DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, D.C.

AFMAN14-403_AFGM 2026-01
17 March 2026

MEMORANDUM FOR DISTRIBUTION C
MAJCOMS/FOAs/DRUs

FROM: Air Force Intelligence (AF/A2)
1700 Air Force Pentagon
Washington DC 20330-1700

SUBJECT: Department of the Air Force Guidance Memorandum (AFGM) to AFMAN 14-403, S*ensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*

By Order of the Deputy Chief of Staff, Intelligence, this AFGM implements addition to AFMAN 14-403 to achieve Office of the Director of National Intelligence (ODNI) direction to implement Zero Trust (ZT). AF Intelligence includes the individuals, organizations, and Information Technology (IT) capabilities that collect, process, or share Sensitive Compartmented Information (SCI), or that, regardless of classification, are operated by the Intelligence Community (IC) and are in whole or in majority funded by the National Intelligence Program (NIP). Compliance with this memorandum is mandatory for all Regular Air Force, Air National Guard and Air Force Reserve operated AF Intelligence Information Enterprise (IE) assets and data, Intelligence, Surveillance, and Reconnaissance (ISR) systems (regardless of classification), AF-operated SCI systems (all which contain or process SCI), Nuclear Command, Control, and Communications (NC3) systems and other systems assigned to the AF Intelligence Authorizing Official (AO). The authorities to waive wing, unit, and delta level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. To the extent its directions are inconsistent with other USAF, Intelligence publications, the information herein prevails, in accordance with Department of the Air Force Instruction (DAFI) 90-160, Publications and Forms Management.

This guidance is applicable to all personnel conducting intelligence or intelligence-related activities, to include civilian employees and uniformed members of the Regular Air Force, the Air Force Reserve, and the Air National Guard, as well as those contractually obligated to comply with Headquarters Air Force (HAF) publications. Air National Guard personnel and units are excluded from this guidance while not in a federalized status supporting an intelligence mission. This publication does not apply to the United States Space Force.

Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (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. (T-2)

This memorandum becomes void after one year has elapsed from the date of this memorandum, or upon publication of an interim change (IC) or rewrite of the affected publication, whichever is earlier.

MAX E. PEARSON, Lt Gen, USAF
Deputy Chief of Staff, Intelligence

Attachment 1
Abbreviations and Acronyms

AC—Access Control

AF IC IE—Air Force Intelligence Community Information Enterprise

AO—Authorizing Official

AT—Awareness and Training

AU—Audit and Accountability

CA—Assessment, Authorization, and Monitoring

CDO—Chief Data Officer

CIO—Chief Information Officer

CISO—Chief Information Security Officer

CM—Configuration Management

CPO—Capability Product Owner

CP—Contingency Planning

DNI—Director of National Intelligence

DRU—Direct Reporting Unit

ESM—Enterprise Service Manager

ESSB—Enterprise Strategy Steering Board

ESSC—Enterprise Strategy Steering Council

FOA—Field Operating Agency

FMO—Functional Management Office

IA—Identification and Authentication

IC—Intelligence Community

ICD—Intelligence Community Directive

IE—Information Enterprise

IR—Incident Response

IT—Information Technology

MA—Maintenance

MAJCOM—Major Command

MP—Media Protection

NC3—Nuclear Command, Control, and Communications

NIP—National Intelligence Program

ODNI—Office of the Director of National Intelligence

PE—Physical and Environmental Protection

PL—Planning

PM—Program Management

PR—Program Reviews

PT—PII Processing and Transparency

RA—Risk Assessment

SA—System and Services Acquisition

SC—System and Communications Protection

SCI—Sensitive Compartmented Information

SI—System and Information Integrity

SoCC—Services of Common Concern

SR—Supply Chain Risk Management

ZT—Zero Trust

Attachment 2
Definitions

Intelligence Community (IC) – Established by statute, the IC, under the leadership of the Director of National Intelligence (DNI), is responsible to gather and analyze the intelligence necessary to conduct foreign relations and national security activities. There are currently 18 elements of the IC: CIA, NGA, NSA, DIA, NRO, the Intelligence element of the 5 military services, and 8 other civilian agencies. (U.S.C. 50)

Air Force Intelligence Community Information Enterprise (AF IC IE) - The integrated network and IT infrastructure supporting intelligence activities within the United States Air Force. The AF IC IE is designed to facilitate the collection, processing, analysis, and dissemination of intelligence information. It encompasses the hardware, software, data, and personnel necessary for Air Force intelligence operations. It aligns with broader Intelligence Community (IC) information enterprise standards to enable interoperability and data sharing across the IC. It includes all AF systems using or connected to Sensitive Compartmented Information (SCI) networks or systems (including those in SAP facilities), non-AF systems connected to AF intelligence networks, and all other AF Intelligence, Surveillance, and Reconnaissance (ISR) mission systems (regardless of classification). (AFMAN 14-403)

AF Intelligence Chief Information Officer (CIO) - Appointed by and responsible to HAF/A2 for oversight and governance of the AF IC IE and implementation of applicable directives, policy, guidance, architectures, standards, and protocols. Zero Trust is one aspect of these responsibilities. (ICD 500)

AF Intelligence Chief Data Officer (CDO) - The AF Intelligence CDO is responsible for the life cycle data management of sensitive, compartmented information (SCI) and other Intelligence data. As such she serves as the AF IC Element's primary authority for data lifecycle management and data governance over all data collected, acquired, created, held, analyzed, stored, accessed or otherwise used by the AF, which includes all use of SCI and all use of data in support of the AF intelligence mission. The AF Intelligence CDO is responsible to establish AF Intelligence guidance, standards, architecture, and procedures to manage data during its life cycle to meet Intelligence Community, DoD, and DAF requirements. (ICD 504)

ZERO TRUST (ZT) - ZT is a security model based on an acknowledgement that threats exist both inside and outside traditional network boundaries with the principle of "never trust, always verify." It shifts from perimeter-based security to a data-centric approach that enforces least privilege access and requires continuous authentication and authorization of every connection to protect sensitive data and resources. A ZT environment results in several key mission benefits: data will be democratized across entire enterprise; secured at the entity level, ensuring need-to-know access; limit the extent of any breach; scale to need; and make all data available to analytics platforms for decision support.

Attachment 3
Mapping of IC Capability Maturity Model to Cybersecurity Controls

Control Family	Affected IC Zero Trust Pillars							Capabilities (NIST SP 800-53 rev 5)
	Application/ Workload	Automation & Orchestration	Data	Device	Network/ Environment	User	Visibility & Analytics	
Access Control (AC)	✓	✓	✓	✓	✓	✓	✓	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-23, AC-24, AC-25
Awareness and Training (AT)			✓					AT-1, AT-2, AT-3
Audit and Accountability (AU)	✓	✓	✓				✓	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-11, AU-12, AU-13, AU-15
Assessment, Authorization, and Monitoring (CA)	✓	✓	✓	✓		✓	✓	CA-2, CA-3, CA-5, CA-7, CA-9
Configuration Management (CM)	✓	✓	✓	✓	✓		✓	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11, CM-12, CM-13, CM-14
Contingency Planning (CP)		✓	✓					CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10
Identification and Authentication (IA)	✓		✓	✓		✓		IA-1, IA-2, IA-3, IA-4, IA-4.4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12
Incident Response (IR)		✓	✓	✓		✓	✓	IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, IR-9, IR-10
Maintenance (MA)			✓			✓		MA-2, MA-4, MA-5
Media Protection (MP)			✓	✓				MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8
Physical and Environmental Protection (PE)		✓	✓					PE-1, PE-3, PE-6, PE-20
Planning (PL)		✓	✓					PL-1, PL-2, PL-4, PL-8, PL-10, PL-11
Program Management (PM)	✓	✓	✓	✓				PM-1, PM-5, PM-6, PM-7, PM-12, PM-16, PM-20, PM-21, PM-22, PM-23, PM-24, PM-25,

								PM-28, PM-30, PM-31
PII Processing and Transparency (PT)		✓	✓					PT-1, PT-2, PT-3, PT-4, PT-5, PT-7, PT-8
Risk Assessment (RA)	✓	✓	✓	✓			✓	RA-3, RA-5, RA-10
System and Services Acquisition (SA)		✓	✓		✓			SA-6, SA-9, SA-10
System and Communications Protection (SC)	✓	✓	✓	✓	✓			SC-1, SC-2, SC-3, SC-4, SC-5, SC-7, SC-8, SC-10, SC-11, SC-12, SC-13, SC-15, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-28, SC-30, SC-32, SC-39, SC-41, SC-43, SC-44, SC-51
System and Information Integrity (SI)	✓	✓	✓	✓			✓	SI-2, SI-3, SI-4, SI-5, SI-7, SI-8, SI-12, SI-15, SI-18, SI-19
Supply Chain Risk Management (SR)	✓							SR-2, SR-3, SR-5, SR-6, SR-7, SR-9, SR-10, SR-11

Attachment 4
AF IC ZT Governance

Responsive AF IC governance is required to ensure timely development and adoption of AF IC ZT solutions to efficiently and effectively mature the AF IC cybersecurity posture to meet ZT standards (Atch 3) and comply with the national mandates. To realize the unified approach established by this AFGM, AF IC governance will be conducted as established here to drive timely decisions, ensure technical and architectural choice alignment, resolve inter-dependency issues and programmatic challenges, and address policy needs, through a structured and collaborative process. (T-1)

The AF Intelligence CIO will appoint ESMs and CPOs in writing and assign them to provide incubator capability solutions and or sustain solutions once transitioned. AF Intelligence CIO will direct transition of proven solutions to an enterprise service provider, set adoption priorities for the AF IC IE, and define any continuing role of an incubator or relieve it of responsibility. (T-1)

An agile framework will be used for detailed planning and collaboration across the ESMs and CPOs. Quarterly planning intervals will drive alignment of all plans prior to execution, and sprint cycles will enable clear communication and adjustment to remain aligned and focused on the common effort. (T-1)

An Enterprise Strategy Steering Board (ESSB), chaired by the AF Intelligence CIO and composed of ESMs, AF IC Chief Information Security Officer (CISO), and AF IC CDO, will meet quarterly and additionally as required for timely decision-making, with the outcome being approved plans and direction to the ESMs and CPOs. This body will review and commit to each year's plans prior to execution, and it will have a strong and continual voice in decisions that impact the enterprise. As such, the Board will enable transparent review of technical alternatives and programmatic decisions with respect to AF IC technical approaches, solutions, and priorities. During Board sessions, tasking, initiation, and relief of responsibilities for both incubators and service providers, including transition points between them, will be approved. Furthermore, the primary hosting environment for AF IC ZT capabilities and services will be determined.
At every ESSB, each ESM will present the status of on-going efforts, a schedule of planned activities, any issues and opportunities, areas requiring decision or adjustment, and evaluation against IC ZT metrics. To track progress of each IC element toward IC ZT compliance, the IC CIO has established metrics against which all elements must report quarterly. The ESSB will review each quarter's AF IC ZT metrics prior to submission to the IC CIO. The AF Intelligence CIO will provide executive updates quarterly on the progress of AF IC ZT implementation. (T-1)

An Enterprise Strategy Steering Council (ESSC), chaired by the AF IC Enterprise ZT Portfolio Lead, will serve as a working group entailing ESMs, CPOs, and Subject Matter Experts (SMEs). The ESSC will be responsible for planning, problem-solving, and developing actionable recommendations related to AF IC ZT enterprise implementation. The ESSC, with support from the ZT FMO, will identify and address technical challenges, coordinate dependencies, align capability roadmaps, and develop well-vetted proposals to the ESSB for decision-making. (T-1)

In support of both the ESSB and the ESSC, the AF IC ZT FMO will establish and maintain in-depth understanding of the engineering, architecture, and compliance implications of the current

state of the enterprise and the proposed solutions. The AF IC ZT FMO will also identify gaps, opportunities, issues for resolution, and viable alternatives across policy, technical, organizational, and operational aspects of AF IC ZT implementation. (T-1)

The AF IC ZT FMO will adopt and maintain the AF IC enterprise perspective, responsive to and reporting to AF Intelligence CIO in its management and oversight roles for the AF IC IE. The AF IC ZT FMO will also maintain an interactive integrated schedule of activities of all the incubator, ESM, and CPO activities, including internal and external dependencies, to ensure a transparent understanding of the progress, opportunities, and risks to meeting ZT compliance across the AF IC IE. (T-1)

In support of the AF Intelligence CIO, the AF IC ZT FMO will leverage its contracted team supporting ESMs and CPOs, as well as its CIO support team, to assess technical and architectural alignment, coordinate activities across the ESMs, and track milestone accomplishment across the AF IC IE. The AF IC ZT FMO will assist the AF Intelligence CIO in completing ZT status reports for AF/A2, ODNI, and the Office of the Under Secretary of War for Intelligence and Security. (T-1)

Once an enterprise capability service provider is selected for a particular solution, detailed review and configuration management for that solution may be conducted by the governing body for that service provider (e.g., JWICS Executive Council for AFSCI). This allows the ESSC and ESSB to maintain a common understanding across the efforts through the ESM updates and focus on addressing cross-provider integration and other enterprise-wide matters. (T-2)

AF/A2OI, in partnership with AF/A2OR, will conduct Program Reviews (PRs) with each recipient of ZT funds, to understand obligation and expenditure status and to ensure best use of available funds to implement ZT capabilities across the AF IC. These reviews will occur quarterly (typically prior to ESSBs), be conducted in person at least once per year, and will include all ZT-related funding sources. While each PR will always require transparent status reporting by each recipient of ZT funds, the focus will rotate, based on the PPBE cycle. (T-1)

Attachment 5
Chapter 4. Zero Trust (ZT)

4.1. Additional guidance is required to achieve ODNI-mandated compliance with specific ZT maturity objectives for the IC, defining and directing roles, responsibilities, and governance required within the Air Force Intelligence to deliver ZT capabilities at "basic level" in FY26 and "intermediate level" in FY27 as directed by the ODNI Chief Information Officer (CIO). (T-0)

4.2. AF Intelligence will take a unified approach to ZT implementation, developing Services of Common Concern (SoCCs) once for use across the intelligence enterprise. In accordance with Intelligence Community Directive (ICD) 122, Intelligence Community Elements will adopt IC (DNI directed) SoCC as first choice solutions. In other cases, when Department of the Air Force (DAF) solutions meet IC requirements and ease implementation and sustainment across the portfolio, they will be selected as AF-level SoCCs. (T-1)

4.3. Air Force Intelligence will implement an IT service management framework in a federated execution model, leveraging service "incubators" when needed. These incubators will develop ZT managed services, prove them internally, then transition them to a service manager for full lifecycle sustainment as enterprise service offerings. This approach maximizes resource efficiency and leverages the best talent from across the enterprise, but it also introduces significant cross-organizational interdependencies which require structured collaboration and enterprise governance to ensure success. Tasking, initiation, and relief of incubators and service provider roles, as well as transition points among them, will be made at the Board, chaired by the AF Intelligence CIO. (T-1)

4.4. To ensure timely development and adoption of AF Intelligence ZT enterprise services, a responsive governance approach is hereby established (Atch 4). The AF Intelligence CIO, in coordination with the AF IC Chief Data Officer (CDO) and AF Intelligence Resources Chief, will govern this effort and report progress to point of contact identified below no less than quarterly. The CIO will issue guidance, as needed, to direct implementation actions required to achieve the outcomes mandated for the AF Intelligence IE. (T-1)

4.5. The AF Intelligence ZT Functional Management Office (AF IC ZT FMO), Enterprise Service Managers (ESMs), and Capability Product Owners (CPOs) will follow IC guidance to develop systems and capabilities to achieve intermediate maturity level ZT across the AF Intelligence IE by the end of FY27. The AF ZT FMO will provide technical and programmatic expertise to support the AF Intelligence CIO for governing ZT implementation, and it will support ESMs and CPOs to ensure a unified, integrated enterprise approach. Under direction of the AF Intelligence CIO, the AF Intelligence ZT FMO will also coordinate the activities necessary to enable and implement ZT solutions in accordance with this memorandum and other policy to ensure compliance with IC standards on their prescribed timelines. (T-1)

4.6. Once an AF Intelligence ZT solution has been made available to the enterprise, all SCI-level systems and capabilities must adopt these services. Specific requirements and timelines will be established by the AF Intelligence CIO in writing. Failure to do so will result in the system being considered untrusted, non-compliant, and external to the AF Intelligence IE.

Subsequent implementation guidance will be provided at the time each capability is delivered. Compliance will be assessed through AF Intelligence Risk Management and factor into Authorization to Operate decisions beginning 1 October 2026. Adoption will improve our cybersecurity posture and reduce mission owner responsibilities to manage duplicative cybersecurity services, freeing mission owners to focus resources on their unique requirements. (T-1)

4.7. My point of contact for this memo is my appointed AF Intelligence CIO, Col Mickey Jordan at (703) 614-2503 or mickey.jordan@us.af.mil.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 14-403

3 SEPTEMBER 2019

Intelligence

SENSITIVE COMPARTMENTED INFORMATION SECURITY AND INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYSTEMS CYBERSECURITY AND GOVERNANCE

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/A2/6UZ

Certified by: AF/A2/6U
(Brig Gen James R. Cluff)

Supersedes: AFMAN14-304, 23 December 2016

Pages: 12

This publication implements Air Force Policy Directive 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*. It is consistent with Department of Defense Manual (DoDM) 5220.22, *National Industrial Security Program Operating Manual,* DoDM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*, Intelligence Community Directive (ICD) 121, *Managing the Intelligence Community Information Environment,* ICD 500, *Director of National Intelligence Chief Information Officer*, ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, ICD 502, *Integrated Defense of the Intelligence Community Information Environment,* ICD 503, *Intelligence Community Information Technology Systems Security Risk Management,* ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information (SCI*), ICD 705, *Sensitive Compartmented Information Facilities*, ICD 710, *Classification Management and Control Markings System*, ICD 731, *Supply Chain Risk Management*. This publication applies to all civilian employees and uniformed members of the Regular Air Force, Air Force Reserve, and Air National Guard, including contractors when included in the terms of their contracts, who conduct or support Air Force intelligence missions.

Ensure 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 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 AF 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 requestors commander for non-tiered compliance items.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Changes include the addition of the Air Force Intelligence Community Chief ISR Information Officer and related roles and responsibilities.

1. Overview. This guidance contains 32 tiered compliance statements: 7 (T-0) and 25 (T-1). This manual provides guidance regarding the governance and management of the Air Force ISR Information Environment and the security, use and dissemination of sensitive compartmented information.

2. Roles and Responsibilities.

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

2.1.1. Manage the Air Force Sensitive Compartmented Information program and is the Air Force final authority for approving the release of intelligence to contractors.

2.1.2. Appoint the Air Force Cognizant Security Authority; an Air Force Intelligence Community Chief Intelligence Surveillance, and Reconnaissance (ISR) Information Officer, and Authorizing Official for Air Force Sensitive Compartmented Information and ISR Mission Systems.

2.1.3. Provide for the Air Force ISR, an information environment that enables the use, storage, processing, fusion, dissemination, and destruction of intelligence within Air Force Sensitive Compartmented Information and ISR mission systems.

2.1.4. Delegate the Cognizant Security Authority as the authority for management and oversight of the security program established for the protection of intelligence sources and methods, and for implementation of Sensitive Compartmented Information security responsibilities and procedures defined in Director of National Intelligence and Department of Defense policies for the activities under the Air Force/A2/6's purview.

2.1.5. Chair the Air Force ISR Information Environment Council to conduct strategic planning and governance of Air Force ISR enterprise architecture services, standards and information technology modernization.

2.2. **The Air Force Cognizant Security Authority will:**

2.2.1. Develop guidance for sensitive compartmented information security and the Intelligence Community Badge System IAW Intelligence Community Standard (ICS) 704-01, *Intelligence Community Badge System*.

2.2.2. Manage and approve access to Scattered Castles, the authoritative database for intelligence community clearances, IAW Intelligence Community Policy Guidance (ICPG) 704.5, *Intelligence Community Personnel Security Database Scattered Castles*, and represent the Air Force on the Scattered Castles Executive Steering Group.

2.2.3. Represent the Air Force on the Office of the Director of National Intelligence Access Control, IAW ICS 704-01; the Classification Markings Implementation, IAW Intelligence Community Directive (ICD) 710, *Classification Management and Control Markings System*, and the Intelligence Community Physical and Technical Security Program Working Groups, IAW ICD 705.

2.2.4. Advise the AF/A2/6 on public disclosure issues.

2.3. **The Air Force Intelligence Community Chief ISR Information Officer will:**

2.3.1. Manage Air Force ISR Information Environment Council structure and activities.

2.3.2. Develop guidance for the Air Force ISR information environment in support of Air Force and Intelligence Community requirements.

2.3.3. Advise the AF/A2/6 regarding Air Force ISR information environment risks and priorities and oversee Air Force ISR Federal Information Security Modernization Act compliance and reporting.

2.3.4. Appoint a Chief ISR Information Security Officer responsible to the Air Force Intelligence Community Chief ISR Information Officer.

2.3.5. Represent the Air Force on the Intelligence Community Chief ISR Information Officer Council and subordinate working groups IAW Intelligence Community Chief Information Officer 2012-0212 *Intelligence Community Information Technology Environment Governance Framework*, IC CIO 2016-0011, *Waiver and Exceptions*, IC CIO 2016-0129, *Program of Activities and Milestones (POA&M) Process*.

2.3.6. Submit associated compliance reporting to the Intelligence Community Chief Information Officer, IAW ICD 500.

2.3.7. Oversee Air Force Intelligence Community Integrated Defense, to include security coordination, incident response, insider threat, and computer network defense, IAW ICD 502 and AFI 16-1402, *Insider Threat Program Management*. Represent the Air Force Intelligence Community on the Air Force Insider Threat working group established by AFI 16-1402.

2.3.8. Implement ICD 121, ICD 501, ICD 503, and ICD 731, across Air Force ISR systems and capabilities. Coordinate with the Air Force Intelligence Community Chief Data Officer as necessary.

2.3.9. Approve Cybersecurity Strategy prior to contract solicitation for sensitive compartmented information and ISR system acquisitions and procurements, regardless of contract value.

2.4. **The Authorizing Official for Air Force Sensitive Compartmented Information and ISR Mission Systems will:**

2.4.1. Chair the Air Force ISR Risk Executive Function, established by this manual, to provide consistent ISR cybersecurity risk management across the Air Force ISR information environment IAW ICD 503.

2.4.1.1. The Risk Executive Function consists of cybersecurity and mission system professionals (Headquarters Air Force, Major Command (MAJCOM), Wing and program office personnel) from across the Air Force ISR community, chartered to inform and advise execution of the Air Force ISR cybersecurity program from an Air Force ISR enterprise-wide perspective. As such, the Risk Executive Function meets no less than quarterly to share information, address issues, and recommend courses of action to ensure the aggregate risk posture of the Air Force ISR enterprise is well aligned with strategic goals and adequate to enable mission success.

2.4.1.2. This Risk Executive Function establishes a strategy, standards and reporting structure, and enable information sharing to all levels of the Air Force ISR community to enable an expedient and comprehensive cybersecurity program, effectively and commonly conducted across all Air Force ISR networks and mission systems.

2.4.2. Execute risk management and authorization decisions for mission systems IAW ICD 503.

2.5. **The Air Force Intelligence Community Chief ISR Information Security Officer will:**

2.5.1. Implement the Air Force ISR Cybersecurity Program across projects that reside on or connect to Air Force sensitive compartmented information networks and Air Force ISR mission systems, IAW *Federal Information Security Modernization Act of 2014*, National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-55, Rev 1, *Performance Measurement Guide for Information Security*, Committee on National Security Systems Instructions (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*, ICD 503, and, as appropriate, Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*. Ensure currency with changes in Department of Defense, NIST, and CNSS standards, and coordinate with the Chief ISR Information Officer to direct appropriate compliance.

2.5.2. Prepare Intelligence Community Directive compliance reports for submission to the Air Force Intelligence Community Chief ISR Information Officer.

2.5.3. Advise program managers and information system owners regarding cybersecurity requirements for sensitive compartmented information and ISR system acquisitions and procurements, prior to Request for Proposal release, regardless of contract value.

2.5.4. Maintain certification IAW DoDM 8570.01, *Information Assurance Workforce Improvement Program.*

2.5.5. Establish and ensure compliance with certification requirements for assigned cybersecurity roles across the Air Force ISR Information Environment IAW DoDM 8570.01.

2.6. **The Air Combat Command (ACC) Director of Intelligence will:**

2.6.1. Serve as lead for implementation of enterprise services for the Air Force ISR Information Environment, including Air Force Joint Worldwide Intelligence Communications System modernization and Intelligence Community Information Technology Environment adoption. Plan, program and budget for common services.

2.6.2. Execute the sensitive compartmented information and collateral ISR Insider Threat Programs, IAW AFI 16-1402 and guidance from the Air Force Intelligence Community Chief ISR Information Officer, Air Force Intelligence Community Authorizing Official, Air Force Intelligence Community Chief Information Security Officer and Administrative Assistant to the Secretary of the Air Force.

2.7. **MAJCOM Directors of Intelligence, Field Operating Agency/Direct-Reporting Unit/Wing Commanders will:**

2.7.1. Establish a command-wide sensitive compartmented information security program and ensure each sensitive compartmented information facility is accredited/reaccredited IAW ICD 705 and DoDM 5105.21 **(T-0)**.

2.7.2. Plan, program, and budget security and Air Force ISR information environment architecture requirements for command-owned (not Air Force JWICS core service) capabilities, mission systems and networks (including enclaves) that operate in or connect to the Air Force ISR Information Environment **(T-1)**.

2.7.3. Ensure command systems and sites within the Air Force ISR Information Environment that cannot be addressed directly by Twenty-Fifth Air Force comply with Air Force Intelligence Community Chief Information Officer and Air Force Cognizant Security Authority direction, and cyber-operational orders for security, modernization, and computer network defense **(T-1)**.

2.7.4. Ensure all appointed MAJCOM Chief ISR Information Security Officials maintain certification IAW DoDM 8570.01 and oversee subordinate unit compliance with ICD 502/ICD 503 **(T-1)**.

2.7.5. Establish a command-wide special security representative, contract special security representative, and a contract officer representative training program **(T-1)**.

2.7.6. Ensure sensitive compartmented information indoctrinated personnel under their cognizance comply with reporting requirements IAW ICD 703and receive security awareness information at least annually. In addition, derivative classifiers training must be completed once every two years **(T-1)**.

2.7.7. Report on and complete Twenty-Fifth Air Force operational orders for the operation, maintenance and defense of special compartmented information and ISR systems **(T-1)**.

2.8. **MAJCOM Directors of Intelligence, Field Operating Agency/Direct-Reporting Unit Special Security Officers will:**

2.8.1. Process temporary/interim eligibility request for access to sensitive compartmented information using the procedures in DoDM 5105.21, Volume 3 **(T-1)**.

2.8.2. Report to the Cognizant Security Authority within 24 hours if an indoctrinated person is killed, captured/missing in action, absent without leave, or considered a deserter **(T-1)**. (**Note:** This applies if a person had Sensitive Compartmented Information access within the last three years.)

2.8.3. Certify the sensitive compartmented information access of foreign nationals authorized to visit their command's sensitive compartmented information facilities **(T-1)**.

2.8.4. Manage the security requirements of contracts requiring access to sensitive compartmented information in a facility under their control IAW DoDM 5220.22 and DoDM 5105. 21, Volume 3 **(T-1)**.

2.8.5. Approve unclassified speakerphones and establish and/or approve Temporary Sensitive Compartmented Information Facilities and Temporary Secure Working Areas for their command **(T-1)**.

2.9. **Senior Intelligence Officers will:**

2.9.1. Manage the sensitive compartmented information security and information systems in their purview, including those they procure, own or operate. For systems without an acquisition Program Manager, appoint an Information System Owner for any ISR information technology system procured, owned or operated by the MAJCOM or subordinate unit, responsible for the overall system lifecycle, including funding requirements and coordination with the MAJCOM Chief ISR Information Security Officer prior to any related procurement action **(T-1)**.

2.9.2. Appoint, oversee and budget for a Special Security Officer and a site Information System Security Manager/Officer or, if at the MAJCOM Directors of Intelligence and Field Operating Agency/Direct Reporting Unit level, oversee and budget for a Chief ISR Information Security Officer **(T-1)**.

2.10. **Commander, 625th Air Communications Squadron will:**

2.10.1. Report incidents and vulnerabilities across the Air Force Intelligence Community Information Environment IAW ICD 502 **(T-0)**.

2.10.2. Operate the Security Coordination Center and the Incident Response Center for the Air Force Intelligence Community **(T-1)**.

2.10.3. Direct, coordinate and resolve security events in coordination with units, the Air Force Intelligence Community Chief ISR Information Officer and Chief ISR Information Security Officer **(T-1)**.

2.10.4. Command and control the Air Force Joint Worldwide Intelligence Communications System and operate a 24/7 Enterprise Operations Center, in coordination with regional Enterprise Service Centers, as required **(T-1)**.

2.10.5. Implement and maintain information technology services required to operate, monitor and defend Air Force Joint Worldwide Intelligence Communications System **(T-1)**.

2.10.6. Manage and implement user activity monitoring for the Air Force Intelligence Community and support the Insider Threat Audit Program IAW AFI 16-1402 **(T-1)**.

2.10.7. Perform security control assessments IAW ICD 503 and the priorities of the Chief ISR Information Officer, Air Force Intelligence Community Chief ISR Information Security Officer and Authorizing Official **(T-1)**.

2.11. **Acquisition Program Managers and Information System Owners for sensitive compartmented information and ISR systems will:**

2.11.1. Coordinate with the Air Force Intelligence Community Chief ISR Information Officer and Air Force Intelligence Community Chief ISR Information Security Officer at program initiation to ensure design and deliverables are sufficient to ensure timely authorization decisions **(T-1)**.

2.11.2. Work with the appropriate MAJCOM Chief ISR Information System Officer to coordinate cybersecurity requirements, produce a cybersecurity strategy for the Chief ISR Information Officer approval, and meet cybersecurity responsibilities across the acquisition lifecycle **(T-0)**.

3. Security.

3.1. **Personnel Security.**

3.1.1. Access control. Sensitive Compartmented Information Security Officials use Joint Personnel Adjudication System, Defense Information System for Security, and/or Scattered Castles to determine if a person is eligible for a Sensitive Compartmented Information indoctrination. During a member's initial indoctrination, the special security officer will use the current Intelligence Community Form 4414, *Sensitive Compartmented Information Nondisclosure Agreement (SCI NDA)* **(T-0)**.

3.1.2. Temporary/Interim Eligibility for Access to Sensitive Compartmented Information. Eligibility requests must be unclassified and forwarded by the servicing special security office to the appropriate Department of Defense Central Adjudication Facility for approval using the procedures in DoDM 5105.21 **(T-0)**.

3.2. **Information Security.** Individuals producing classified documents, either originally or derivatively, must mark the document using the Intelligence Community Markings System Register, IAW ICD **(T-0)**.

3.3. **Physical Security.**

3.3.1. Defense Intelligence Agency is the authority for accrediting Department of Defense permanent sensitive compartmented information facilities, except for those facilities under the control of the National Security Agency, National Geospatial Agency, or National Reconnaissance Office.

3.3.2. Special security officers will establish written procedures for random inspections of hand-carried items entering or exiting sensitive compartmented information facilities during operational hours **(T-0)**.

3.3.3. MAJCOM/A2, or designee, approves Sensitive Compartmented Information Facility's concept approvals to be constructed within their area of responsibility. MAJCOM Special Security Officer forwards approved concept approval and construction security plan to Defense Intelligence Agency for project approval.

3.3.4. MAJCOM/A2 is the approval authority for special access programs residing in sensitive compartmented information facilities. Air Force Cognizant Security Authority approves special access programs in multiple sensitive compartmented information facilities and the associated Co-Use Agreements.

3.4. **Industrial Security.**

3.4.1. Special security officers will forward DD Form 254 and the associated Sensitive Compartmented Information Addendum to the MAJCOM when the contract involves multiple bases **(T-1)**. Local contracts may be approved by the base special security officer.

3.4.2. The local contracting officer's representative will be indoctrinated into sensitive compartmented information to endorse and verify sensitive compartmented information contract deliverables **(T-1)**.

3.4.3. Special security officers will notify the appropriate contracting officer's representative and cognizant contracting officer of any incident that involves a contractor **(T-1)**.

3.4.4. Special security officers maintain current DD Form 254, *Contract Security Classification Specifications,* contracting office's representative appointment and duty letters, and a list of contractors working the specific contract (validated by contracting office representative on an annual basis or when changes are made). Records will be maintained for two years after contract ends **(T-1)**.

3.4.5. Special Security Officers will process requests for National Interest Determinations for companies operating under a Special Security Agreement to mitigate Foreign Ownership, Control, or Influence using the procedures provided in AFI 16-1406, *Air Force Industrial Security Program* **(T-1)**.

VERALINN JAMIESON, 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

AFI 16-1402, *Insider Threat Program Management*, 5 August 2014

AFI 16-1406, *Air Force Industrial Security Program,* 25 August 2015

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

AFI 63-101/20-101, *Integrated Life Cycle Management*, 9 May 2017

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

DoDM 5220.22, *National Industrial Security Program Operating Manual,* May 18, 2016

DoDM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security,* May 16, 2016

DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, April 5, 2018

DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*, April 4, 2018

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* March 12, 2014

DoDM 8570.01, *Information Assurance Workforce Improvement Program*, 10 November, 2015

ICD 121, *Managing the Intelligence Community Information Environment,* 19 January 2017

ICD 500, *Director of National Intelligence Chief Information Officer*, 7 August 2008

ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, 29 January 2009

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

ICD 503, *Intelligence Community Information Technology Systems Security Risk Management,* 21 July 2015

ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information (SCI*), 21 July 2013

ICD 705, *Sensitive Compartmented Information Facilities,* 26 May 2010

ICD 710, *Classification Management and Control Markings System*, 21 June 2013

ICD 731, *Supply Chain Risk Management*, 7 December 2013

ICPG 704.5, *Intelligence Community Personnel Security Database Scattered Castles*, 2 October 2008

ICS 704-01, *Intelligence Community Badge System*, 7 January 2016

IC CIO 2012-0212, *Intelligence Community Information Technology Environment Governance Framework*, 18 April 2012

IC CIO 2016-0011, *Waiver and Exceptions*, 9 May 2016 [**https://intelshare.intelink.ic.gov/sites/odni/cio/guidancecatalog**]

IC CIO 2016-0129, *Program of Activities and Milestones (POA&M) Process*, 21 July 2016[**https://intelshare.intelink.ic.gov/sites/odni/cio/guidancecatalog**]

CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014

FISMA, *Federal Information Security Modernization Act of 2014*, 18 December 2014

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, December 2018

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

NIST SP 800-55, Rev 1, *Performance Measurement Guide for Information Security*, 16 July 2008 [**https://intelshare.intelink.ic.gov/sites/odni/cio/guidancecatalog**]

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 254, *Contract Security Classification Specifications*

IC Form 4414, *Sensitive Compartmented Information (SCI) NdA*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

ACC—Air Combat Command

CNSSI—Committee on National Security Systems Instruction

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

IAW—In Accordance With

ICD—Intelligence Community Directive

ICPG—Intelligence Community Policy Guidance

ICS—Intelligence Community Standard

ISR—Intelligence, Surveillance, and Reconnaissance

MAJCOM—Major Command

NIST—National Institute of Standards and Technology

Terms

Scattered Castles—Intelligence community's authoritative personnel security repository for verifying personnel security access approvals regarding sensitive compartmented information and other controlled access programs, visit certifications and documented exceptions to personnel security standards.