This Air Force (AF) policy directive establishes AF policy for information technology (IT) governance and compliance under the direction of the Chief of Information Dominance and Chief Information Officer (SAF/CIO A6). This directive implements Office of Management and Budget (OMB) Circular A-11, Preparation, Submission, and Execution of the Budget; OMB Circular A-130, Management of Federal Information Resources; OMB Memorandum M-11-29, Chief Information Officer Authorities; Department of Defense Directive (DoDD) 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS); DoDD 8000.01, Management of the Department of Defense Information Enterprise; DoDD 5000.01, The Defense Acquisition System; Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System; Directive Type Memorandum (DTM) 11-009, Acquisition Policy for Defense Business Systems; DoDD 8115.01 Information Technology Portfolio Management; DoDI 8115.02 Information Technology Portfolio Management Implementation; Department of Defense Instruction (DoDI) 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS); Subtitle III of Title 40 of the Clinger-Cohen Act (CCA) of 1996, National Defense Authorization Act (NDAA) 2005 § 2222, NDAA 2009 (PL110-417) § 908, NDAA 2010 § 1072, NDAA 2010 § 804 and NDAA 2012 § 901; Federal Information Security Management Act (FISMA), 44 USC § 3541, 2002, Title 10, USC, Section 2223(b) Information Technology: Additional Responsibilities of Chief Information Officers of Military Department, 2007. This directive applies to all military and civilian AF personnel, members of the AF Reserve and Air National Guard, and AF contractors. Comments and recommended changes regarding this publication should be sent through appropriate channels using AF Form 847, Recommendation.
for Change of Publication, to the office of primary responsibility (OPR) for SAF/CIO A6 policy, SAF/A6PPA, safa6ppa@pentagon.af.mil. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the AF Records Disposition Schedule (RDS) located at: https://www.my.af.mil/afrims/afrims/afrms/rims.cfm.
SUMMARY OF CHANGES

This document has been substantially revised and formalizes the Information Technology (IT) Governance Executive Board (GEB) chartered in the terms of reference signed by the Secretary of the Air Force (SECAF) on 3 April 2012. In addition to change in title, this directive aligns IT management with current Air Force (AF) doctrine, statutory, and regulatory guidelines.

1. Overview.

1.1. Purpose. This directive establishes the AF policy for IT governance to provide a process for the SAF/CIO A6 to fulfill the duties of the AF Chief Information Officer (CIO) established in federal laws and Department of Defense (DoD) issuances, SAF/CIO A6 and CIO are used interchangeably in this publication. This directive establishes the policy, guidance, and oversight as they apply to all information, information systems (IS), and IT infrastructure within AF purview. Non-AF space systems are multi-component space systems (e.g., those supporting more than one DoD component) and are under the purview of United States Strategic Command. This directive also establishes the AF ITGEB, which will oversee the execution of IT councils, boards, and working groups throughout the IT lifecycle, and provide a means in which the AF can cross functionally align AF Enterprise IT activities to effectively and efficiently deliver capabilities to users.

1.2. Scope. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements. The scope of this directive includes but is not limited to IT governance in the context of IT business and mission strategy alignment, IT performance measurement and delivery, requirements definition, program development (including sustainment), test, deployment, and operations, under the direction and authority of the AF ITGEB, chaired by the AF CIO.

2. Policy. It is AF policy to establish guidance, objectives, and standards for IT compliance and governance; to oversee IT investment strategy with business and mission strategy; and to establish performance measures under which requirements, investments, programs, and acquisitions will reach targeted results. Accordingly, the AF shall:

2.1. Develop AF Enterprise Architecture (EA) guidance, objective, and standards consistent with DoDD 4630.05. The AFEA, as part of the DoD EA links the DoD Information EA and the subordinate AF network architecture. As such, the AFEA will be used to identify capability gaps, reduce duplication, and drive modernization efforts.

2.2. Develop guidance, objectives, and standards for IT reporting, IT portfolio management, and IT investment management as prescribed by OMB Circular A-11, OMB Circular A-130, DoDD 8115.01, and DoDI 8115.02.

2.3. Develop guidance, objectives, and standards for interoperability and supportability of IT systems as prescribed in DoDD 4630.05.

2.5. Develop guidance, objectives, and standards for compliance with the *Clinger-Cohen Act of 1996* as prescribed in DoDI 5000.02 and 10 USC § 8014 and 1704.

2.6. Develop AF Information Assurance (IA) and computer network defense guidelines, objectives, and standards in accordance with Federal Information Security Management Act (FISMA), 2002.

3. **Responsibilities.** The responsibilities for IT governance are shared among numerous key stakeholders. CIO responsibilities are codified in *Clinger-Cohen Act 1996*, Title 40, 10 USC § 2222, 2223b, and 8014, and 40 USC § 11315; Acquisition authority in 10 USC § 8014 and 1704; Chief Financial Officer authority in 10 USC § 8022 (a) and (b); and Chief Management Officer authority in NDAA 2009 § 908, NDAA 2010 § 1072, and 10 USC § 2222. These key stakeholders, along with the Assistant Secretary of the Air Force for Acquisition (SAF/AQ), the Deputy Chief of Staff for Plans, Operations and Requirements (AF/A3/5), the Vice Commander, Air Force Space Command (AFSPC/CV) and the Program Executive Officer (PEO) for Command, Control, Communications and Information Networks (C3I&N), are members of the ITGEB and are identified within this directive. Each position on the board holds important responsibilities for IT governance, many of which are responsibilities previously established in federal law and/or DoD issuances:

3.1. **SAF/CIO A6 shall:**

3.1.1. Oversee governance and accountability of IT policy and capabilities IAW 10 USC § 2222, 2223b, and 8014, on behalf of the SECAF. As the AF CIO, chairs the ITGEB.

3.1.2. Co-Chair Warfighting Systems Integration (WFI) General Officer Steering Group (GOSG).

3.1.3. Focus on four main areas: governance, commodity IT, oversight of AF’s IT portfolio, and IA. In each of these focus areas; the AF CIO shall facilitate the resolution of issues that affect multiple organizational areas of responsibility (e.g., acquisition and functional, other Services and agencies). As such, the CIO engages and partners with other key stakeholders to reach resolution. The organizations with which the CIO engages include Headquarters (HQ) AF Space Command (AFSPC) for IT infrastructure requirements and operations; SAF/AQ and the AF Deputy Chief Management Officer (DCMO) as defined in the Cyberspace Core Functional Master Plan (CFPM); SAF/AQ for IT acquisition and program management policy and training; the AF DCMO and Assistant Secretary of the Air Force/Financial Management and Comptroller (SAF/FM) for business system certification; the Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (AF/A2) as the functional manager for intelligence, surveillance, and reconnaissance (ISR); and the AF/A3/5 for IT mission systems.

3.1.4. Develop policy and guidance for AF IT portfolio management activities.

3.1.5. Provide IT planning, budget, management, and compliance oversight and other measures deemed necessary to evaluate the adequacy and efficiency of information resources and compliance with statutory and regulatory guidelines.

3.1.6. Ensure interoperability and supportability of IT in business and NSS programs across the AF and with the Joint community, as well as compliance with the associated baselines and standards and plans put forth by the DoD.
3.1.7. Direct functionals, major commands (MAJCOMs), field operating agencies (FOAs), and direct reporting units (DRUs) to maintain a consolidated inventory of mission critical, mission essential, and mission support IT systems, identify interfaces between those systems and other IT systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those mission critical, mission essential, and mission support systems.

3.1.7.1. Develop AFEA guidance, objective, and standards consistent with DoDD 4630.05.

3.1.7.2. Maintain the overarching AFEA that enables architecture artifacts and information to be exchanged across the AF and with other DoD elements. Ensure solution architectures are maintained and demonstrate the AF capabilities and mission/business processes that the systems support.

3.1.7.3. Integrate architectures from the target organizations.

3.1.7.4. Establish policy for the application of identity attributes into an operational environment.

3.1.7.5. Standardize and integrate architectures from each AF Service Core Function (SCF) and lower-level domains where appropriate.

3.1.8. Oversee AF emerging technology efforts for applicability to existing and future IT programs and systems. Identify relevant approaches through establishment and maintenance of the target baseline.

3.1.9. Advise SECAF and the AF corporate structure on the budgetary implications of decisions concerning IT and on an annual basis provide the AF corporate structure with budgetary options to increase efficiency and effectiveness of AF IT expenditures.

3.1.10. Integrate the target baseline (TB), implementation baseline (IB), and operational baseline (OB) with ITGEB coordination.

3.1.11. Develop, implement, and provide oversight for the AF IA program in accordance with 44 USC § 3542 (PL 107-347), FISMA.

3.2. AF/A3/5 shall:

3.2.1. Serve as the coordination point between SAF/CIO A6 Cyber, and AF/3/5 Cyber Operations.

3.2.2. Chair/Co-Chair the command and control (C2) GOSG.

3.2.3. Co-Chair WFI GOSG.

3.2.4. Coordinate with AF/A2 and SAF/CIO A6 and facilitate the cross Functional review of AF C2ISR policy, processes, requirements, and supporting systems.

3.2.5. Provide status updates to the AF ITGEB as needed. Bring perspective, priorities, and challenges from the functional community.

3.3. SAF/AQ shall:

3.3.1. Execute delegated responsibilities for the SECAF as the service acquisition executive.
3.3.2. Establish an acquisition approach to AF IT that applies the target, implementation and operational baselines and supports an AF commoditized IT infrastructure to the maximum extent possible.

3.3.3. Align IT acquisition strategies and requirements across the mission capability PEOs, PEO Battle Management, and PEO C3I&N.

3.3.4. Provide for the timely acquisition and lifecycle management of required IT.

3.3.5. Oversee AF IT program execution and provide status updates, as needed, to the AF ITGEB. Provide acquisition policy, cost, schedule, risk, and performance inputs to the ITGEB.

3.4. The SAF/FM shall:

3.4.1. Ensure business case analysis (BCA) and economic analysis supporting IT requirements complies with policy, procedures, and guidance. Review and coordinate on BCAs and economic analysis supporting IT requirements when requested by senior HQ USAF functional leadership or senior leadership of MAJCOMs or other field units.

3.4.2. IAW 10 USC § 8022, approve and supervise all financial IT programs to ensure achievement of finance and accounting standards and provide status updates, as needed, to the AF ITGEB.

3.4.3. Provide budget and cost perspective, priorities, and challenges to the ITGEB.

3.5. DCMO shall:

3.5.1. Provide quantitative analysis addressing the use of IT and promote change management across the AF to improve productivity, efficiency, and effectiveness of AF mission and business processes, including those supported by IT capability.

3.5.2. Coordinate and facilitate, IAW NDAA 2012 § 901, the cross-functional review of AF DBS and serve as the business systems Pre-Certification Authority.

3.5.2.1. Coordinate and facilitate, with the AF functional leaders, the grouping of business capability requirements and assign priorities to the same.

3.5.3. Coordinate and facilitate, with the AF functional leaders, the development of business sub-enterprise architecture, including the capture of business processes and supporting IT DBS.

3.5.3.1. Coordinate and facilitate, with the AF functional leaders, validation and concurrence with the DoD business EA.

3.5.4. Lead business process reengineering efforts across functional domains. Define AF information requirements in support of business processes through communities of interest.

3.5.5. Provide relevant issue status updates to the ITGEB.

3.6. Director, Air Force Test and Evaluation (AF/TE) shall:

3.6.1. Function as the chief T&E advisor to AF senior leadership according to Headquarters Air Force (HAF) Mission Directive (MD) 1-52, Director of Test and Evaluation, and AFI 99-103, Capabilities-Based Test and Evaluation. Responsible to the
Chief of Staff of the Air Force (CSAF) for establishing AF T&E policy, determining the adequacy of T&E resources required to support weapons system development, and resolving T&E issues.

3.6.2. Adjudicate T&E issues between MAJCOMs, contractor, developmental and operational test organizations, HAF principals, the Services, Office of the Secretary of Defense, and Congress.

3.6.3. Oversee the AF T&E infrastructure by ensuring adequate T&E resources to support system acquisition activities, administer various T&E resources processes and chair or serve on various committees, boards, and groups listed in HAF MD 1-52.

3.6.4. Coordinate with AF organizations and other DoD components to provision and maintain IT test environments in support of the continuum of T&E activities.

3.7. AF Chief Technology Officer (CTO), under the guidance and direction of the SAF/CIO A6 shall:

3.7.1. Advise the CIO and executive/senior level technical leadership on IT emerging technology, EA, enterprise infrastructure, and strategy including identifying short- and long-term goals of DoD-wide IT initiatives, ensuring the integrity, interoperability, supportability, and cost-effectiveness of the Department’s IT.

3.7.2. Chair the AF Target Baseline (TB) Configuration Control Board (CCB).

3.7.3. Develop, manage, and maintain the TB consisting of the architectures, standards, protocols, and guidelines that define an AF enterprise-wide and government-owned technical architecture required for inclusion in the IB and OB.

3.7.4. Maintain constant communication and synchronization of the TB, under ITGEB authority, with the IB and OB.

3.7.5. Partner with the Senior Information Assurance Officer (SIAO) to ensure emerging technologies, capabilities, enterprise architecture, and infrastructure are properly analyzed to assessed security risk, linkage to IA policies, and secure integration prior to implementation.

3.8. AF SIAO, under the guidance and direction of the SAF/CIO A6 shall:

3.8.1. Manage the AF IA program and serve as the senior advisor to the CIO on all matters related to IA, providing technical leadership, direction, and oversight of the department-wide IA program.

3.8.2. Develop and certify IA policies and ensures AF compliance with statutory, DoD, and Joint directives to ensure the confidentiality, integrity, availability, authentication, and non-repudiation of AF information and ISs.

3.8.3. Chair the AF IA Technical Advisory Group. This group assists the AF SIAO in the management and oversight of the AF IA program and escalates enterprise risk decisions to the ITGEB.

3.8.4. Partner with the CTO to conduct programmatic risk analysis on emerging technologies, capabilities, enterprise architecture, and infrastructure.

3.9. HQ AFSPC shall:
3.9.1. Serve as lead MAJCOM for cyberspace operations.

3.9.2. Serve as Cyberspace Superiority (CS) Core Function Lead Integrator (CFLI).

3.9.3. Work with SAF/CIO A6 on IT programs/concepts inside the CS Core Function Master Plan (CFMP).

3.9.4. Establish capability needs and requirements for IT infrastructure within the cyber CFLI portfolio.

3.9.5. Serve as final approving authority for deployment of mission and functional IT systems/applications into the OB.

3.9.6. Designate the chair of the AF OB configuration management process.

3.9.7. Establish, implement, and maintain AF processes that ensure configuration conformance for both infrastructure configuration and applications in the OB.

3.9.8. Establish capability needs and requirements for IT infrastructure within the scope of the CS CFMP.

3.9.9. Plan, program, and execute approved investments for IT infrastructure. Operate the AF IT infrastructure worldwide per the CS CFMP.

3.9.10. Provide oversight and guidance for the development, deployment, administration, maintenance, documentation, and sustainment of the AF IT Infrastructure OB.

3.9.11. Maintains constant communication and synchronization of the OB, under CFLI authority, with the TB and IB.

3.10. CFLIs shall:

3.10.1. Plan and program investments for IT infrastructure for that SCF.

3.10.2. Coordinate with CS CFLI to deconflict and prevent duplication of enterprise capabilities within the CS CFMP.

3.11. PEO C3I&N, under the guidance and direction of the SAF/AQ shall:

3.11.1. Develop and provide the AF a commoditized IT infrastructure environment, as specified by the IB, where possible.

3.11.2. Designate the chair of the AF IB CCB.

3.11.3. Develop, manage, and maintain the IB consisting of selected products and their allowed configurations that implement the technical architecture, standards, protocols, and guidelines specified in the TB.

3.11.4. Coordinate with mission/business PEOs to ensure successful deployment of mission and functional IT systems/applications into the commoditized infrastructure.

3.11.5. Assist HQ AFSPC with provisioning mission/functional systems/applications into the enterprise hosting environment.

3.11.6. Provide mission/functional systems/applications access to AF enterprise test and development, certification and accreditation, and testing environment for pre-deployment test, evaluation, and accreditation.
3.11.7. Maintains constant communication and synchronization of the IB, under ITGEB authority, with the TB and OB.

3.12. Mission Capability PEOs, under the guidance and direction of the SAF/AQ.

3.12.1. Shall coordinate, facilitate, and promote a process that captures and documents requirements, develops capability architecture artifacts that conform to the AFEA, and promotes reusable application designs.

3.12.2. Implement Information Technology Infrastructure Library (ITIL) to develop common services.

3.12.3. Deliver standards and processes that facilitate requirements analysis, product acquisition, and code development of service and capabilities.

3.12.4. Maximize end-user participation to validate mission accomplishment through the use of automated test capabilities.

3.13. **All other HAF functional, MAJCOMs, DRUs, and FOAs:**

3.13.1. Support the governance structures with membership as each chair defines in AFIs.

3.13.2. Implement policies as delegated and defined in AFIs by the IT governance structure.

3.13.3. Ensure all IT investments are identified within AF data collection systems to support the AF CIO responsibility within paragraph 3.1.7.

4. **IT Governance for ISR.** Nothing in this directive shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) or intelligence Special Access Programs. The application of the provisions and procedures of this directive to SCI or other intelligence ISs is encouraged where they may complement or address areas not otherwise specifically addressed. AF ISR governance, compliance, and reporting is through DNI (per OMB Title 40 & 44), Under Secretary of Defense (Intelligence) (AF DCGS Memo, 27 Mar 2012), and Director of Central Intelligence Agency and Director of National Security Agency (National Institute of Standards and Technology Special Publication 800-59 & Executive Order 12333).

Michael B. Donley
Secretary of the Air Force
Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References
AFI 33-360, Publications and Form Management, 18 May 2006
AFI 99-103, Capabilities-Based Test and Evaluation, 26 February 2008
AFMAN 33-363, Management of Records, 1 March 2008
National Defense Authorization Act (NDAA), Published Annually
Clinger-Cohen Act (CCA), 1996
OMB Circular A-11, Preparation, Submission, and Execution of the Budget, 3 August 2012
OMB Memorandum M-11-29, Chief Information Officer Authorities, 8 August 2011
DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and, National Security Systems (NSS), 5 May 2004
DoDD 5000.01, The Defense Acquisition System, 12 May 2003
DoDD 8000.01, Management of the Department of Defense Information Enterprise, 10 February 2009
DoDD 8115.01, Information Technology Portfolio Management, 10 October 2005
DoDI 8115.02, Information Technology Portfolio Management Implementation, 30 October 2006
DoDD 8500.01, Information Assurance, 24 October 2002
DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004
DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008
DTM 09-013, Registration of Architecture Descriptions in the DOD Architecture Registry System, IC 2, 18 December 2009
FISMA, 44 USC § 3541, 2002
Title 10, USC, Section 2223(b) “Information Technology: Additional Responsibilities of Chief Information Officers of Military Department, 2007
National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System, August 2003
Prescribed Forms
None.

Adopted Forms
AF Form 847, *Recommendation for Change of Publication*

*Abbreviations and Acronyms*

AF—GIG—Air Force-Global Information Grid
AFI—Air Force Instruction
AFMAN—Air Force Manual
AFPD—Air Force Policy Directive
AFSPC—Air Force Space Command
BCA—Business Case Analysis
C2—Command and Control
C3I—Command, Control, Communications and Intelligence
CCA—Clinger-Cohen Act
CCB—Configuration Control Board
CFLI—Core Function Lead Integrator
CIO—Chief Information Officer
CSAF—Chief of Staff of the Air Force
CTO—Chief Technology Officer
DBS—Defense Business System
DCMO—Deputy Chief Management Officer
DoD—Department of Defense
DoDD—Department of Defense Directive
DoDI—Department of Defense Instruction
DTM—Directive Type Memorandum
DRU—Direct Report Units
EA—Enterprise Architecture
E-SWG—Enterprise Senior Working Group
FISMA—Federal Information Security Management Act
FOA—Field Operating Agency
GIG—Global Information Grid
GOSG—General Officer Steering Group
HAF—Headquarters Air Force
HQ—Headquarters
IA—Information Assurance
IAW—In Accordance With
IB—Implementation Baseline
ISR—Intelligence, Surveillance, and Reconnaissance
IT—Information Technology
ITGEB—IT Governance Executive Board
ITIL—Information Technology Infrastructure Library
MAJCOM—Major Command
NDAA—National Defense Authorization Act
NSS—National Security System
OB—Operational Baseline
OMB—Office of Management and Budget
OPR—Office of Primary Responsibility
PEO—Program Executive Officer
PEO C3I&N—Program Executive Officer for Command, Control, Communications and Intelligence and Networks
SCF—Service Core Function
SECAF—Secretary of the Air Force
TB—Target Baseline
TEMP—Test and Evaluation Master Plan
T&E—Test and Evaluation
ToR—Terms of Reference
WFI—Warfighting Integration

Terms
Air Force Corporate Structure—Embodies the corporate review process for HAF. It does not replace the functional staff but, rather, enhances it by allowing time critical or time limited functional reviews at the appropriate levels. The deliberative components of the Corporate Structure are the Air Force Council, the Air Force Board, the Air Force Group, and the thirteen Mission and Mission Support Panels. This structure increases management effectiveness and improves cross-functional decision-making by providing a forum in which senior AF leadership can apply their collective judgment, experience, and analysis to major programs, objectives, and issues. This process balances programs among mission areas, between force structure and support, and between readiness, modernization, and transformation. Additionally, this approach
ensures the AF program is capabilities based and supports the Joint warfighter. Only military or DoD civilian personnel assigned to the Air Staff or Office of the Secretary of the Air Force may serve as members of the corporate structure.

**AF-GIG Infrastructure**—The AF cyberspace infrastructure consisting of AF-owned/leased and controlled components (hardware, software, networks, systems, equipment, facilities, and services) operated by DoD, AF, contractor or other entity on behalf of the AF, which stores, transmits, receives, or processes information, regardless of classification or sensitivity.

**Commoditize**—to render (a good or service) widely available and interchangeable with one provided by another company.

**Community of Interest (COI)**—COIs will detail the requirements for all information exchanges within the entire material solution, regardless of the technical implementation of each information exchange.

**Direct Reporting Unit (DRU)**—Has a specialized and restricted mission, and is directly subordinate to the CSAF or to Chief of Staff’s representative on the Air Staff.

**Enterprise Architecture (EA)**—The explicit description and documentation of the current and desired relationships among business and management processes and supporting resources (e.g., IT, personnel). It describes the "current architecture" and "target architecture," to include the rules, standards, and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with Government Paperwork Elimination Act, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail.

**Enterprise Senior Working Group (E-SWG)**—The E-SWG provides cross-functional review and guidance to AF modernization efforts with focus on Business Mission Area. It also supports the SAF/CIO A6 AF CIO responsibilities of ensuring compliance with public law, Federal, DoD, and AF directives regulating the investment in, and management and operation of IT.

**Field Operating Agency (FOA)**—A subdivision that carries out activities under the operational control of a HAF functional manager.

**Form**—A document with a fixed arrangement of captioned spaces designed for entering and extracting prescribed information. Categories of forms include internal, interagency, public use, standard, and optional.

**General Officer Steering Group (GOSG)**—A forum that provides senior executive leadership the venue to develop, review, and recommend guidance for the Air Force, synchronize transformation, modernization, and functional support efforts. A GOSG, advises, assists, and makes recommendations to the SECAF, CSAF, HAF, CFLIs, and the MAJCOMs on their focus
area(s). It is generally chaired by an Air Staff functional two-letter director (e.g. SAF/CIO A6) and its members are selected, in part, by their equities in the steering group’s focus area(s).

**Implementation Baseline (IB)**—The Implementation Baseline is the baseline of acquisition selected products and their informed/allowed configurations that implement the architecture, standards and protocols, and guidelines specified in the Target Baseline. The Implementation Baseline informs the Operational Baseline of the acquisition selected products and how they are to be configured to support deployment of user applications across the infrastructure topology. The Implementation Baseline governs the implementation of the Development and Integration/Test environments.

**Information Assurance (IA)**—Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD 8500.01)

**Information System (IS)**—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (JP 3-13) A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated IS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

**Information Technology (IT)**—Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term “IT” does not include any equipment that is required by a Federal contractor incidental to a Federal contract. Note: The above term is considered synonymous with the term “information system” as defined and used in AF programs.

**Information Technology Governance Executive Board (ITGEB)**—The scope for the ITGEB includes the entire AF IT enterprise for business and mission capabilities, including business and national security systems, and excluding the imbedded software in support of weapons platforms. The senior leadership team shall include the SAF/CIO A6, SAF/AQ, AFSPC/CV, PEO C3I&N, AF/A3/5, and SAF/US(M). SAF/CIO A6 shall chair this decision making body. This senior leadership team shall charter a subordinate working group to plan, recommend, and support the senior leaders in the implementation of process alignment initiatives, description of functions and skill sets required to support enterprise capabilities, and development of the enabling capabilities necessary to achieve the AF IT vision. This team shall focus on the commoditization and operational configuration management of a baseline IT infrastructure and the business practices to exploit that IT infrastructure for AF users.

**Integrated Test Lifecycle Capability (ITLC)**—A concept for organizing, integrating, and directing widely distributed T&E organizations, skilled personnel, and capabilities at the Air
Force Enterprise level into an efficient continuum that rapidly designs, develops, acquires, tests, operates, and sustains IT systems throughout their life cycle. It is the basis for a common, secure, agile, and versatile development environment for IT systems that integrates the efforts of multiple AF functions, domains, and processes. It leverages and aligns policies, processes (e.g., requirements, funding, systems development, acquisition, T&E, training, operations, management, systems sustainment), skilled IT practitioners, test “ranges” and capabilities, and operational users to efficiently deliver IT capabilities and core services to support AF missions.

**IT Portfolio Management (Portfolio management)**—The management of selected groupings of IT resources using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing). Source: DoDD 8115.01

**National Security System (NSS)**—Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Adapted from NIST SP 800-59)

**Operational Baseline (OB)**—The Operational Baseline is the set of components of the AF IT infrastructure that specifies the exact laydown and configurations of hardware and software within all facilities in the AF infrastructure topology and provide the required warfighter capabilities and performance.

**Target Baseline (TB)**—The Target Baseline specifies the standards, protocols, guidelines and implementation constraints for the future state of the AF-GIG Infrastructure. It is used to inform the development of the implementation baseline. The Target Baseline is thoroughly documented and continually updated based upon emerging industry standards and the evolving AFEA.