



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

AFGM2015-33-03

23 July 2015

25 July 2016

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Air Force Guidance Memorandum, *Air Force Interoperability and Supportability of Information Technology and National Security Systems (IT/NSS)*

ACCESSIBILITY: Publication is available for downloading on the e-Publishing web site at:
www.e-Publishing.af.mil

RELEASABILITY: There are no releasability restrictions on this publication.

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately issues policy on Air Force Interoperability and Supportability of Information Technology and National Security Systems (IT/NSS). Compliance with this Memorandum is mandatory.

This guidance memo applies to all military and civilian Air Force personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.

This AFGM may be supplemented at any level, but all supplements that directly implement this publication must be routed to SAF/CIO A6 Policy Branch for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items.

Ensure that 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 Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). 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 Air Force.

Air Force Interoperability & Supportability Policy and Information Support Plan Process

The guidance below defines the policy, roles and responsibilities on management, implementation and interoperability and supportability certification of Air Force IT/NSS programs, including subsystems that are integral to embedded weapons platforms and non-program of record materiel solution efforts as detailed in the JCIDS Manual, pending publication of the AFI, Interoperability and Supportability certification of Air Force Information Technology and National Security Systems (IT/NSS).

1. Introduction. In accordance with Title 10, USC. Section 2223, *Information Technology; Additional Responsibilities of the Chief Information Officer* (Reference (a)), the Chief Information Officers (CIO) of Military Departments will “ensure that information technology and national security systems are in compliance with standards of the Government and the Department of Defense; ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense; and coordinate with the Joint Staff with respect to information technology and national security systems”. These and other interoperability-related responsibilities of the CIO are outlined in detail in DoDI 8330.01, *Interoperability of IT, Including NSS* (Reference (b)) which tasks the Military Department CIO with oversight and implementation of programs and processes to ensure interoperability risk mitigation and avoidance for IT and NSS.

1.1. All Air Force IT and NSS must participate in and comply with interoperability risk assessments via the Information Support Plan or through alternative means set forth in the ISP program. This is true for all mission areas: warfighter, business, intelligence and enterprise information environment. A viable interoperability strategy within Air Force programs is a key enabler to our ability to interoperate within the bounds of the Air Force as well as across component, joint, combined, and coalition forces, other US Government department and agencies, and non-governmental organizations as required based on operational context.

1.2. DoDI 8330.01 (Ref b) directs that DoD Component IT must interoperate to the maximum extent practicable; be evaluated early and with sufficient frequency throughout its lifecycle to capture and assess changes affecting interoperability in a joint, multinational, and interagency environment; and be certified for interoperability or attain interim or waiver approval before connection to any DoD network, other than for test purposes. The following policy and process for Interoperability and Supportability risk assessments performed through the Information Support Plan and technical support documents are based on SAF/CIO A6 roles and responsibilities identified in DoD, Joint and Air Force upper-level guidance:

2. Information Support Plan (ISP)

2.1. The Information Support Plan is a technical document required by DoDI 5000.02 and DoDI 8330.01 that provides Program Managers a means to identify and resolve potential information support implementation issues and risks that, if not properly managed, will limit or restrict the

ability of a program to be operationally employed to support existing and future mission requirements. It is an authoritative document that directly informs the program's Test and Evaluation Master Plan with threshold and objective operations parameters, and it is a key vehicle that supports validation of a program's eligibility for interoperability certification. The ISP contains or includes links to the Net-Ready Key Performance Parameter (NR-KPP) along with supporting architectural data. Acquisition programs develop ISPs when required by DoDI 5000.02 IAW with the requirements provided in DoDI 8330.01 and Air Force guidance.

2.2. The ISP identifies IT and information (including intelligence) needs, dependencies, and interfaces for programs in all acquisition categories, focusing on net-readiness, interoperability, information and system supportability, and information sufficiency concerns. The ISP assesses the program's path toward becoming Net-centric and describes the program's Cybersecurity compliance, Bandwidth and Frequency Spectrum dependencies, among others.

2.3. The direction to develop information support plans is contained in DoDI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*, 21 May 2014. In accordance with DoDI 8330, the SAF/CIO A6, or designate is the approval authority for Air Force Information Support Plans. The Air Force Interoperability Certification Manager is designated to oversee development, review, and approval of AF ISPs. Air Force commands with equity in programs undergoing review will provide subject-matter expert (SME) support for assessment of ISPs from their mission perspective via the Global Information Grid (GIG) Technical Guidance Federation (GTG-F) system.

2.4. Air Force Instructions that require the development of ISPs include: AFI 10-601, *Capabilities Based Requirements Development*, 12 July 2010; AFI 63-101/20-101, *Integrated Life Cycle Management (ILCM)*, 23 February 2015; and AFI 99-103, *Capabilities Based Test and Evaluation*, 16 October 2013. All Air Force organizations involved in the acquisition of IT or NSS are required to develop ISPs in accordance with the above Directives/Instructions. Specific guidance and instructions for ISP development are provided in the *Air Force Program Manager's Guide for Development of the Information Support Plan*, available on the Air Force Interoperability & ISP SharePoint site: https://cs3.eis.af.mil/sites/OO-AQ-AF-18/_layouts/user.aspx

3. GIG Technical Guidance Federation (GTG-F)

3.1. The Information Support Plan will be developed within the GIG Technical Guidance Federation (GTG-F) using the Enhanced Information Support Plan (EISP) Enterprise Service Version (ESV) template. The GTG-F is an integrated ISP development, staffing, analysis, approval and archiving environment used by DoD, Joint and COCOM agencies. The GTG-F replaces and consolidates capabilities of the old Air Force C4I Program Assessment Tool (ACPAT) and Joint C4I Program Assessment Tool (JCPAT) systems. The GTG-F homepage is located at <https://gtg.csd.disa.mil/>.

3.2. Program Managers, with sponsor support, shall develop an ISP for all IT and National Security Systems that exchange data, unless waived by the SAF/CIO A6 ISP Manager. The required format, content, and process for ISP assessment provides a mechanism to identify and resolve implementation issues related to IT and NSS infrastructure and support elements. ISPs

will identify system information needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency. The ISP will include an operational employment concept; system interface descriptions; required information exchanges; IT and NSS information support requirements derived from analysis of applicable Joint Operating Concepts (JOC), Joint Functional Concepts (JFC), Joint Integrating Concepts (JIC) and JCIDS documentation. In addition, it will include the associated integrated architecture(s); potential issues/risks; and proposed solutions or risk mitigation plans.

3.3. Program Managers shall describe IT/NSS dependencies and interface requirements in sufficient detail to enable supportability requirements planning, test planning, and for verification of the Net-Ready Key Performance Parameter. Programs completing the ISP process are required to coordinate with the AF Interoperability Steering Group (ISG) representative for system certification test. The ISP enables the Air Force and Joint communities to conduct IT/NSS supportability reviews for all ACAT-designated programs.

4. Net-Ready Key Performance Parameter (NR-KPP):

4.1. In order to ensure system interoperability, DoDI 8330.01 and the JCIDS Manual, *Manual for The Operation of the Joint Capabilities Integration*, 12 February 2015, require all IT/NSS to receive formal approval for Net Ready KPPs. When systems have joint interfaces, the Joint Staff, through the Joint Capabilities Integration Development System, certifies Net Ready KPPs. SAF/CIO A6 will coordinate on NR KPPs for IT/NSS without joint, multinational, or interagency interoperability requirements prior to the Air Force Requirements Oversight Council (AFROC) and prior to Joint Requirements Oversight Council (JROC) when the Air Force is the sponsor.

5. Architecture Requirements:

5.1. Solution architectures for all Air Force IT programs undergoing development or modification will be submitted with the Information Support Plan. The ISP review will include assessment for DoD Information Enterprise Architecture (DIEA) alignment and applicable Joint Mission Thread (JMT) architectures. In addition, solution architectures will be reviewed to ensure standards compliance for interoperability, and to ensure system supportability by Air Force commands and agencies tasked with mission support in various areas of responsibility. Although the architecture assessment includes the requirements of Clinger-Cohen Act (CCA) Table Element #8 Interoperability requirements, additional considerations apply for a complete CCA compliance review, per AFMAN 33-407, *Air Force Clinger-Cohen Act Compliance Guide*, dated 24 October 2012.

5.2. Following Air Force approval, artifacts will be staffed to the DoD and Joint communities as part of the ISP package for Joint-level assessment and approval, when applicable. If concurrent staffing is conducted, the ISP packages will be simultaneously staffed to both the Air Force and Joint communities for assessment.

6. Air Force Implementation Baseline (IB) and Common Computing Environment (AF CCE):

6.1. As the Air Force transitions to the Joint Information Environment, accelerated application releases for mission capability and enhanced cybersecurity of our enterprise information

environment, among other technology improvements, will be key to our success. We will realize greater capability faster and at reduced costs through the use of Air Force CCE and IB tools and services.

6.2 All Air Force IT programs are required to use the following actions to document the current status of implementing IB and CCE specifications, as outlined in AFGM2014-33-05 *Common Computing Environment*, 17 Sep 14: The data will be entered in the Enterprise Information Technology Data Repository (EITDR) via the Interoperability Filter under Question G-13. In this section, program offices will address issues a thru d below. In addition, every program submitting an Information Support Plan for assessment will enter the following statement in Section 3.1 (Time Phases) of the EISP Template in the GTG-F, indicating they have updated question G-13 in EITDR with CCE planning data as required: "IAW AFGM 2014-33-05, the [cite name of program/system] program planning data for CCE implementation has been entered in EITDR under Interoperability/ISP Filter Question G-13".

- a) Identify what items or services, i.e., Platforms and additional application support tools/capabilities, are being used and implemented from the current AF CCE Service Catalog.
- b) If the program has not implemented the requirements of an approved CCE (utilizing the AF Implementation Baseline (IB) specifications), explain the reasons why not.
- c) If the program office is using other than approved platforms and application support tools, state whether this requirement has been documented and identified to the SAF/CIO A6 Target Baseline Team at: usaf.pentagon.saf-cio-a6.mbx.a6sa-workflow@mail.mil, and the Implementation Baseline Team at: Program Executive Office Command, Control, Communications, Intelligence and Networks (<https://intelshare.intelink.gov/sites/ib/SitePages/Home.aspx>). The point of contact, who can also be reached via this site, is Ms. Maria N. Stanley, AFMC AFLCMC/HNII.
- d) Provide a "get well" plan, with implementation dates, to become compliant with AF IB/CCE requirements.

NOTE: For all systems in sustainment, the response in EITDR will be "N/A." As systems or applications comply with Federal Data Center Consolidation Initiative (FDDCI), Joint Information Environment (JIE), and Cyber Discipline efforts, the responsible program management offices must determine whether to sunset or modernize each system/application. If modernizing, program offices must use approved CCE tools and will need to update program information accordingly in EITDR per item a above. In addition, CCE and IB do not apply to NSS embedded software (such as aircraft platform IT).

The effective date for all IT programs to update the Interoperability Filter G-13 with IB/CCE status information is 31 July 2015.

7. Air Force Interoperability Steering Group (ISG) Representative:

7.1 The SAF/CIO A6 appointed representative to the DoD Interoperability Steering Group (ISG) is the Air Force interface to DoD CIO, Joint Staff, PMs, sponsors and the Joint Interoperability Test Command (JITC) on coordination of interoperability issues among the DoD Components,

and between DoD and other Federal level agencies/activities, and allied/coalition partners, as required.

7.2. The DoD Interoperability Steering Group is a chartered group of representatives from the Military Departments, the Office of the Secretary of Defense, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense.

7.3. The ISG provides recommendations on the management and oversight of the DoD Components' interoperability activities, to include: review of critical interoperability issues and recommend solutions, review and resolve issues related to interoperability test and certification, adjudicate requests for ICTOs, provide advice to the DoD CIO, when requested on waivers to interoperability policy; nominate systems for inclusion on the DoD Interoperability Operating at Risk List (OARL), and adjudicate unresolved issues resulting from the ISP review process.

7.4. Details on the activities and functions of the ISG and guidance on interoperability processes and procedures for the military services are located in the JITC Interoperability Process Guide (IPG), version 2.0, dated 23 March 2015.

Questions regarding this policy may be directed to the Compliance Division Interoperability Certification Program Office at usaf.pentagon.saf-cio-a6.mbx.af-isp-information-support@mail.mil. My point of contact for this memo and for Air Force Interoperability & Supportability Certification issues is Ms. Telia A. Hughes, SAF/A6XA (Telia.A.Hughes.civ@mail.mil), DSN 225-6111 (703) 695-6111.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon release of an Air Force publication incorporating this guidance, whichever is earlier.

WILLIAM J. BENDER, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

Attachments:

1. Required Architecture Viewpoints for Air Force ISP Assessment
2. Glossary of References and Supporting Information

Attachment 2

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

- (a) Title 10, USC. Section 2223, Information Technology; Additional Responsibilities of the Chief Information Officer
- (b) DoDI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*, 21 May 2014
- (c) JCIDS Manual, *Manual for The Operation of the Joint Capabilities Integration*, 12 February 2015
- (d) AFGM2014-33-05, *Common Computing Environment*, 17 September 2014
- (e) AFI 63-101/20-101, *Integrated Life Cycle Management (ILCM)*, 23 February 2015

Additional Guidance

Additional publications that address Air Force Interoperability & Supportability requirements and align with this guidance are listed below:

AFI 10-601, Operational Capability Requirements Development, addresses Joint Capabilities Integration and Development (JCIDS)

AFI 33-580, Spectrum Supportability, Air Force Communications and Information Spectrum Management provides guidance on policy and processes for spectrum requirements which must be documented in the Information Support Plan, pre-coordinated through the Air Force Spectrum Management Office (AFSMO).

AFMAN 33-145, Collaboration Services and Voice Systems Management, 16 May 2013 provides policy and guidance on the use of Information Technology Unified Capabilities (UC) for the Air Force.

AFPD 33-5, Warfighting Integration addresses policy on Information Technology Integration for Air Force systems.

Joint Interoperability Test Command (JITC) Interoperability Process Guide (IPG), version 2.0, dated 23 March 2015 provides policy and guidance for documenting and obtaining interoperability certification for joint systems.

AFLCMC Managed Services Office, Mr. Michael Clark (michael.clark.71@us.af.mil)

Common Computing Environment Software Registration Portal:

<https://software.forge.mil/sf/projects/af-cce?uri=/sf/projects/af-cce>