

**BY ORDER OF THE COMMANDER  
NATIONAL AIR & SPACE  
INTELLIGENCE CENTER**

**NASIC INSTRUCTION 33-108**

**6 JUNE 2013**



**Communications**

**NASIC STRATEGIC IT MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the E-Publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: NASIC/SCXE

Certified by: NASIC/SC  
(Col William Stevenson)

Supersedes: NASICI 33-108, 30 August  
2010

Pages: 9

---

The NASIC Communications and Information (SC) Director is also the NASIC Chief Information Officer (CIO) and is the authority on and responsible for the content and accuracy of this instruction. This Instruction implements Air Force Policy Directive (AFPD) 33-1, *Cyberspace Support*. This instruction establishes guidance to ensure standardized planning, acquisition, prioritization, implementation, sustainment, and all other aspects of life-cycle management of Information Technology (IT) at the National Air and Space Intelligence Center (NASIC). All military, civilian, contractors, visitors, and tenant partners are required to adhere to the policies and standards in this instruction to ensure effective management and execution of all IT implemented within the NASIC complex and its annexes. This instruction also applies to Air Force Reserve Command (AFRC) Units and Air National Guard (ANG) Units assigned to NASIC. 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 Form 847s from the field to NASIC Publications Office (NASIC/SCOK), 4180 Watson Way, Wright-Patterson AFB, OH 45433-5648, ATTN: Publications/Forms Managers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual 33-363, Management of Records, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at

<http://myaf.mil/afrims/afrims/afrims/rims.cfm>. The use of the name or mark of any specific manufacturer, commercial product, commodity, or servi

e in this publication does not imply endorsement by the Air Force.

## ***SUMMARY OF CHANGES***

This revision reflects updates to the roles and responsibilities of NASIC/SC and the Center as a result of any changes that may have taken place since the last revision. Additional language was added to require that all Proposed Contractual Documents (PCD) include a statement that reflects higher headquarter policy and directives regarding IT. Other administrative changes were made for clarity and consistency such as updating source references as applicable as well as the names of applicable higher headquarter offices, agencies, and other applicable policies, and directives.

### **1. IT MANAGEMENT OBJECTIVES.**

1.1. With authority delegated by the NASIC Commander, the CIO is the focal point for NASIC IT governance and the authority to ensure the following objectives are met.

1.1.1. NASIC clientele is provided with agile, interoperable, and enterprise compliant IT systems that support the Center, the Intelligence Community, and joint service worldwide operational arenas.

1.1.2. Guidance is provided for bringing in new information systems and technologies and developing processes to facilitate the acquisition and implementation of systems, requirements, and services throughout the Center.

1.1.3. All new programs, projects, and acquisitions are evaluated for potential impacts on the NASIC IT infrastructure and architectures while maintaining all NASIC IT under the SC umbrella through a rigorous program and portfolio management concept illustrated in Section 3 of this instruction.

1.2. As delegated by the CIO, the Systems Integration Management Office (SIMO) is the IT enterprise architect and leads the Architecture and Engineering Review Panel (AERP) to review all IT requirements and acquisitions for impact to the existing NASIC IT enterprise architecture. Any proposed deviations from NASIC IT standards shall be addressed at the AERP and exceptions or waivers will be adjudicated in accordance with the NASIC Corporate Process as defined in NASIC Instruction 90-103, *NASIC Council*.

1.2.1. The AERP will maintain the architecture to include current standards that maximize efficiencies while enabling future strategies, innovation, and the establishment of new standards. While oversight and compliance requirements will be observed, risks will also be assessed to ensure mission area innovation will not be inhibited by stagnate IT standards.

### **2. Organization and Leadership Responsibilities.**

2.1. The NASIC IT Council and IT Management Board (ITMB), as established by NASIC Instruction 90-103, *NASIC Council*, will provide strategic guidance regarding the overall management of NASIC IT. In accordance with the delegated authorities granted by the Commander, the CIO serves as the decision authority and execution arm on all directives

associated with strategic IT management, acquisition, and modernization initiatives. As chaired by the office of the CIO, the ITMB is comprised of senior representatives (i.e., Deputy Commanders/Directors) from each of the production Groups and serves to ensure all IT development and deployment activities are consistent with the NASIC strategic intent and direction. As such, the ITMB provides decision authority and management oversight for the NASIC IT enterprise to ensure all functional requirements are satisfied. The NASIC IT Council will address IT related issues that cannot be resolved in other subordinate IT venues such as the ITMB and will conduct ad-hoc or out-of-cycle sessions as necessary the discretion of the CIO.

2.1.1. The office of the CIO will provide semi-annual IT State of the Union briefings to ensure IT management and investments are planned and executed in accordance with Council direction.

### **3. Program and Portfolio Management.**

3.1. In order to meet NASIC strategic IT objectives, the CIO has aligned NASIC IT resources into functional portfolios. Each portfolio is further broken down into manageable programs that directly correlate to that portfolio's major function. Portfolio Management is recognized as a "best practice" method for the management of IT resources in a manner that provides transparency and accountability as well as a strategic approach to IT investments and decisions. (AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*).

3.2. Portfolio Managers are delegated by the office of the CIO to manage SC's portfolios spanning the core IT functions of the entire enterprise. These portfolio managers are responsible for managing the resources for all programs assigned to their respective portfolio, making recommendations to leadership for decision making purposes, and meeting on a regular basis to discuss and prioritize requirements.

3.2.1. An additional portfolio has been established to manage the Center's mission-unique IT requirements that are not covered under SC's core IT resource program. These requirements are typically resourced by the mission area and documented in signed agreements (i.e., Service Level Agreements) that detail the responsibilities, expectations, and associated resources to be provided by the requirements owner and SC.

3.2.2. *Core IT* is defined as the Standard IT hardware, equipment, networks, software and support services typically used by most every user in the Center enabling them to be productive.

3.2.3. *Mission Unique IT* is defined as the IT hardware, equipment, networks and software typically used by a sub-set of users primarily supporting accomplishment of their mission-specific responsibilities.

3.2.4. To accomplish the intent of this instruction, associated processes have been documented. All personnel are also required to adhere to the processes outlined in those process documents found on the SC SharePoint site within the Strategic IT Management folder.

### **4. Requirements and Acquisition Management.**

4.1. Requirements and requests for change arise from a deficiency in an existing operational capability, a need for a new capability, or an opportunity to replace or modernize an existing system with improved technology. All internal NASIC requesting organizations will provide SC IT requirements managers with their functional requirements via the current NASIC Communication System Requirements Document (CSRD) process. An SC requirements manager will work with the requesting organization, IT engineers, and IT portfolio managers as applicable to clarify each requirement, develop a potential technical solution, and keep all stakeholders posted on status. Other directives that drive requirements and acquisition management processes assist the NASIC CIO as follows.

4.1.1. All NASIC IT requirements, acquisition packages, contractual documents (Task Assignment Guides, Statements Of Work, Other Direct Costs, etc), and agreement documents (i.e., MOA, MOU, SLA etc.) are coordinated through and reviewed by SC to determine if they contain references to hardware, software, labor related to IT, or have an impact to the IT architecture prior to approval by the Plans and Policy Directorate (NASIC/XP).

4.1.1.1. All Task Assignment Guides, Statements Of Work, and Performance Work Statements will include the language from Figure 4.1 to ensure the chosen contractor follows IT architectural standards established by the CIO. Supporting documentation demonstrating certification and training mentioned in Figure 4.1 will be provided annually to the SC Information Assurance Branch.

**Figure 4.1. Required Contract Statement.**

All IT solutions to be implemented at NASIC must conform to and be in compliance with the NASIC Enterprise Architecture as published by the Systems Integration Management Office (SIMO) and approved by the Chief Information Officer (CIO). Any deviations from the NASIC IT standards will be addressed through the processes outlined in NASICI 33-108. All contractors and personnel requiring accounts with elevated system/network privileges must be trained and certified in accordance with [DoD 8570.01-M](#), *Information Assurance Workforce Improvement Program* and [DFARS 252.239-7001](#), *Information Assurance Contractor Training and Certification*.

4.1.1.2. All IT hardware items are required to be delivered to the Courtesy Storage Facility (CSF). These items are prohibited from entering NASIC through any other means and SC is the approval authority for all deviations to this requirement.

4.1.2. NASIC's Development Testing and Integration Capability (DTIC) maintains the authority to minimize risk to production networks by testing all hardware and software prior to operational implementation. The development aspect of the DTIC may also be used to investigate design concepts and evaluate prototypes of hardware and software and the established roles and responsibilities in support of the DTIC as a required and integral part of NASIC Strategic IT Management requirements, acquisitions, development, and advanced program initiatives. The DTIC also informs NASIC requesting organizations of incompatibilities and schedule corrective actions.

4.2. Use USAF and IC IT architectures and standards to develop and build NASIC IT architectures and standards which are used to design or modify systems within NASIC or that interact with NASIC IT systems.

4.2.1. Ensure that all IT systems are acquired following DoDD 5000.01, *The Defense Acquisition System*, and are certified by DISA/JITC (JTC3A [JIEO] Circular 9002, *Requirements Assessment and Interoperability Certification of C4I and Automated Information Systems and Equipment*).

4.2.2. Ensure NASIC Requirements & Acquisition Managers provide oversight to all IT systems throughout their life cycle by addressing identified requirements and testing interoperability in accordance with the following.

4.2.2.1. DoDI 5000.02, *Operation of the Defense Acquisition System*

## 5. Technical Solutions.

5.1. The development of all technical solutions for IT requirements falls within the purview of the Communications Systems Requirements Document (CSRD) process made available through the IT Management Plans and Policy office. Using the CSRD and additional information from the submitting office's points of contact, the requirements management and systems engineering teams will formulate a recommended overall solution that will provide the best value for the customer and will be consistent, compliant, and interoperable within the NASIC IT environment and architecture. The solutions will integrate with Wright Patterson Air Force Base (WPAFB) (88 Communications Group)(CG)), AF, DoD, and Intelligence Community (IC) architectures as applicable to comply with community standards to expedite the development of local solutions in accordance with routine requirements. Such routine requirements may include procurement of software and/or hardware that is commercially available and compatible with other locally used IT resources and requires minimal acquisition and maintenance funding. The technical solution identifies the full costs and recommended course of action to satisfy the user's need. Full costs encompass all program costs and must include all life-cycle costs, including manpower and training requirements. Technical solutions also describe alternatives considered when applicable and include any supporting information.

5.2. Where the technical solution is proposed and funded by organizations outside or external to the NASIC Communications and Information Directorate, SC system engineering representatives will assist in developing lifecycle costs estimates and other organizational impacts including cable plant, recapitalization of core IT assets used, floor space, equipment racks, power, etc. These cost estimates will be included in the models provided to the NASIC planning and programming and financial management offices. A formal project may be initiated to address potential exceptions and other requirements based upon the complexity, importance, and resource needs associated with the requirements. This determination will be made by the office of the CIO and a project manager will be assigned.

5.2.1. If the requester modifies the requirements after the technical solution has already been provided or approved or the resources have already been allocated, additional review actions will be necessary as specified in the IT Requirements process document.

5.2.2. If the modification results in an increase in the cost or impacts architectural and interoperability standards, the requirements management and systems engineering teams

will evaluate the impacts and report to the AERP, ITMB, or IT Council. This will result in a more detailed evaluation to determine if the originally identified solution is scalable or if a new package will be required or resubmitted for a new technical solution and reiteration of the approval cycle.

## **6. System Sustainment and Disposal.**

6.1. SC is responsible for the sustained care and support of NASIC Core IT. When IT is considered mission unique, the requesting organization is responsible for all maintenance and sustainment as negotiated, agreed to, and resourced accordingly in a Service Level Agreement (SLA). Where there is commonality across systems, SC will work with the requesting organization to develop a coordinated SLA to provide technical support as applicable.

6.2. The Equipment Control Officer (ECO), as delegated by the CIO, is the focal point for NASIC hardware accountability. NASIC groups and directorates will assign IT Equipment Custodians (ITECs) who are accountable to the NASIC ECO. The ITEC's, Commanders/Directors, and all permanent and tenant personnel at NASIC will ensure the inventory system is used to provide accountability of all computer resources assigned to NASIC in accordance with AFI 33-112, *Information Technology Hardware Asset Management*, and the NASIC IT Hardware Asset Management Process. The official inventory system of record for IT equipment is the Air Force Equipment Management System – Asset Inventory Management (AFEMS-AIM).

6.2.1. All AFEMS-AIM IT accountable equipment within NASIC conference and training rooms will be accounted for by the ITEC and controlled by the organization having primary responsibility for that specific room. Tenant and associate units having responsibility for conference or training rooms with non-NASIC government owned IT equipment will account for the property using their own processes and procedures. Tenant and associate unit owned IT Equipment will not be controlled by the NASIC Equipment Control Officer (ECO). NASIC IT Equipment Custodians will exclude tenant, and associate unit owned assets during physical inventories. Responsibilities for communal and shared VTC/Conference rooms will be provided by the ECO.

6.2.2. All NASIC owned IT equipment located within communications equipment and NASIC data center rooms will be controlled and accounted for by the SC Infrastructure Branch. Contractor, tenant, and associate unit owned IT Equipment in these rooms will not be controlled by the NASIC Equipment Control Officer (ECO). IT Equipment Custodians will exclude contractor, tenant, and associate unit owned assets during physical inventories.

6.2.3. Any equipment at NASIC entrance points will be controlled and accounted for by SO.

6.2.4. All IT equipment located in Conference, Training, Communications Equipment, Data Center, and entrance areas will be moved with approval from the applicable ITEC and with SC coordination.

6.2.5. An item is considered excess when it is no longer required due to mission change, equipment upgrades, technology changes, obsolescence, etc. The ECO and the Networks and Infrastructure Branch offices will assist the ITECs with this process but at a

minimum, the disposal of excess systems will meet minimal requirements as spelled out in AFI33-112.

6.3. The Software License Manager (SLM), as delegated by the CIO, is the focal point for NASIC software accountability to ensure all NASIC software acquisitions and enhancements meet security, interoperability, and usability standards before installation on NASIC networks and used within the Enterprise Architecture. If a software application is declared excess to NASIC needs, the functional owner of the software will notify the SLM who will in turn coordinate archival/removal procedures in accordance with AFI 33-114, *Software Management*.

AARON M. PRUPAS, Colonel, USAF  
Commander

## ATTACHMENT 1

### GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

#### *References*

- AFI 33-112, *Information Technology Hardware Asset Management*, 7 January 2011
- AFI 33-114, *Software Management*, 13 May 2004
- AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*, 23 December 2008
- AFMAN 33-363, *Management of Records*, 1 March 2008
- AFPD 33-1, *Cyberspace Support*, 9 August 2012
- DFARS 252.239-7001, *Information Assurance Contractor Training and Certification*, January 2008
- DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 Dec 2005
- DISA/JITC (JTC3A [JIEO] Circular 9002), *Requirements Assessment and Interoperability Certification of C4I and Automated Information Systems and Equipment*
- DODD 5000.01, *The Defense Acquisition System*, 20 November 2007
- DoDI 5000.02, *Operation of the Defense Acquisition System*, 8 Dec 2008
- NASIC Instruction 90-103, *NASIC Council*, 17 June 2010

#### *Adopted Forms*

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

#### *Abbreviations and Acronyms*

- AERP**—Architecture and Engineering Review Panel
- AF**—Air Force
- AFISRA**—Air Force Intelligence, Surveillance, Reconnaissance Agency
- AFMAN**—Air Force Manual
- AFPD**—Air Force Policy Directive
- AFRC**—Air Force Reserve Command
- AFRIMS**—Air Force Records Information Management Systems
- ANG**—Air National Guard
- CG**—Communications Group
- CSRD**—Communication System Requirements Document
- CIO**—Chief Information Officer
- CSRD**—Communication System Requirements Document
- DoD**—Department of Defense

**DTIC**—Development Testing and Integration Center  
**EC**—Equipment Custodian  
**ECO**—Equipment Control Officer  
**IAW**—In Accordance With  
**IC**—Intelligence Community  
**IT**—Information Technology  
**ITMB**—Information Technology Management Board  
**NASIC**—National Air and Space Intelligence Center  
**OPR**—Office of Primary Responsibility  
**PCD**—Proposed Contractual Documents  
**RDS**—Records Disposition Schedule  
**SIMO**—Systems Integration Management Office  
**SLA**—Service Level Agreement  
**WPAFB**—Wright Patterson Air Force Base