intelligence Agency*, DoDD 5240.01, *DoD Intelligence Activities*, DoDD 5148.13, *Intelligence Oversight*, DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, DoDM 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, Intelligence Community Directive (ICD) 191, *Duty to Warn*, ICD 203, *Analytic Standards*, ICD 204, *National Intelligence Priorities Framework*, ICD 205, *Analytic Outreach*, ICD 501, *Discovery and Dissemination or Retrieval of Information within the*

Intelligence Community, ICD 502, *Integrated Defense of the Intelligence Community Information Environment,* ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information,* ICD 704, *Personnel Security,* ICD 705, *Sensitive Compartmented Information Facilities,* ICD 706, *Security Standards for Protecting Domestic IC Facilities.* This Policy Directive applies to all Air Force organizations, including the Air Force Reserve and Air National Guard, and their respective members. Ensure all records created as a result of processes prescribed in this publication are maintained per Air Force Manual 33-363, *Management of Records*, and disposed of per the Air Force Records Disposition Schedule in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility using the Air Force Form 847, *Recommendation for Change of Publication;* route AF Forms 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

This is a new publication that consolidates three previously existing Air Force Policy Directives (AFPDs); AFPD 14-1, AFPD 14-2 and AFPD 14-3, relating to Intelligence, Surveillance and Reconnaissance. This publication must be thoroughly reviewed for the changes it makes in those superseded AFPDs. Changes include: consolidation of content that referenced organizations and activities that have changed as the result of Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations reorganization.

1. OVERVIEW. This directive establishes Air Force policy to ensure the Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise provides intelligence to theater customers and decision-makers at all levels while enabling the Air Force to prepare for and conduct multi-domain operations across the full range of military operations.

2. POLICY. The Air Force will:

2.1. Oversee the training and proficiency in achieving intelligence and cyber effects operations activities of Combatant Commands by assigned forces and assets based on national, service and joint missions, capabilities, priorities, requirements, and responsibilities.

2.2. Train Air Force intelligence specialists to conduct intelligence activities in a manner that fully respects the rights and civil liberties of all United States persons while executing assigned Intelligence Community missions and functions.

2.3. Establish analysis and targeting capabilities necessary to fulfill national, service and joint requirements and leverage enterprise services to facilitate the secure sharing of information, technologies, and capabilities across the Intelligence Community in accordance with applicable Intelligence Community Directives.

2.4. Establish cryptologic policy and guidance necessary to perform Air Force cryptologic missions.

2.5. Embed intelligence as a collaborative partner into Air Force acquisition programs to ensure early and sustained support throughout the lifecycle of a program.

2.6. Ensure compliance with Intelligence Community and Department of Defense policy and guidance pertaining to the integrity and trustworthiness of the Air Force Intelligence, Surveillance, and Reconnaissance Enterprise, as well as information, personnel, systems,

facilities, security program management, and risk assessment in accordance with applicable Department of Defense and Intelligence Community Directives. Pay special attention to ensuring safeguards and proper oversight of the separation of Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations authorities and funding.

2.7. Ensure all intelligence community and cyber effects operations training is technically and operationally sound, conforms to Intelligence and Department of Defense standards and certification guidance, and supports applicable national, joint, and service missions.

3. ROLES AND RESPONSIBILITIES.

3.1. **The Secretary of the Air Force** designates an organization as the Service Cryptologic Component and assigns, after consulting with the Director, National Security Agency/Chief, Central Security Office, the Commander of the Service Cryptologic Component.

3.2. **Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6)** will:

3.2.1. Except as provided in para 3.1, execute all intelligence activity responsibilities assigned to the Secretary of the Air Force as the Service Component Head or Service Secretary for all applicable intelligence-related laws, executive orders and Intelligence Community and Department of Defense policy and guidance, as provided in Headquarter Air Force Mission Directive 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance Reconnaissance*. This does not apply to counterintelligence activities.

3.2.2. Ensure service intelligence collection, analysis, production, and dissemination align with national and joint intelligence priorities and adhere to Intelligence Community and Department of Defense standards and guidance. This ensures that associated intelligence entities align working environments and associated information technology infrastructure and capabilities to function as an integrated element of the Intelligence Community Information Technology Environment.

3.2.3. Appoint and ensure the Air Force Intelligence Oversight Officer has sufficient intelligence experience commensurate with assigned oversight responsibilities, has access to all component intelligence and intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments), has direct access to the Secretary of the Air Force to report on intelligence oversight compliance and has the appropriate support to fulfill the duties of the position.

3.3. **The Service Cryptologic Component Commander** shall:

3.3.1. Serve as the primary Service authority for all operations, programming, budgeting, training, personnel, policy, doctrine and foreign relationships for cryptologic activities.

3.3.2. Develop and publish Air Force-level policy and guidance relating to cryptologic matters as outlined in DoDI O-3115.07 and DoDD 5100.20. All Service Cryptologic Component publications associated with cryptologic and cryptologic-related matters.

3.3.3. Ensure Service cryptologic activities align with national and joint intelligence priorities, and comply with Unites States law as well as policies, directives and guidance promulgated by the President, Intelligence Community and Department of Defense.

Matthew P. Donovan
Acting Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

Executive Order Number 12333, *United States Intelligence Activities*

Public Law 108-458, *Intelligence Reform and Terrorism Prevention Act of 2004*,

Executive Order Number 12333, *United States Intelligence Activities*

Public Law 108-458, *Intelligence Reform and Terrorism Prevention Act of 2004*

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

DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis*, November16, 2016

DoDI 3305.02, *DoD General Intelligence Training and Certification*, August 12, 2015

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

DoDI 3305.10, *Geospatial-Intelligence (GEOINT) Training*, July 3, 2013

DoDI 3305.15, *DoD Human Intelligence (HUMINT) Training and Certification*, August 13, 2015

DoDI 3305.16, *DoD Measurement and Signature Intelligence (MASINT) Training and Certification*, August 13, 2015

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

DoDI 5000.56, *Programming Geospatial-Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems*, July 9, 2010

DoDD 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*, January 26, 2010

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

DoDD 5240.01, *DoD Intelligence Activities*, August 27, 2007

DoDD 5148.13, *Intelligence Oversight*, April 26, 2017

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

DoDM 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, December 7, 1982

Intelligence Community Directive Library: **https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives**

ICD 191, *Duty to Warn*, 21 July 2015

ICD 203, *Analytic Standards*, 2 January 2015

ICD 204, *National Intelligence Priorities Framework*, 2 January 2015

ICD 205, *Analytic Outreach*, 28 August 2013

ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, 21 January 2009

ICD 502, *Integrated Defense of the Intelligence Community Information Environment*, 11 March 2011

ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, 21 June 2013

ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, 1 October 2008

ICD 705, Sensitive Compartmented Information Facilities, 26 June 2010

ICD 706, Security Standards for Protecting Domestic IC Facilities, 16 June 2016

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

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

AFPD—Air Force Policy Directive

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

ICD—Intelligence Community Directive

Terms

Service Cryptologic Component—Term used to designate, separately or collectively, elements of the United States Army, Marine Corps, Navy, Air Force, and Coast Guard assigned to a CSS by the Secretary of Defense for the conduct of cryptologic operations funded by National Security Agency/Central Security Service. The Service Cryptologic Componet Commanders represent the interests of their respective cryptologic forces.